COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 16 November / 16 novembre 2017 T-PD(2017)16Rev

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL

(T-PD)

Compilation of comments on the draft practical guide on the use of personal data in the police sector

Compilation des commentaires sur le projet de guide pratique sur l'utilisation de données à caractère personnel par la police

Directorate General of Human Rights and the Rule of Law /

Direction Générale droits de l'Homme et Etat de droit

TABLE DES MATIERES

BELGIUM / BELGIQUE

1. Au point 2, paragraphe 2 :

   Remplacer « La collecte de données personnelles pour des objectifs de police devrait être limitée à ce qui est nécessaire à la prévention d'un danger réel ou la suppression d'une infraction précise. Toute exception à cette disposition devrait faire l'objet d'une législation nationale particulière »
   Par « La collecte de données personnelles pour des objectifs de police devrait être limitée à ce qui est nécessaire à l'enquête ou à d'autres taches de la police comme prévu au point 1. Toute exception à cette disposition devrait faire l'objet d'une législation nationale particulière »

Justificatif

Il serait préférable de reprendre ou de référer à ce qui est prévu au Pt 1 pour les finalités possibles des traitements.

2. Au point 5, encadré exemple :

   Remplacer « Cependant, une fois que le but de la surveillance secrète est atteint, la personne concernée doit être informée qu'elle ou il a été sujet(te) à une telle mesure »
   Par « Cependant, une fois que le but de la surveillance secrète est atteint et que la procédure le permet, la personne concernée devrait être informée qu'elle ou il a été sujet(te) à une telle mesure »

Justificatif :

L'exemple n'est pas assez nuancé lorsqu'il dit que la personne doit être informée. Il ne correspond pas à l'explication qui le précède : "Même si des restrictions ou des dérogations au droit à l'information ..., des informations devraient être fournies aux personnes concernées dès que cela ne crée plus d'obstacles au but pour lequel leurs données ont été utilisées".

L'exemple résume en disant : "Cependant, une fois que le but de la surveillance secrète est atteint, la personne concernée doit être informée qu'elle ou il a été sujet(te) à une telle mesure".

Dans l'exemple, deux adaptations sont demandées :

- utiliser le conditionnel;

- le but de la surveillance est peut être atteint mais la procédure n'est pas pour autant terminée et la communication peut ne pas encore pouvoir se faire.

T-PD (2017)16

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied to ensure the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").
Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed application and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[1] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level.
The present Guide was therefore preparedto highlight the most important issues that may arise in the use of personal data in the police sector and to pointout the key elements to be considered in that context.
This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance.
The overarching principles set out in Recommendation (87)15 and their practical implications aim to ensure that the processing of personal data by the police is carried out in full respect of the rights of the individual to privacy and data protection.
To facilitate the reading of the Guide, a glossary of the terms used is provided at the end of the document.

General considerations

The collection and use of personal data for law enforcement purposes constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and, as such, it *must* be based on law (clear, foreseeable and accessible), pursue a legitimate aim and be limited to what is necessary and proportionate to achieve that legitimate aim. (Former second paragraph moved upfront)

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data processing within the police should be based on predefined, clear and legitimate purposes set in the law; it should be necessary and proportionate to these legitimate purposes and should not be processed in a way incompatible with those purposes. Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible.

1. Scope

The principles explained in the present guide apply to the processing of personal data for police purposes, for the purposes of the prevention, investigation and prosecution of criminal offences, the execution of criminal penalties [and for the maintenance of public order by the police] (hereafter referred to as "tasks of the police", ["police purposes"]). Where 'police' is used in the text, it can be taken to mean wider law enforcement authorities, and/or other public and/or private bodies authorised by law to process personal data for the same purposes.

[1] See Report "Twenty–five years down the line" – by Joseph A. Cannataci

Deleted: for ensuring

Deleted: clear

Deleted: , aiming

Deleted: ing

Deleted: in the police

Deleted: use

Deleted: are

Deleted: the a balance is struck between the essential objectives of general public interest (prevention, investigation and prosecution of criminal offences, the execution of criminal penalties and maintenance of public order), and the respect for

Deleted: that it

Deleted: [in principle]

Deleted: always be in compliance with the original purpose. The

Deleted: d

Deleted: It

Deleted: data which are processed within the police

Deleted: (Start) The collection and use of personal data for law enforcement purposes can constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and as such it *must* be based on law (clear and publicly available), pursue a legitimate aim/aim and be limited to what is necessary to achieve that legitimate /aimaim.

Deleted: primarily

Deleted: specific

Deleted: offences and the

2. Collection of data and use of data

The police as data controller is responsible for all data processing it undertakes and is accountable for its data processing operations.

The collection of personal data for police purposes should be limited to what is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

It is understood from Point 2.1 of the Recommendation that inforthe fulfilment of both of the main police tasks (prevention of a real danger and the suppression of a specific criminal offence), an evident and direct correlation should exist between the data processing carried out by the police and a situation where individuals have already committed or are likely to commit a crime.

The police should always choose the adequate legal basis to process personal data and should process personal data in a legitimate way. A careful assessment should be carried out by police to make sure that the processing is based on an appropriate legislation and the procedures for data processing foreseen by it are fully respected.

The police should apply at all stages of the processing the relevant data protection principles (most importantly the principles of necessity, proportionality and purpose-bound data processing), and should not continue to process data which are not needed for the purposes. In this context, personal data collected at an early phase of the investigation, which then proves with the process of the investigation to be no longer relevant should no longer be processed (e.g. innocence of a suspect is confirmed), and should therefore either be blocked or deleted. This does not apply where subsequent use of the data is allowed (point 3).

Prior to and during the collection of such data, the question of whether the personal data collected is necessary for the investigation or for a task of the police as described in Point 1, should always be considered. One should note that once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific task of the police) should exist. This link together with compliance to the data protection principles as described in the Guide, must be demonstrable at all times. After the collection phase and at different stages of the investigation and prosecution, a thorough analysis is needed to assess which data are to be retained and which are to be deleted.

Before collecting any personal data, investigators should ask themselves the question 'Why is it necessary to acquire the data?', 'What, exactly, do you seek to achieve?'.

Example – For personal data such as Telephone Billing: only the number(s) required for the time periods being investigated should be sought and only for those individuals suspected of having a link with the offence.

A list of phone numbers of the person(s) involved in the suspected offence can be collected if there are indications that such data serve the purpose of the investigation. It cannot be kept or processed after the analysis shows that the data are not strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for police purposes should be used for those purposes only and should not be used in any other way that is incompatible with the original purpose stated at the time of collection and is necessary for and proportionate to the pursuing of police purposes, unless this is provided for in law (see Article 9 of Convention 108). [In assessing the compatibility of the use of data for the same purpose, one should consider the following criteria: (i) relation between purposes; (ii) context of the collection and information given to data subjects; (iii) nature of personal data; (iv) consequences for data subjects of the intended subsequent use; (v) existence of appropriate safeguards.]

Deleted: The collection and use of personal data for police purposes should be limited to is necessary for the purpose of prevention, investigation and prosecution of criminal offences and the execution of criminal penalties (i.e. to a specific criminal offence or the suspicion thereof) and where personal data is processed for the purpose of the maintenance of public order.

Deleted: therefore

Deleted: it can be

Deleted: held

Deleted: has to be reiterated that according to

Deleted: during

Deleted:

Deleted: The collection and use of personal data for law enforcement purposes can constitute an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and as such it *must* be based on law (clear and publicly available), pursue a legitimate aim and be limited to what is necessary to achieve that legitimate aim.

Deleted: P

Deleted: e

Deleted: f (e.g.: for testimonies consent seems to be adequate, but for cross-checking data in different data base legal provisions must exist). Legitimate data processing implies that the processing shall be lawful and ...

Deleted: P

Deleted: -

Deleted: ,

Deleted: principle

Deleted: they should be

Deleted: permanently

Deleted: .

Deleted: specific

Deleted: asked

Deleted: During collection, provided ...

Comment [A1]: to reflect that the pul ...

Deleted: in order

Deleted: Police should apply the da ...

Deleted: the relevant people.

Deleted: collection,

Deleted: in law

Deleted:).

Comment [A2]: we are not convince ...

Subsequent use of data is considered for the purposes of this guide as a new data processing operation which has to fulfil all the criteria and conditions mentioned above. The subsequent use of data shall be lawful, undertaken for a legitimate aim and necessary and proportionate to this legitimate aim.

The police shall ensure at all stages of the data processing and for the subsequent use of data as stated in the General considerations that the personal data are accurate, up-to-date, adequate, relevant and not excessive in relation to the purposes for which they are processed.

Example: Police data collected for an investigation where the political affiliation is irrelevant, cannot then be used to determine the political affiliation of the concerned person.

3. Subsequent use of data

Every subsequent processing of data for police purposes other than that the data were originally collected for, must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be undertaken for a legitimate aim and should be necessary and proportionate to the legitimate aim pursued.

Personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set out in Point 2. The general rule is that if data are likely to be used in a different case or in a different operation of the police, the assessment of compliance described in Point 2 shall be applied to this new processing as well. (This is not applicable if data are used for purely statistical or scientific purposes). Notwithstanding thecomputerised and/or automated data processing and the large volume of personal data stored very often in different processing environments, the personal data collected and retained for police purposes should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

It should be noted, moreover, that any subsequent use of personal data related to vulnerable individuals such as victims, minors, or of those enjoying international protection, should be subject to additional care and legal analysis with a special attention to the application of the principles of necessity and proportionality.

In cases such as trafficking in human beings, drug trafficking or sexual exploitation, where victims' data may subsequently be used also when they are considered as suspects, or where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to look at existing international good practice (in international or regional police bodies) and to enhance their exchange of information on the matter with other national police bodies.If all legal requirements as put forward in Point 2 are met, it should not represent any obstacle to the use of data of these persons for police purpose, but during these exchanges, confidentiality rules have to be followed.

Example - Data collected for tax purposes from a data subject can only be processed for law enforcement use by police () if the law allows it, if they are used for a legitimate aim and in a way that is necessary and proportionate to the aim pursued. In a concrete investigation of money laundering, the use of tax declarations' data of an individual can be envisaged to establish or deny a link between the individual and the money laundering operations.

4. Processing of special categories of data (sensitive data)[2]

Special categories of data, such as genetic data, personal data related to offences, criminal proceedings and convictions and related security measures, biometric data uniquely identifying a person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical nature, for instance additional security measures, and of an organisational nature, for instance having such sensitive data processed separately from the processing environment of the "ordinary" categories of data. Safeguards should be adjusted to each data processing operations taking into account their specificities and it is highly recommended to use multiple

[2] Paragraph removed from previous Point 8

Deleted: use
Deleted: applicable to the collection and the use of data.
Deleted: ¶ ¶
Deleted: by police (irrespective of the fact that the original processing has been carried out for a police purpose or for other purposes)
Deleted: ~~same~~
Deleted: Due to the nature of data processing, it is possible to use personal data collected for one purpose for another, personal data collected and retained for police purposes should not be kept and processed in an ...
Deleted: specific, well-defined
Deleted: point
Deleted: a
Deleted: for
Deleted: the
Deleted: tests
Deleted: .
Deleted: all data held by police shou ...
Deleted: Due to
Deleted: isz
Deleted: the
Deleted: nature of data processing ...
Deleted: in an unstructured manne ...
Deleted: however
Deleted: data, in particular in respe ...
Deleted: which shall include ...
Deleted: ,
Deleted: other
Deleted: This
Deleted: does
Deleted: if all legal requirements as ...
Deleted: .
Deleted: Biometric d
Deleted: taken
Deleted: immigration medical
Deleted: such as checks against ...
Deleted: allows
Deleted: it and appropriate ...
Deleted: Any such use should be ...
Deleted: The purpose of appropriat ...
Deleted: of
Deleted: its

levels of protection for those categories of data (e.g.: separate main-frames, shorter data retention periods, etc.). It is of paramount importance to prevent unauthorised or unwanted access to those categories of data even with additional security measures.

A careful balance of interests taking into account the purpose of the investigation, the context and the nature of the data is necessary to determine whether or not, and to which extent, the police could process sensitive data. For instance, it would be advisable to differentiate when biometric data is processed by the police whether it is for identification purposes (where for instance 2 fingerprints could suffice) or it is for crime investigation purposes (where more fingerprints could be needed).

The use of Data Protection Impact Assessments (DPIA) which is in general is to be carried out where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons can be recommended also in order to help to ensure that appropriate safeguards are put in place. The data controller should assess and demonstrate whether the purpose of the processing can be achieved in a manner that impacts less on the right to privacy and data protection and if the processing of special categories of data does not represent a risk of discrimination for the data subject.

Moreover, it should be recalled that the collection and processing of sensitive data in the context of profiling is prohibited (Principle 3.11 of Recommendation 2010 (13)[3] except if these data are necessary for and proportionate to the lawful and specific purposes of processing and as long as domestic law provides appropriate safeguards. In this context, besides measures detailed above, the use of PETs and more frequent checks on the lawfulness of the processing can be recommended. This could, for example, translate into measures put in place to counter the assumption that individuals belong to a criminal organisation because of where they live, where a criminal organisation is active or where the individuals have the same ethnic origin.

Example - Targeting groups or individuals based solely on religious beliefs would not be allowed. In an investigation into a group of individuals engaging in possible terrorist activities that were attached to a particular religious group, it could nevertheless be of importance to process data specific to the followers of this specific religious group (related to worshipping place, religious preachers, customs, teachings, members and structure of the religious community, etc. that was pertinent to the investigation).

5. Providing information to data subjects

One of the most important obligations of a data controller is to provide information on data processing to data subjects. This obligation is two-fold: it requires the data controller to provide *general information* to the public on the data processing that it carries out, and to give *specific* information to data subjects if no restrictions or derogations apply to the data processing.

Information provided to the wider public, should promote awareness, inform them of their rights and provide clear guidance on exercising their rights. The information provided should be effectively and broadly accessible. Moreover it should include details about the conditions under which exceptions apply to the data subject's rights and how they could submit an appeal to the DPA or to the judiciary.

Websites and other easily accessible media perform a role in informing the public. It is recommended to have in place letter templates on these websites or other media to help the data subjects exercise their rights. It is the responsibility of the data controller to provide information which adequately highlights data protection and data subjects' rights.

[3] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member stateson the protection of individuals with regard to automatic processing of personal data in the context of profiling (https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00)

Deleted: anonimisation,

Deleted: which takes

Deleted: can

Deleted: on the top of personal criminal data

Deleted: 8 to 10

Deleted: would

Deleted: A greater

Deleted:)

Deleted: is

Deleted: the

Deleted: adequately

Deleted: (i.e. tasks of the police)

Deleted: of the data subject

Deleted: Regarding these data the potential risk of negative discrimination or of adverse legal effect significantly affecting the data subject should be avoided as all profiling based on sensitive data which result in a negative discrimination are prohibited

Deleted: pseudo-anonymisation,

Deleted: legitimate

Deleted: (of these data

Deleted: can

Deleted: are from

Deleted: al

Deleted: There should be additional criteria to allow the processing of data on this ground.

Deleted: allowed. However, in

Deleted: However to target all ...

Deleted: It should be noted that t

Deleted: ;

Deleted: prior

Deleted: and *upon request* on the ...

Deleted: The *general obligation* ...

Deleted: The i

Deleted: in respect of broader ...

Deleted: in general

Deleted: regarding these files

Deleted: Information provided

Deleted: can

Deleted: against a decision of the ...

Deleted: as best practice

Deleted: in

Deleted: ing

Deleted: In respect of making ...

In order to comply with the second obligation of giving data subjects specific information regarding data processed, the police shall inform data subjects on the data processing envisaged before the processing or, if it is not possible, for objective reasons, shortly after it. This communication shall comprise information on the data processing, on the collection of the individuals' data and comprehensive information on their rights.

The obligation to provide specific information implies that, in principle, the data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.

The information should be provided unless a restriction or derogation applies as described in Point 7 taking into account the specific nature of sensitive files, such as criminal intelligence files, files containing sensitive data, in order to avoid serious prejudice to the performance of police functions or to the rights of individuals. Even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.

Very often data subjects, because of restrictions or derogations of their right to information, cannot receive complete information on the processing the police undertake with their data; this should not affect their exercise of the right of access.

Example - For the purpose of covert monitoring of a high risk sex offender, data processing and long-term data retention may be justified without informing the individuals under surveillance if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved, the data subject should be informed about the fact that she or he was subject to such measure.

6. Data subject's rights[4]

Accessing their personal data is a fundamental right for data subjects as it allows them to be aware of the processing on data related to them. Moreover, it can also be a prerequisite to enable the exercise of further rights, such as thethe right to information, the right of rectification and the right of erasure.

In case an individual has her/his data collected during the course of an investigation or other tasks of the police as described in Point 1, as soon as circumstances safely permit, the police [in principle] should inform the individual of the data processing if there is such request. Specific information should be given in clear and plain language upon request. The communication has to contain the same information as described in point 5, unless data subjects wish otherwise.

The law can provide, under the strict conditions described in Point 7, that the right to be informed upon request may also be limited or excluded, should the provision of such information prejudice the investigation, or another important police task, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified.

The police should aim to answer even general questions arising from data subjects on the processing activities in relation to their personal data, but can use standardised forms to facilitate communication.

Example: If a data subject asks the police on data it processes on them, the police, if no exception is applicable, should provide a detailed answer with legal references, but should do so in a plain language, avoiding uncommon or specialised expressions.

The right of access should, in principle, be free of charge.

[4] Paragraph removed from previous Point 17.

Deleted: According to the second obligation of giving data subjects specific information regarding their data processed by police *ex officio*, it responds to the general principle that an individual should always be in control of her/his data.

Deleted: this obligation

Deleted: it envisages undertaking

Deleted: before the processing

Deleted: undertook in relation to her/his data

Deleted: If there are objective obstacles for providing this communication to the data subject, it can be done shortly after data processing has started, but in time which allows data subjects to exercise effectively, if they so wish, effectively their rights as prescribed in Point 6. Police can however apply restrictions or derogations to this obligation if it is foreseen by nationaldomestic law legislation for the reasons described in Point 7.

Deleted: 7 taking

Deleted: of

Deleted: , etc

Deleted: police in performing theirits functions

Deleted: is

Deleted: t

Deleted: ing

Deleted: any more

Deleted: ¶

Deleted: a

Deleted: the

Deleted: in relation to their personal data. ¶
T

Deleted: on request, the right of access

Deleted: are interdependent rights.The right to access is a prerequisite for th ...

Deleted: ¶ ...

Deleted: The

Deleted: as soon as data are ...

Deleted: as

Deleted: providing

Deleted: , for instance

Deleted: Very often data subjects, ...

Deleted: P

Deleted: the

Deleted: using

It is possible to charge a reasonable administrative fee for the request, if national law permits and the request is manifestly unfounded or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such refusal.

To ensure a fair exercise of the right of access, the communication "in an intelligible form" applies to the content as well as to the form of a standardised digital communication. It is, however, advisable to refer to national legislation to ensure consistency and to avoid suspects utilising this method to find out whether there is an on-going investigation into them.

In respect of direct access, the data subject can request access to the controller of the files. The data controller will assess the request and any possible restriction or derogation which can only be used if it is vital for the performance of a specific police task as described in Point 1, or it is necessary for the protection of the data subject or the rights and freedoms of others, and reply directly to the data subject. In case of a restriction, partial information, and in case of derogation, information on the use of derogation, shall be still given, with the motivation for using such measures in both cases, as well as information concerning redress.

Example: The access request can be refused if there is an on-going investigation on the person, and providing the data subject access to the data could compromise such investigation.

If restriction or derogation were to be used, any answer should take into consideration, according to national law or practice, all circumstances to which the restriction or the derogation is applicable.

As a rule, domestic law should, ideally, provide for direct access. If the right of access provided for is indirect, the data subjects may direct their request to the supervisory authority, which after being properly mandated, will carry out the request on their behalf and conduct checks regarding the availability and lawfulness of the processing of the data subject's personal data. The supervisory authority will then reply to the data subject (providing what data it is possible to release, subject to any legally allowed restrictions or derogation). In case of a restriction or derogation, the same communication should be made possible as in case of a direct access.

The data controller should assess the request and reply to the data subject within a reasonable time limit, as provided for by domestic law.

There should be arrangements in place to confirm the identity of the data subject before access to any data is granted as well as to obtain information on the processing activities to which the request refers. The same holds if the data subjects delegate the authority to someone else to exercise their rights.

It is an essential right of the data subjects to be able to amend any incorrect data held on them. If the data subject finds data that are incorrect or irrelevant, she/he should have the right to challenge it and ensure that they are amended or deleted.

In some cases, it may be appropriate to add additional or corrective information to the file. It is important to underline that this right can only be exercised with due respect to other individuals' rights, for instance to the rights related to a testimony in a criminal case (which does not preclude per se the exercise of the data subjects' rights related to soft police data).

Data subjects can ask for the deletion of their personal data where such processing is unlawful.

If the data to be corrected or erased has been communicated elsewhere the relevant authorities should be informed of the changes to be made.

All proposed changes should be supported by evidence. If data subjects can prove by use of the official documentation that the data processed by police in respect to them are incorrect, the data controller shall not have the right of discretion whether to correct them.

It may be necessary for the police, as dealt with under Point 7, not to give information or grant the right of access, of deletion and of correction which might jeopardise an investigation and should therefore be

Deleted: a

Deleted: of approach

Deleted: of the police

Deleted: the

Deleted: s

Deleted: ,

Deleted: excessive

Deleted: of

excluded for its duration. Similar restrictions or derogation may be imposed by national law as described in Point 7.

Restrictions or derogations to the rights of data should only apply to the extent necessary and be interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis. Any decision to refuse a data subject's request should be provided in writing (including by electronic means). The response should provide clear justification of the decision making which can be verified by an independent authority or a court. It is possible that communicating the reasons for refusal could pose a risk to law enforcement or the data subject or to the rights and freedoms of others. If this is the case, it should be documented and provided to the independent authority or court to be verified, if required.

Example - If person A submitted a declaration against person B accusing her/him of committing a serious offence and later it emerges that the accusation was false, it might be relevant for the police to retain the false statement and the information surrounding it.

Although the statement was proven to be false, if the police needs to retain the data in the interest of the investigation for instance , a clear corrective statement on the file, instead of removing the false statement, would be necessary.

The data subject should be informed of all available options following a refusal decision such as an appeal either to the supervisory authority, to court or to another independent administrative authority.
Depending upon national legislation, specifically whether there is a direct or an indirect right of access, the actual communication of the result of the review or appeal may differ. In the case of indirect access the data subject should at least be informed that a verification of the police file has taken place. Alternatively, the supervisory body may request the police to release the data contained in the file to the data subject. The court or tribunal may have powers to enforce the access, correction or deletion of data from the file even in access-request cases referred to them by police or the supervisory authority.

If police sends a refusal letter it should contain the name, address, web address, etc. of all possible forafor redress.

The data subject should have access to a court or tribunal in order to submit an appeal, and have the reasons for refusal verified if they are not satisfied with the reply given by the supervisory authority or the independent authority. The supervisory authority should have sufficient powers to examine the police file concerned and have the assessment communicated.

7. Exceptions from the application of data protection principles

Exceptions can only be used for specific purposes foreseen by article 8 of European Convention on Human Rights and article 9 of Convention 108, if foreseen by law (the law should be public, open and transparent and, in addition, detailed enough) and if they constitute a necessary and proportionate measure in a democratic society.

The exceptions which have to be incorporated into national legislation should not be described in a general way, but should serve a well-defined purpose.Exceptions can be applicable to those principles described under Points 2,3, 5 as well as to the data subjects' rights (Point 6) in case of some specific purposes in relation to which data processing activities are undertaken. In particular they concern activities undertaken for the purpose of the protection of national security, defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest (which includes purposes in connection with the fulfilment of a state's international legal commitments or obligations, most prominently deriving from the binding decisions of United Nations' bodies, and humanitarian purposes) or the protection of the rights and fundamental freedoms of others.

Example - If giving information to a data subject may endanger the safety of a witness or an informant; this right can be limited in light of such circumstances.

Deleted: ¶
A data subject may be required, as per national legislation, to obtain a copy of their police file. However, to obtain a written copy or statement may not always be in their interest or feasible for the police and therefore in such cases domestic law may authorise oral communication of the contents.¶

Deleted: require retaining the data

Deleted: It is possible that the inspecting body cannot communicate the data to the individual even if there is no justification for refusing access.

Deleted: this

Deleted: inspecting body

Deleted: Example: If police sends a refusal letter it should contain the name, address, web address, etc. of all possible forum for redress.¶

Deleted: ¶

Deleted: Under the European Convention on Human Rights and Convention 108, e

Deleted: should be

Deleted: exceptions

Deleted: and have to be incorporated into national legislation in a manner compatible with the ECtHR jurisprudence

Deleted: ¶
¶

Deleted: p

Deleted: 4

Deleted: 7

Deleted: p

Deleted: 17

Deleted: it

Deleted: affects

Deleted: s

Deleted: those

Deleted: from international

Deleted: obligations

Deleted: ,

Deleted: Other applicable exceptions are foreseen in Article 3 Convention 108.

If the exception, as defined by national law providing specific safeguards is used by the police, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. The aim of using exceptions by the police should be limited to cases where the use of those rules and principles would endanger tasks of the police described under Point 1.

Example: If data collected for police purpose in an investigation are likely to serve national security purposes they can also be used to this latter purposes to the extent set forth by national legislation. If specific intelligence proves that money laundering operations have been carried out to finance terrorist operations, data collected on individuals during the investigations on money laundering can be used for the purpose of eliminating the close and imminent terrorist risk.

8. Use of special investigative techniques

The police should always adopt the least intrusive means of data processing during its operations. If less intrusive methods can be realistically used to achieve the desired ends, they should be preferred. The use of special investigative techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods.

With increasingly sophisticated technological developments, electronic surveillance has become easier, however, the use of these techniques interferes with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the high potential of severe interference with the right to privacy has to be balanced with cost-effectiveness, use of resources and the efficiency of investigations.

Example: In an investigation, the evidence for communication between two suspects can be gathered in various ways. If, by the use of interrogations, testimonies, the obtaining of call data, the same result can be achieved without jeopardising the effectiveness of the investigation, it is to be preferred to the use of more intrusive surveillance measures, such as wiretapping.

9. Introduction of new data processing technologies

If the introduction of new technologies is likely to result in a high risk to the individual's rights, the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. The introduction of new data processing technologies is considered to be subject to a DPIA as probability of risks to the individual's rights is usually high. It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity. The relevance of the DPIA shall be checked at reasonable intervals.

It is also of great importance, that in terms of data security and safety of communications, the highest standard is taken into account when introducing such technologies.

Example - New data mining techniques may offer extended possibilities for identification of possible suspects and should be assessed carefully for their compliance with existing data protection law, together with assessment of the risks it may represent to individual's rights and suggestions for the adoption of safeguards to ensure the protection of data, including with regard to data security.

The data protection authority has an important role in advising which risks are involved for data protection and which safeguards should be provided to ensure that any technical means comply with data protection law. However, the police do not have an obligation to turn in every case to the supervisory authority where it introduces new technologies. It may do so if the DPIA it previously conducted demonstrates a significantly persisting high risk to the individual's rights notwithstanding the adoption of specific safeguards.

Deleted: ¶

Deleted: ,

Deleted: based on

Deleted: the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police

Deleted: ¶

Example - If giving information to a data subject may endanger the safety of a witness or an informant; this right can be limited in light of such circumstances. ¶

¶

Example: Police data, if explicitly provided for by national law can be shared in compliance with stringent conditions set forth by the national law with national security agencies in respect of national security, for example to prevent investigate in a case of a recent terrorist attack. In order to rapidly identify the perpetrator of a terrorist act, police shall can envisage an urgent and extraordinary cooperation e actively and following a special procedure which takes into account the imminent risk of other individual's life and physical safety and security and share personal data stored on identified suspects with national ...

Deleted: ¶ ...

Comment [A3]: Sometimes, the less intrusive methods are not excluded in ...

Deleted: ¶

Deleted: it must be remembered that

Deleted: can

Comment [A4]: these are legitimate considerations since they impact police ...

Deleted: those considerations

Deleted: have

Deleted: cost-effectiveness, use of resources and

Deleted: or discreet surveillance

Deleted: covert

Deleted: Use

Deleted: It is advisable when new technical means for data processing ...

Deleted: processing

Deleted: continuous (i.e.

Deleted:)

Deleted: should

Deleted: every

Deleted: by

Deleted: or the national legislation does not provide sufficient clarity on ...

The consultation between the supervisory authority and the data controller should provide the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.

Appropriate details should be provided to the supervisory authority, in particular regarding the type of file, the data controller, data processor, the legal basis and the purpose of the data processing, the type of data being processed and by whom the data is being accessed, as well as information on retention of data, log policy and access policy, and other relevant technical aspects of implementation.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data could be reported to or made available for consultation to the data protection authority.

Following consultation, the data controller should consider carefully to implement any necessary measures and safeguards that have been recommended by the data protection authority.

Example - Introducing an automatic facial recognition system or other system based on the automated processing of biometric data would be very likely to need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed and recommended by the data protection authority after being consulted on the issue, specific safeguards should be put in place (concerning the data retention time, the cross matching functionalities, the place of the storage of data and the access to data issues, etc.) to comply with data protection principles and provisions

Use of the Internet of Things (IoT) technology in police work

Data sent to and from police during operational activity via the internet are good examples of the IoT already in use. Due to potential security vulnerabilities, IoT requires measures such as data authentication, access control to ensure data security and resilience to (cyber) attacks.

Example: In light of their potential security vulnerabilities, smart glass used by police should not be directly connected to a national criminal record data base and data collected should be guaranteed a high level of security.

Big data analytics in the police

Technological advances in processing and analysing large and complex data sets leading to big data and big data analytics present opportunities and challenges to the police, who is turning to digital sources and profiling techniques to perform their tasks.

Big data technologies enable bulk collection and analysis of a vast quantity of data generated by electronic communications and devices aggregated with other bulk data. This could interfere with the right to privacy and data protection.

The Council of Europe's Recommendation CM/Rec(2010)13[5] on the protection of individuals with regard to automatic processing of personal data in the context of profiling and the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[6] can be of use in the context of Big Data analysis for police use too.

Big data technologies and analysis techniques may help assist detecting crime, but there are, however, considerable risks to this type of data processing that should be taken into account:

Deleted: be defined in a way that

Deleted: s

Deleted: During the process with the supervisory authority the focus should be on mitigating the specific negative impacts that the data processing would represent to the right to privacy and to data protection.¶
¶
The consultation between the supervisory authority and the data controller should be defined in a way that provides the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.¶
¶
During the consultation process appropriate

Deleted: contained

Deleted: important

Deleted: are to

Deleted: Data protection authority is preferably to be consulted during the legislative procedure.

Deleted: which is directly linked to relevant databases

Deleted: ; they should gather information which is to be downloaded to a secure IT environment for further analysis

Deleted: *and profiling*

Deleted: are

Deleted: legal

Deleted: way of processing data

Deleted: potentially and inadvertently

Deleted: ¶

[5] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[6] Document T-PD(2017)1 - Big Data Guidelines

- Databases originating from one domain can be used in another domain and for another purpose, which changes the context and may lead to inaccurate conclusions and lack of valid legal basis, therefore to unlawful data processing with possibly serious consequences for the individuals involved.
- Profiling may lead to drawing discriminatory conclusions, which can result in the reinforcement of stereotypes, stigmatisation and discrimination.
- The increasing amount of personal data held in databases may lead to severe vulnerabilities and subsequent risk of data breaches if information security is not guaranteed.

Where big data relies on personal data, data controllers should pay additional attention to the following requirements:

- Verification of data accuracy, context and relevance of the data.
- Its use requires a high level of accountability.
- Its use shall be combined with methods of investigation which complement the conclusions drawn from the big data analysis. A decision affecting a person shall not be taken solely on automated processing of personal data.
- As for other types of data processing, it is of paramount importance that its use shall be ~~shall be be~~ necessary and proportionate for the fulfilment of police tasks described in Point 1, with special attention for the data processed to be adequate, relevant and non-excessive in relation to the purpose for which they are processed.
- Predictive analysis requires human intervention to assess the relevance of the analysis and conclusions.
- Ethical guidelines developed at national or at international level should be taken into consideration.
- As a principle and subject to restrictions and derogations mentioned in Point 7, transparency should be ensured by the data controller by explaining how the data are processed in accordance with privacy and data protection principles. If data collected for one purpose is used for another purpose, the data controller should in principle make the data subjects aware of this subsequent use.
- Even if complex methods are used, the lawfulness of the processing – including subsequent use of data - and compliance with the conditions set by Article 8 ECHR and Convention 108 should be demonstrated.
- An information security policy should be in place and implemented throughout the processing.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals and the administrative and judicial means exist for individuals to challenge those decisions. This implies data subjects' awareness of the reasoning of the algorythm used and the purposes for which it was used.

The above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones, are even more necessary when sensitive data are processed in Big Data analytics.

10. Storage of data

"As pointed out in Point 2" data shall be processed until they have served the purpose for which they were collected. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

There should be a clear distinction in how the police stores and processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses. This should also relate to the specific purpose for which the data was collected. Additional safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence. Clear rules have to be established in relation to the handling of different data bases with special attention to the analysis of multiple results.

The principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve the purpose of the prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where personal data is processed for the purpose of the maintenance of public order.

Deleted: take
Deleted: due account of
Deleted: traditional less intrusive other
Deleted: to
Deleted: such
Deleted: ized
Deleted: l
Deleted: use
Deleted:
Deleted: purpose
Deleted: notably
Deleted: Where possible
Deleted: provided
Deleted: compatible
Deleted: secondary
Deleted: and/or lengthy processing are undertaken L
Deleted: be
Deleted: allow the data subjects to know the
Deleted: ensure transparency
Deleted: h
Deleted: for to avoid any negative discriminatory action
Deleted: If data are no longer relevant for the purpose collected, they should be deleted, unless subsequent processing is possible on the grounds put forward in Point 3. S
Deleted: s
Deleted: S
Deleted: queries in

The grounds for retention and processing should be reviewed periodically. The unlawful processing of personal data outside of the legal framework allowed for the retention constitutes a severe violation of the right to protection of personal data. If the law in relation with a specific crime provides for a data retention period of 4 years and if personal data are processed in relation with this crime by the police solely on this ground after 4 years have passed since the collection of the data in question and no other legal ground to process this data exists, the retention of this data could be considered as unlawful.

General data retention periods are usually regulated in national or international law. In order to comply with the legislation while ensuring the effectiveness and the success of an investigation police bodies are strongly advised to develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data.

For example, in a case where the law prescribes a 4 year data retention period but the individual subject to an investigation is acquitted from all charges by the court after 2 years, her/his data shall be deleted (if the individual is not a recidivist or there is no information on her/him committing again the same category of crime) from the database, provided that all deadlines for the review of the case have expired. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judicial procedure terminates completely (which means all redress have been made or all deadline for redress have been passed).

The police should provide systems and mechanisms to ensure that the data that are stored are accurate and that their integrity is maintained.

International obligations, which include providing data to international bodies such as Europol, Eurojust and INTERPOL, bilateral agreements and mutual legal assistance between member states and third countries must be observed when shaping internal policies.

Data should be categorised according to the degree of accuracy and reliability in order to assist the police in their activities. It is recommended that handling codes are used to distinguish these categories. A classification system facilitates the assessment of the quality of the data and how reliable it is. Classification of data is also important when it is to be communicated to other police bodies or states.

Example - Information collected directly from a person's statement will be assessed differently than information collected from a person's hearsay statement. Data based on facts, or 'hard' data, will be assessed differently than data based on opinions or personal assessments, or 'soft' data.

Personal data collected by police for administrative purposes must be kept (as far as possible: logically and physically) separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by law.

Examples of administrative data include lists of data on licence holders or data on human resources and firearms certificates.

11. Communication of data within the police sector

A distinction should be made between domestic communication of data and international transfer of data. Within these two distinct operations different requirements apply, depending upon who is receiving the data, whether it is the police, another public body or a private party. The police can only communicate personal data within the police sector if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

Deleted: can

Deleted: and evidence gathered in this way can be seen as unlawful

Deleted: an individual is retained kept in custody

Deleted: , 4 years later the evidence based solely on

Deleted:

Deleted: and the measures undertaken by the police based solely on this data

Deleted: possibly

Deleted: by the court

Deleted:

Deleted: revision

Deleted: also

Deleted: the

Deleted: of the data

Deleted: When shaping internal policies i

Deleted: This uses a

Deleted: to

Deleted: if feasible

Deleted: the

Deleted: ent

Deleted: As a general rule p

There should be clear and transparent rules on how the police grant access to data held by it and on which grounds.

The police, domestically, should only share information (among police) when there is a legal basis for the request, e.g. an on-going criminal investigation or a shared law enforcement task and laws or agreements allowing the communication

The police can share data with other police organisations if the personal data are relevant for the purpose of prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where they are processed for the purpose of the maintenance of public order.

The communication of personal data in general should be in line with the general considerations described above.

Example: A police unit can share data on a suspect who presumably committed a tax fraud with another police unit investigating a murder case if there is indication that the suspect for this crime could be the same person or if doing so will materially assist the investigation.

12. Communication of data by the police to other public bodies

The communication of data outside police is permissible if it is provided for by law and the data are required by the recipient to enable them to fulfil their lawful task. Mutual assistance agreements foreseen by the law between law enforcement and public bodies allows the public bodies to have access to law enforcement data which would be essential in the fulfilment of their duties and tasks (for example in their investigations or other legal duties in accordance with national law).

Stricter principles than those set forth in Point 11 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the processing of personal data, which are considered sensitive, could result in adverse effects for the individual.

Communication of data to any other public authority may also be allowed if it is foreseen by law, is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to other persons or to public order or to public security.

The communicated data may only be used by the receiving body for the purposes for which the data were transferred.

Example - A claim for a residence permit made by a migrant. Police data may be required to verify if the person was ever involved in criminal activity. It would be in the interest of the Immigration Office and the claimant for this communication of data to take place.

13. Communication of data by the police to private parties

There may be occasions when, under strict conditions, the police can communicate data to private bodies. This communication has to be based in law and can only be done by the authority which is processing the data. Such communication can only be done for the purpose of the investigation or other important police tasks as described in Point 1, in the interest of the data subject, for humanitarian reasons or if it is necessary to prevent serious and imminent risk to public order or public security. For example, there might also be instances where police data may be communicated to humanitarian organisations based on international law, in the interest of the data subject or for humanitarian reasons.

Where the police shares data with media in respect of making information related to an investigation public, special consideration should be given to the assessment to determine that it is necessary and in the public interest that such publicity is allowed.

Deleted: that

Deleted: is

Deleted: personal data

Deleted: is

Deleted: subject to the principle of necessity and proportionality and has to serve the above mentioned purposes

Deleted: G

Deleted: is

Deleted: m

Deleted: 0

Deleted: criminal

Deleted: the communicated data

Deleted: be used for non-law enforcement purposes

Deleted: negative discrimination

Deleted: against

Deleted: In practice detailed ¶ ¶ As an exception, c

Deleted: as

Deleted: missions

Such communication should only be on a case by case basis and in each case there must be a clear legal basis providing the necessary procedure (e.g. need for specific authorisation) to be followed for any such communication to occur.

Example - When the police communicate with the financial sector in relation to known fraud or theft offenders, when it communicates with an airline about stolen or lost travel documents or when the police releases details of wanted persons believed to pose a risk to the general public.

14. International transfer

Any transfer of police data internationally should be limited to police bodies and should be fit for purpose and in accordance with the law. For this, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data handling, regional legal frameworks such as EU and EU institutions' legislation (on Europol, Eurojust, Frontex, etc.) and subsequent agreements (operational bilateral agreements), bilateral treaties and in general, international agreements on mutual assistance, or other bilateral or multilateral agreements made regarding effective cooperation can be of use.

When considering sharing any data, consideration should be given as to whether the receiving authority is performing a function conferred to it in law related to the prevention, investigation, or prosecution of criminal offences, the execution of criminal penalties and the maintenance of public order, and whether the sharing of the data is necessary to perform its specific task.

The sending authority should ascertain that there is an appropriate level of data protection in the receiving state and that the receiving state complies with the relevant rules of international transfers of personal data. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. This means of transfer should be used as a last resort option. International transfers framework such as "INTERPOL's Rule on the Processing of Data" and its "Statute of the Commission for the Control of INTERPOL's files" Rules on the Control of Information and access to INTERPOL's Files", the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185) may be taken into account[7] so as to ensure that any transfer of data is legally justified and has appropriate safeguards in place. The request should clearly state all the necessary elements from the requesting party to enable the receiving party to make a sound decision on the request. These details would be expected to include the reason for the request as well as the purpose for the transfer of data.

An appropriate level of data protection should be guaranteed (e.g. through ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments) if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

If there are conditions applied by the sending authority in relation to the use of the data in the receiving state these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout its lifecycle.

Example - Further transfer of data should only be allowed if this is necessary for the same police purpose as the original transfer and the second recipient is also a police body ensuring an appropriate level of data protection. The police body which originally sent the data must also consent to the onward transfer. If the police from country X sends personal data to the police of country Y it is only permissible for the country Y to transfer this data if above all requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) if country X consents to the transfer. If the data is sent to country Z which is a non-

Deleted: which should
Deleted: e
Deleted: they
Deleted: wanted who are
Deleted: organisations
Deleted: contained within its legal framework
Deleted: ,
Deleted: in respect
Deleted: Interpol's "Rules Governing the Processing of Data
Deleted: can be applicable
Deleted: in place
Deleted: to
Deleted: its
Deleted: onward
Deleted: specific
Deleted: with

[7] This is without prejudice to the right of the Committee of Convention 108 and other instances disposing such power to assess and to review if necessary the level of data protection guaranteed by those multilateral agreements

member of the Convention 108, then country Y should ascertain that this country provides an appropriate level of protection of personal data and effective means of exercise of the related data subject rights.

The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases if it is required for the performance of the task of the transferring authority and there is no effective means of transferring the data to a police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers.

Example: If tax authorities in country X requests the police in country Y about the whereabouts of a person involved in non-criminal tax evasion because they have evidence that the person is involved in criminal matters in country X, the police can transfer the personal data of the individual.

The international transfer of personal data between police and private bodies in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police as described in Point 1, provided by legal means and where the emergency, the gravity of the crime, its trans-border nature and where the involvement of the police would not be possible for objective reasons. Other facts as data security, the reassurance received as to the use of the data and the lawfulness of the data transfer in the receiving country have to be taken into account. In this context it is to be noted that in such a case, the data controller has a double obligation with respect to the protection of personal data: one imposed by the legal framework of the country where it resides and the one which is related to the data transfer. The local police should be informed afterwards. The police are required, wherever possible, to make use of existing international legal instruments, in respect of this type of data transfer. International transfers may also exceptionally occur where the police communicates personal data for humanitarian purposes.

Example: In an investigation, carried out within the framework of an international multilateral agreement, into child sexual exploitation where the victim is in country Y and the police there have commenced an investigation, and the material has been made available on the internet by the suspect residing in another (country X) and there is a high risk that the suspect seeks to avoid justice by fleeing country X, the police in country Y can request, on an exceptional basis, that a service provider in country X provide the whereabouts of its customer. However, the police of country Y should inform the police in country X of its operation as soon as is possible and then seek to resolve the matter in cooperation.

15. Conditions for communications

Since there is a general obligation for the data controller to ensure a high level of data quality, it is advisable to have in place an additional check before sharing the data with others. When communicating or transferring data, it is always advisable to double-check the quality of data, if it is correct, up-to-date and complete. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated. It is required to establish secure channels of communication which ensure data security at the highest level possible. The quality of data can be assessed up to the moment of communication.

Example: If personal data that contain incorrect data (personal or otherwise) are sent they could adversely affect the investigation, cause harm to the individual concerned or others involved, or who may become involved as a result of the incorrect data being transferred. This can, as a result, leave the police in the transmitting and receiving states open to civil redress. In essence, if an individual is arrested based on a wrong communication of the suspect's name, it seriously harms several human rights of the individual concerned and can undermine any criminal investigation.

16. Safeguards for communication

It is of utmost importance that the necessity and purpose limitation principle should be applicable for any domestic communication or international transfer of personal data outside of police organisations.

Deleted: has, in place, appropriate legal protection in terms of personal data processing and can guarantee an

Deleted: level for the

Deleted: it has

Deleted: police

Deleted: to

Deleted: a

Deleted: y

Deleted: residing

Deleted: the

Deleted: the fact that

Deleted: the involvement of the local police would compromise the purpose of the investigation because of the length of the procedure

Deleted: As

Deleted: or transferring

Deleted: ,

Deleted: and data based on opinions or personal assessments cheked at source before being communicated and their degree of accuracy or reliability indicated

Deleted: seems

Deleted: to be preferable

Deleted: transfers

Deleted: is sent

Deleted: s

Deleted: it can

Deleted: the

Any data communicated should not be used for anything other than the purpose for which it was sent or received. The exceptions to this are when the sending authority, based on legal provisions, gives agreement to any further use, , and if it is necessary and vital for the recipient to fulfil their task. Data can also be communicated if it is in the interest of the data subject for humanitarian reasons, is necessary to prevent serious and imminent risk to public order or public security or an appropriate level of data protection is guaranteed by the recipient by international, national legal instrument, ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments, as foreseen by Convention 108.

Example: Personal data sent by the police of country X to the police of country Y in a money laundering case cannot be used by the police as profiling on the given individual in respect of her/his religious beliefs or political activities (unless those are relevant to the crime committed and police in country X has given its consent for this use).

17. Interconnection of files and on-line access to files

In specific circumstances the police may seek to collect data by coordinating its information with other data controllers and processors. Furthermore, it may combine personal data stored in different files or in different databases that are held for different purposes, such as those held by other public bodies and/or private organisations. This may be in relation to an on-going criminal investigation or to identify thematic trends in relation to a certain type of crime.

In order for these actions to be legitimate they must be authorised or be underpinned by a legal obligation to comply with the purpose limitation principle.

If the relevant police body has direct access to files of other police or non-police bodies, it must only access and use the data if domestic law, which should reflect the key data protection principles, so permits.

Clear legislation and guidance, which adheres to the data protection principles, should exist for cross-referencing of databases. Such cross referencing should be necessary, purpose bound and proportionate. With relation to personal data stored in other data controllers' or processors' data base all conditions described in Point 2 have to be fulfilled and regularly checked.

Example - Data held for citizenship purposes can only be used in an investigation if the national legislation allows it and to the extent to which it is necessary for the purpose of the investigation to do so. For instance, the number of children a suspect has may not be relevant in an investigation, and should therefore not be processed by police. Access in this case to a database can be perfectly lawful but it can only be legitimate if it respects the principles of data protection.

18. Data security

The police must take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The controller must notify, without delay, at least, the competent supervisory authority of those data breaches which according to its assessment may seriously interfere with the rights and fundamental freedoms of data subjects. The information of data subjects of data breaches which may seriously interfere with their rights may also have to be ensured without undue delay, unless it jeopardises the task of the police.

Information security is essential to data protection. It is a set of procedures to ensure the integrity, availability and confidentiality of all forms of information within the police organisation, with the aim of providing security of data and information, and limiting the impact of security incidents and data breaches to a predetermined level.

Deleted: only
Deleted: is
Deleted: and if the processing is based on law,
Deleted:
Deleted: safely
Deleted: ,
Deleted: or
Deleted: or
Deleted: and
Deleted: as well
Deleted: crime
Deleted: have
Deleted: they
Deleted: in
Deleted: accordance with
Deleted: permits legislation
Deleted: ,
Deleted: of
Deleted: therefore
Deleted: any
Deleted: affect
Deleted: them
Deleted: shall also
Deleted: ing
Deleted: ¶
Deleted: ,

The level of protection given to a database and/or an information system or network is determined by a risk assessment. The more sensitive the data are, the greater protection is required.

Authorisation and authentication mechanisms are essential to protect the data, and sensitive information should always be encrypted. It is considered best practice to have in place an audit regime to regularly check that the level of security is appropriate.

Police authorities are advised, where necessary, to conduct DPIA (see Point 4) to assess the privacy risks to individuals in respect of the collection, use and any disclosure of information. This will help to identify risks and develop solutions to ensure that concerns are addressed appropriately. Any such impact assessment should cover relevant systems and processes of processing operations, but not individual cases.

A Data Protection Officer (DPO) within the police can play an essential role in carrying out internal audits and assessing the legitimacy of the processing, which contributes to a higher level of data protection and data security within the organisation. Moreover, the DPO can facilitate the dialogue between the organisation and the data subjects, as well as the organisation and the supervisory authority which can add to the overall transparency of the police body.

An Identity & Access Management System (IAM) may be recommended to manage employees and third party access to information. This will require authentication and authorisation to access the system and set privilege rights to determine what can be viewed. IAM can be seen as a useful requirement to ensure safe and appropriate access to data.

The data controller, following an evaluation of the risks, should at implement measures in respect of:

- equipment access control,
- data media control,
- storage control,
- user control,
- data access control,
- communication control,
- input control,
- transport control,
- recovery and system integrity,
- reliability and integrity.

Privacy-by-Design

The concept of privacy-by-design is an integral part of data security. Data protection and security may be embedded directly into information systems and processes, using technical and organisational measures, to ensure a high level of data protection and security and, in particular, to minimise the likelihood of data breaches. This approach is known as Privacy–by–Design, promoting privacy and data protection compliance from the start. It can be achieved through software and/or hardware. It requires a threat analysis, a full life cycle approach and rigorous testing.

Data controllers should ensure that privacy and data protection is a key consideration in the early stages of any project and then through its life cycle. Specifically, when building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have privacy implications and embarking on an information sharing initiative using data for new purposes.

Privacy-by-Design requires the implementation of Privacy Enhancing Technologies (PETs) to enable a better protection of personal data. PETs prevent unnecessary processing of personal data, without losing functionality in the information system itself.

Deleted: …

Deleted: P

Deleted:

Deleted: *Privacy-Enhancing Technologies (PETs)* ¶

Deleted: This is the common name for a range of different technologies to protect sensitive personal data within information systems.

Deleted: users to

Deleted: their

Deleted: The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.¶

Example: Body scanners used for police purposes have to be designed to respect the privacy of the individuals being inspected while fulfilling the purpose of their use. Therefore the body image in such tools has to be blurred by default.

19. External control

There has to be, at least, one supervisory authority responsible for ensuring compliance of data processing to the international and national legislation within the law enforcement sector.

Certain states may require more than one supervisory authority, for instance a national or federal authority and a number of decentralised or regional authorities, whilst others will prefer to have a single supervisory authority, responsible for the entirety of the supervision of data processing operations.

The supervisory body should be completely independent, meaning that it does not belong to the law enforcement organisation, nor is it directed by another body whithin the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties and should not be instructed or forced to accept instructions from anybody. The personal independence of its chair/president including political, financial, functional and operational independence, are decisive factors when judging how independent the supervisory body is.

Deleted: organisation

Deleted:

National law should provide for advisory, investigative and enforcement powers to enable it to investigate complaints, to have regulatory measures or to be able to impose sanctions where needed. The legal and administrative tools at its disposal shall be efficient and enforceable.

Supervisory authorities should have the ability to cooperate in law enforcement matters bilaterally and also via the Committee of Convention 108.

Example: The supervisory authority must be independent and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

a. “personal data” means any information relating to an identified or identifiable individual (“data subject”);

b. “genetic data” are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

c. “biometric data” are data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual;

d. “soft data” (evidence based on testimony or other personal assessment) means data acquired through testimony of person involved in the investigation;

e. “hard data “ (evidence based on documents or proven facts) means data acquired from official documents or other certified sources;

f. “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

g. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

h. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

i. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

j. Internet of Things (IoT): is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

k. “covert surveillance” means all measures aiming at monitoring discreetly the movements of persons, vehicles and containers, particularly those involved in organised or cross-border crime.

l. “special investigative techniques” techniques applied by the competent authorities in the context of criminal investigation for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person.

m. “privacy-enhancing technologies” (PETs) means a range of different technologies to protect personal data within information systems. The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.

Deleted: g. “competent authority” means: public or private entity authorised by law having a competence in the prevention, investigation and prosecution of criminal offences and to the execution of criminal penalties;¶

Deleted: h

Deleted: i

Deleted: j

Deleted: k

Deleted: l

Deleted: m

COMMITTEE OF EXPERTS ON TERRORISM/COMITE D'EXPERT SUR LE TERRORISM

1. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "T-PD") prepared a "Draft practical guide on the use of personal data in the police sector" (hereinafter "the Draft practical guide") "to highlight the most important issues that may arise in the use of personal data in the police sector and to point out the key elements to be considered in that context".

2. The T-PD will discuss the "Draft practical guide on the use of personal data in the police sector" in view of adoption at its forthcoming 35th Plenary Meeting (Strasbourg, 22-24 November 2017).

3. The T-PD Secretariat presented a revised version of the "Draft practical guide" to the Secretariat of the European Committee on Crime Problems (CDPC) and the Committee of Experts on Terrorism (CODEXTER) asking for comments on the draft from the two Steering Committees by 13 November 2017.

4. Replying to this request of the T-PD, at its 10th meeting (19-20 October 2017), the Bureau of the CODEXTER examined the text [and approved the present opinion, which was finally adopted by the CODEXTER following the written procedure]:

5. The CODEXTER welcomes the attention given to the important issues of collection and use of personal data for law enforcement purposes by the T-PD. It also agrees on the need to guarantee that any interference with the rights provided for by Article 8 of the European Convention on Human Rights and by Convention 108 shall "comply with the necessity, proportionality and purpose limitation principles".

6. However, the CODEXTER notes that the lawful collection and use of personal data for law enforcement purposes are crucial in the interests of national security and for the prevention of disorder or crime (on secret surveillance and its implications, see paragraph 48, *Klass and Others v. Germany*, (Application no. 5029/71), 6 September 1978; on collection of personal data, see *Uzun v. Germany*, (Application no. 35623/05), 2 September 2010). These police practices are, when conducted lawfully, to the advantage of democratic societies. This aspect could be further addressed in the text so as to strengthen the fundamental approach of the Council of Europe, that the prevention and suppression of crime, including through the collection and use of personal data for law enforcement purposes should and can be efficiently conducted in complete compliance with the law.

7. The CODEXTER further notes that the text devotes a short paragraph to the "use of special investigation techniques" which reads:

   "The police should always adopt the least intrusive means of data processing during its operations. If less intrusive methods can be used to achieve the desired ends, they should be preferred. The use of special investigative techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods.
   With increasingly sophisticated technological developments, electronic surveillance has become easier, however, the use of these techniques interferes with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the high potential of severe interference with the right to privacy has to be balanced with the efficiency of investigations.
   Example: In an investigation, the evidence for communication between two suspects can be gathered in various ways. If, by the use of interrogations, testimonies, the obtaining of call data, the same result can be achieved without jeopardising the effectiveness of the investigation, it is to be preferred to the use of more intrusive surveillance measures, such as wiretapping."

8. The CODEXTER finds that the reference to the use of special investigation techniques in the text is pertinent and adequately highlights some of the challenges faced by the police having recourse to these techniques.

9. In this connection, it wishes to draw the T-PD's attention to Recommendation CM/Rec(2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism, adopted on 5 July 2017.

10. In particular, with regards to data processing, the CODEXTER shares the approach of the revised draft where it underlines the importance of preferring the least intrusive means. In this context, the T-PD could consider referring to Chapter II of Rec(2017)6, focusing on the "Use of special investigation techniques at national level". Indeed, it is established in paragraphs 7-10 that:
"Special investigation techniques should only be used where there is sufficient reason to believe that a serious crime has been committed or prepared, or is being prepared, by one or more particular persons or an as-yet-unidentified individual or group of individuals. Member States should ensure proportionality between the special investigation techniques used and the legitimate aims pursued. In this respect, when deciding on their use, an evaluation in the light of the seriousness of the offence and the intrusive nature of the specific special investigation technique used should be made. Also the urgency and general complexity of the case could be considered. Member States should ensure that competent authorities apply less intrusive investigation methods than special investigation techniques if such methods enable the offence to be prevented, detected, investigated, prosecuted and supressed with adequate effectiveness. Member States should take appropriate legislative measures to permit the production of evidence gained from the lawful use of special investigation techniques before courts. Procedural rules governing the production and admissibility of such evidence shall safeguard the rights of the accused to a fair trial."

11. Finally, the CODEXTER is of the opinion that the wording "the seriousness of the offence to be prevented or investigated and" should be included in the end of the paragraph on the "use of special investigation technique", which should therefore read: *"With increasingly sophisticated technological developments, electronic surveillance has become easier, however, the use of these techniques interferes with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the high potential of severe interference with the right to privacy has to be balanced with the seriousness of the offence to be prevented or investigated and the efficiency of investigations."*

****

CONFERENCE OF INGOs/CONFERENCE DES OING (CDMSI)

- Critères pour l'hébergement des données : localisation (quel territoire), certification des prestataires, critères de disponibilité (pour que les personnes concernées conservent à tout moment leur droit d'accès et de rectification);

- Habilitation des personnes effectuant des traitement sur les données à caractère personnel: idéalement autorisation express par le responsable du traitement des personnes manipulant les données (quel agent effectue quel traitement et dans quel but, cet agent doit être formellement autorisé et accuser réception de cette autorisation).

- Puisqu'il s'agit d'un guide opérationnel, encourager le recours à la pseudonymisation dès que cela est possible.

EUROPEAN COMMISSION / COMMISSION EUROPEENNE

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied to ensure the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").
Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed application and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[8] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level.
The present Guide was therefore preparedto highlight the most important issues that may arise in the use of personal data in the police sector and to pointout the key elements to be considered in that context.
This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance.
The overarching principles set out in Recommendation (87)15 and their practical implications aim to ensure that the processing of personal data by the police is carried out in full respect of the rights of the individual to privacy and data protection.
To facilitate the reading of the Guide, a glossary of the terms used is provided at the end of the document.

General considerations

The collection and use of personal data for law enforcement purposes constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and, as such, it *must* be based on law (clear, foreseeable and accessible), pursue a legitimate aim and be limited to what is necessary and proportionate to achieve that legitimate aim. (Former second paragraph moved upfront)

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data processing within the police should be based on predefined, clear and legitimate purposes set in the law; it should be necessary and proportionate to these legitimate purposes and should not be processed in a way incompatible with those purposes Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible.

1. Scope

The principles explained in the present guide apply to the processing of personal data for police purposes, for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (hereafter referred to as "tasks of the police", ["police purposes"]). Where 'police' is used in the text, it can be taken to mean wider law enforcement authorities, and/or other public and/or private bodies authorised by law to process personal data for the same purposes.

[8] See Report "Twenty–five years down the line" – by Joseph A. Cannataci

2. Collection of data and use of data

The police as data controller is responsible for all data processing it undertakes and is accountable for its data processing operations.

The collection of personal data for police purposes should be limited to what is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

It is understood from Point 2.1 of the Recommendation that inforthe fulfilment of both of the main police tasks (prevention of a real danger and the suppression of a specific criminal offence), an evident and direct correlation should exist between the data processing carried out by the police and a situation where individuals have already committed or are likely to commit a crime.

The police should always choose the adequate legal basis to process personal data and should process personal data in a legitimate way. A careful assessment should be carried out by police to make sure that the processing is based on an appropriate legislation and the procedures for data processing foreseen by it are fully respected.

The police should apply at all stages of the processing the relevant data protection principles (most importantly the principles of necessity, proportionality and purpose-bound data processing) and should not continue to process data which are not needed for the purposes. In this context, personal data collected at an early phase of the investigation, which then proves with the process of the investigation to be no longer relevant should no longer be processed (e.g. innocence of a suspect is confirmed), and should therefore either be blocked or deleted. This does not apply where subsequent use of the data is allowed (point 3).

Prior to and during the collection of such data, the question of whether the personal data collected is necessary for the investigation or for a task of the police as described in Point 1, should always be considered. One should note that once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific task of the police) should exist. This link together with compliance to the data protection principles as described in the Guide, must be demonstrable at all times. After the collection phase and at different stages of the investigation, a thorough analysis is needed to assess which data are to be retained and which are to be deleted.

Before collecting any personal data, investigators should ask themselves the question 'Why is it necessary to acquire the data?', 'What, exactly, do you seek to achieve?'.

Example – For personal data such as Telephone Billing: only the number(s) required for the time periods being investigated should be sought and only for those individuals suspected of having a link with the offence.

A list of phone numbers of the person(s) involved in the suspected offence can be collected if there are indications that such data serve the purpose of the investigation. It cannot be kept or processed after the analysis shows that the data are not strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for police purposes should be used for those purposes only and should not be used in any other way that is incompatible with the original purpose stated at the time of collection and is necessary for and proportionate to the pursuing of police purposes, unless this is provided for in law (see Article 9 of Convention 108) [In assessing the compatibility of the use of data for the same purpose, one should consider the following criteria: (i) relation between purposes; (ii) context of the collection and information given to data subjects; (iii) nature of personal data; (iv) consequences for data subjects of the intended subsequent use; (v) existence of appropriate safeguards.]

Comment [A5]: Reference to « compatible processing » is very confusing. In paragraph 3 you refer to processing for "police purpose" other than the one for which the data have been collected. This seems to embrace both data collected originally for police purposes and those collected for non-police purposes. In this context you say that the analysis of the "compliance criteria" referred to paragraph 2 is necessary. Do you mean "compatibility criteria"? However, for any processing for a "police" purpose, you need a law. Thus, does it mean that, despite a law permitting to process data for a police purpose, you still need to apply the compatibility criteria? This would be very restrictive (more restrictive that required under the EU Police Directive).
If in paragraph 3 you refer to processing for another "police" purpose, one should understand that in paragraph 2 you refer to "compatible processing" for other purposes (unless in paragraph 3 you refer only to data initially collected for non-police purposes). Again, it is not clear if you mean processing based on another legal ground or processing based on the same legal ground. The latter seems impossible: how can you imagine processing based on "police" law for a non-police purpose? The former would, again, go beyond the requirements of the EU law (here: GDPR). Under Article 6 GDPR, there is no need to check compatibility of processing based on another (valid) legal ground.
In any case, the concept of "compatibility" referred to in paragraph 2 (and perhaps 3) is not the one referred to in the EU law (while the compatibility criteria referred to in the text are clearly inspired by the GDPR) and hence should be explained.

Subsequent use of data is considered for the purposes of this guide as a new data processing operation which has to fulfil all the criteria and conditions mentioned above. The subsequent use of data shall be lawful, undertaken for a legitimate aim and necessary and proportionate to this legitimate aim.

The police shall ensure at all stages of the data processing and for the subsequent use of data as stated in the General considerations that the personal data are accurate, up-to-date, adequate, relevant and not excessive in relation to the purposes for which they are processed.

Example: Police data collected for an investigation where the political affiliation is irrelevant, cannot then be used to determine the political affiliation of the concerned person.

3. Subsequent use of data

Every subsequent processing of data for police purposes other than that the data were originally collected for, must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be undertaken for a legitimate aim and should be necessary and proportionate to the legitimate aim pursued.

Personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set out in Point 2. The general rule is that if data are likely to be used in a different case or in a different operation of the police, the assessment of compliance described in Point 2 shall be applied to this new processing as well (This is not applicable if data are used for purely statistical or scientific purposes). Notwithstanding thecomputerised and/or automated data processing and the large volume of personal data stored very often in different processing environments, the, personal data collected and retained for police purposes should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

Comment [A6]: See above.

It should be noted, moreover, that any subsequent use of personal data related to vulnerable individuals such as victims, minors, or of those enjoying international protection, should be subject to additional care and legal analysis with a special attention to the application of the principles of necessity and proportionality.

In cases such as trafficking in human beings, drug trafficking or sexual exploitation, where victims' data may subsequently be used also when they are considered as suspects, or where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to look at existing international good practice (in international or regional police bodies) and to enhance their exchange of information on the matter with other national police bodies.If all legal requirements as put forward in Point 2 are met, it should not represent any obstacle to the use of data of these persons for police purpose, but during these exchanges, confidentiality rules have to be followed.

Example - Data collected for tax purposes from a data subject can only be processed for law enforcement use by police () if the law allows it, if they are used for a legitimate aim and in a way that is necessary and proportionate to the aim pursued. In a concrete investigation of money laundering, the use of tax declarations' data of an individual can be envisaged to establish or deny a link between the individual and the money laundering operations. .

4. Processing of special categories of data (sensitive data)[9]

Special categories of data, such as genetic data, personal data related to offences, criminal proceedings and convictions and related security measures, biometric data uniquely identifying a person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical nature, for instance additional security measures, and of an organisational nature, for instance having such sensitive data processed separately from the processing environment of the "ordinary" categories of data. Safeguards should be adjusted to each data processing operations taking into account their specificities and it is highly recommended to use multiple

[9] Paragraph removed from previous Point 8

levels of protection for those categories of data (e.g.: separate main-frames, shorter data retention periods, etc.). It is of paramount importance to prevent unauthorised or unwanted access to those categories of data even with additional security measures.

A careful balance of interests taking into account the purpose of the investigation, the context and the nature of the data is necessary to determine whether or not, and to which extent, the police could process sensitive data. For instance, it would be advisable to differentiate when biometric data is processed by the police whether it is for identification purposes (where for instance 2 fingerprints could suffice) or it is for crime investigation purposes (where more fingerprints could be needed).

The use of Data Protection Impact Assessments (DPIA) which is in general is to be carried out where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons can be recommended also in order to help to ensure that appropriate safeguards are put in place. The data controller should assess and demonstrate whether the purpose of the processing can be achieved in a manner that impacts less on the right to privacy and data protection and if the processing of special categories of data does not represent a risk of discrimination for the data subject.

Moreover, it should be recalled that the collection and processing of sensitive data in the context of profiling is prohibited (Principle 3.11 of Recommendation 2010 (13)[10] except if these data are necessary for and proportionate to the lawful and specific purposes of processing and as long as domestic law provides appropriate safeguards. In this context, besides measures detailed above, the use of PETs and more frequent checks on the lawfulness of the processing can be recommended. This could, for example, translate into measures put in place to counter the assumption that individuals belong to a criminal organisation because of where they live, where a criminal organisation is active or where the individuals have the same ethnic origin.

Example - Targeting groups or individuals based solely on religious beliefs would not be allowed. In an investigation into a group of individuals engaging in possible terrorist activities that were attached to a particular religious group, it could nevertheless be of importance to process data specific to the followers of this specific religious group (related to worshipping place, religious preachers, customs, teachings, members and structure of the religious community, etc. that was pertinent to the investigation).

5. Providing information to data subjects

One of the most important obligations of a data controller is to provide information on data processing to data subjects. This obligation is two-fold: it requires the data controller to provide *general information* to the public on the data processing that it carries out, and to give *specific* information to data subjects if no restrictions or derogations apply to the data processing.

Information provided to the wider public, should promote awareness, inform them of their rights and provide clear guidance on exercising their rights. The information provided should be effectively and broadly accessible. Moreover it, should include details about the conditions under which exceptions apply to the data subject's rights and how they could submit an appeal to the DPA or to the judiciary..

Deleted: ,

Deleted:

Websites and other easily accessible media perform a role in informing the public. It is recommended to have in place letter templates on these websites or other media to help the data subjects exercise their rights. It is the responsibility of the data controller to provide information which adequately highlights data protection and data subjects' rights.

[10] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member stateson the protection of individuals with regard to automatic processing
of personal data in the context of profiling
(https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00)

In order to comply with the second obligation of giving data subjects specific information regarding data processed, the police shall inform data subjects on the data processing envisaged before the processing or, if it is not possible, for objective reasons, shortly after it. This communication shall comprise information on the data processing, on the collection of the individuals' data and comprehensive information on their rights.

The obligation to provide specific information implies that, in principle, the data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.

The information should be provided unless a restriction or derogation applies as described in Point 7 taking into account the specific nature of sensitive files, such as criminal intelligence files, files containing sensitive data. in order to avoid serious prejudice to the performance of police functions or to the rights of individuals. Even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.

Very often data subjects, because of restrictions or derogations of their right to information, cannot receive complete information on the processing the police undertake with their data; this should not affect their exercise of the right of access.

Example - For the purpose of covert monitoring of a high risk sex offender, data processing and long-term data retention may be justified without informing the individuals under surveillance if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved, the data subject should be informed about the fact that she or he was subject to such measure.

6. Data subject's rights[11]

Accessing their personal data is a fundamental right for data subjects as it allows them to be aware of the processing on data related to them, Moreover, it can also be a prerequisite to enable the exercise of further rights, such as thethe right to information, the right of rectification and the right of erasure

In case an individual has her/his data collected during the course of an investigation or other tasks of the police as described in Point 1, as soon as circumstances safely permit, the police [in principle] should inform the individual of the data processing if there is such request. Specific information should be given in clear and plain language upon request . The communication has to contain the same information as described in point 5, unless data subjects wish otherwise.

The law can provide, under the strict conditions described in Point 7, that the right to be informed upon request may also be limited or excluded, should the provision of such information prejudice the investigation, or another important police task, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified.

The police should aim to answer even general questions arising from data subjects on the processing activities in relation to their personal data, but can use standardised forms to facilitate communication.

Example: If a data subject asks the police on data it processes on them, the police, if no exception is applicable, should provide a detailed answer with legal references, but should do so in a plain language, avoiding uncommon or specialised expressions.

The right of access should, in principle, be free of charge.

[11] Paragraph removed from previous Point 17.

It is possible to charge a reasonable administrative fee for the request, if national law permits and the request is manifestly unfounded or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such refusal.

To ensure a fair exercise of the right of access, the communication "in an intelligible form" applies to the content as well as to the form of a standardised digital communication. It is, however, advisable to refer to national legislation to ensure consistency and to avoid suspects utilising this method to find out whether there is an on-going investigation into them.

In respect of direct access, the data subject can request access to the controller of the files. The data controller will assess the request and any possible restriction or derogation which can only be used if it is vital for the performance of a specific police task as described in Point 1, or it is necessary for the protection of the data subject or the rights and freedoms of others, and reply directly to the data subject. In case of a restriction, partial information, and in case of derogation, information on the use of derogation, shall be still given, with the motivation for using such measures in both cases, as well as information concerning redress.

Example: The access request can be refused if there is an on-going investigation on the person, and providing the data subject access to the data could compromise such investigation.

If restriction or derogation were to be used, any answer should take into consideration, according to national law or practice, all circumstances to which the restriction or the derogation is applicable.

As a rule, domestic law should, ideally, provide for direct access. If the right of access provided for is indirect, the data subjects may direct their request to the supervisory authority, which after being properly mandated, will carry out the request on their behalf and conduct checks regarding the availability and lawfulness of the processing of the data subject's personal data. The supervisory authority will then reply to the data subject (providing what data it is possible to release, subject to any legally allowed restrictions or derogation). In case of a restriction or derogation, the same communication should be made possible as in case of a direct access.

The data controller should assess the request and reply to the data subject within a reasonable time limit, as provided for by domestic law.

There should be arrangements in place to confirm the identity of the data subject before access to any data is granted as well as to obtain information on the processing activities to which the request refers. The same holds if the data subjects delegate the authority to someone else to exercise their rights.

It is an essential right of the data subjects to be able to amend any incorrect data held on them. If the data subject finds data that are incorrect or irrelevant, she/he should have the right to challenge it and ensure that they are amended or deleted.

In some cases, it may be appropriate to add additional or corrective information to the file. It is important to underline that this right can only be exercised with due respect to other individuals' rights, for instance to the rights related to a testimony in a criminal case (which does not preclude per se the exercise of the data subjects' rights related to soft police data).

Data subjects can ask for the deletion of their personal data where such processing is unlawful.

If the data to be corrected or erased has been communicated elsewhere the relevant authorities should be informed of the changes to be made.

All proposed changes should be supported by evidence. If data subjects can prove by use of the official documentation that the data processed by police in respect to them are incorrect, the data controller shall not have the right of discretion whether to correct them.

It may be necessary for the police, as dealt with under Point 7, not to give information or grant the right of access, of deletion and of correction which might jeopardise an investigation and should therefore be

excluded for its duration. Similar restrictions or derogation may be imposed by national law as described in Point 7.

Restrictions or derogations to the rights of data should only apply to the extent necessary and be interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis. Any decision to refuse a data subject's request should be provided in writing (including by electronic means). The response should provide clear justification of the decision making which can be verified by an independent authority or a court. It is possible that communicating the reasons for refusal could pose a risk to law enforcement or the data subject or to the rights and freedoms of others. If this is the case, it should be documented and provided to the independent authority or court to be verified, if required.

Example - If person A submitted a declaration against person B accusing her/him of committing a serious offence and later it emerges that the accusation was false, it might be relevant for the police to retain the false statement and the information surrounding it.

Although the statement was proven to be false, if the police needs to retain the data in the interest of the investigation for instance , a clear corrective statement on the file, instead of removing the false statement, would be necessary.

The data subject should be informed of all available options following a refusal decision such as an appeal either to the supervisory authority, to court or to another independent administrative authority.
Depending upon national legislation, specifically whether there is a direct or an indirect right of access, the actual communication of the result of the review or appeal may differ. In the case of indirect access the data subject should at least be informed that a verification of the police file has taken place. Alternatively, the supervisory body may request the police to release the data contained in the file to the data subject. The court or tribunal may have powers to enforce the access, correction or deletion of data from the file even in access-request cases referred to them by police or the supervisory authority.

If police sends a refusal letter it should contain the name, address, web address, etc. of all possible forafor redress.

The data subject should have access to a court or tribunal in order to submit an appeal, and have the reasons for refusal verified if they are not satisfied with the reply given by the supervisory authority or the independent authority. The supervisory authority should have sufficient powers to examine the police file concerned and have the assessment communicated.

7. Exceptions from the application of data protection principles

Exceptions can only be used for specific purposes foreseen by article 8 of European Convention on Human Rights and article 9 of Convention 108, if foreseen by law (the law should be public, open and transparent and, in addition, detailed enough) and if they constitute a necessary and proportionate measure in a democratic society.

The exceptions which have to be incorporated into national legislation should not be described in a general way, but should serve a well-defined purpose. Exceptions can be applicable to those principles described under Points 2,3,,5,as well as to the data subjects' rights (Point 6) in case of some specific purposes in relation to which data processing activities are undertaken. In particular they concern activities undertaken for the purpose of the protection of national security, defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest (which includes purposes in connection with the fulfilment of a state's international legal commitments or obligations, most prominently deriving from the binding decisions of United Nations' bodies, and humanitarian purposes.) or the protection of the rights and fundamental freedoms of others.

Example - If giving information to a data subject may endanger the safety of a witness or an informant; this right can be limited in light of such circumstances.

If the exception, as defined by national law providing specific safeguards is used by the police, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. The aim of using exceptions by the police should be limited to cases where the use of those rules and principles would endanger tasks of the police described under Point 1..

Example: If data collected for police purpose in an investigation are likely to serve national security purposes they can also be used to this latter purposes to the extent set forth by national legislation. If specific intelligence proves that money laundering operations have been carried out to finance terrorist operations, data collected on individuals during the investigations on money laundering can be used for the purpose of eliminating the close and imminent terrorist risk.

Comment [A7]: And not national security, defence, etc… e.g. public security, rights & freedoms of others?

Comment [A8]: Not sure about this example. It refers to the use of data for another purpose, based on another (valid) legal ground. Would you need an exception for this?

8. Use of special investigative techniques

The police should always adopt the least intrusive means of data processing during its operations. If less intrusive methods can be used to achieve the desired ends, they should be preferred. The use of special investigative techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods.
With increasingly sophisticated technological developments, electronic surveillance has become easier, however, the use of these techniques interferes with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the high potential of severe interference with the right to privacy has to be balanced with the efficiency of investigations.

Example: In an investigation, the evidence for communication between two suspects can be gathered in various ways. If, by the use of interrogations, testimonies, the obtaining of call data, the same result can be achieved without jeopardising the effectiveness of the investigation, it is to be preferred to the use of more intrusive surveillance measures, such as wiretapping.

9. Introduction of new data processing technologies

If the introduction of new technologies is likely to result in a high risk to the individual's rights, the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. The introduction of new data processing technologies is considered to be subject to a DPIA as probability of risks to the individual's rights is usually high. It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity. The relevance of the DPIA shall be checked at reasonable intervals.

It is also of great importance, that in terms of data security and safety of communications, the highest standard is taken into account when introducing such technologies.

Example - New data mining techniques may offer extended possibilities for identification of possible suspects and should be assessed carefully for their compliance with existing data protection law, together with assessment of the risks it may represent to individual's rights and suggestions for the adoption of safeguards to ensure the protection of data, including with regard to data security.

The data protection authority has an important role in advising which risks are involved for data protection and which safeguards should be provided to ensure that any technical means comply with data protection law. However, the police do not have an obligation to turn in every case to the supervisory authority where it introduces new technologies. It may do so if the DPIA it previously conducted demonstrates a significantly persisting high risk to the individual's rights notwithstanding the adoption of specific safeguards.

The consultation between the supervisory authority and the data controller should provide the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.

. Appropriate details should be provided to the supervisory authority, in particular regarding the type of file, the data controller, data processor, the legal basis and the purpose of the data processing, the type of data being processed and by whom the data is being accessed, as well as information on retention of data, log policy and access policy, and other relevant technical aspects of implementation.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data could be reported to or made available for consultation to the data protection authority.

Following consultation, the data controller should consider carefully to implement any necessary measures and safeguards that have been recommended by the data protection authority.

Example - Introducing an automatic facial recognition system or other system based on the automated processing of biometric data would be very likely to need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed and recommended by the data protection authority after being consulted on the issue, specific safeguards should be put in place (concerning the data retention time, the cross matching functionalities, the place of the storage of data and the access to data issues, etc.) to comply with data protection principles and provisions

Use of the Internet of Things (IoT) technology in police work

Data sent to and from police during operational activity via the internet are good examples of the IoT already in use. Due to potential security vulnerabilities, IoT requires measures such as data authentication, access control to ensure data security and resilience to (cyber) attacks.

Example: In light of their potential security vulnerabilities, smart glass used by police should not be directly connected to a national criminal record data base and data collected should be guaranteed a high level of security.

Big data analytics in the police

Technological advances in processing and analysing large and complex data sets leading to big data and big data analytics present opportunities and challenges to the police, who is turning to digital sources and profiling techniques to perform their tasks.

Big data technologies enable bulk collection and analysis of a vast quantity of data generated by electronic communications and devices aggregated with other bulk data. This could interfere with the right to privacy and data protection.

The Council of Europe's Recommendation CM/Rec(2010)13[12] on the protection of individuals with regard to automatic processing of personal data in the context of profiling and the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[13] can be of use in the context of Big Data analysis for police use too.

Big data technologies and analysis techniques may help assist detecting crime, but there are, however, considerable risks to this type of data processing that should be taken into account:

- Databases originating from one domain can be used in another domain and for another purpose, which changes the context and may lead to inaccurate conclusions and lack of valid legal basis, therefore to unlawful data processing with possibly serious consequences for the individuals involved.

[12] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling
[13] Document T-PD(2017)1 - Big Data Guidelines

- Profiling may lead to drawing discriminatory conclusions, which can result in the reinforcement of stereotypes, stigmatisation and discrimination.
- The increasing amount of personal data held in databases may lead to severe vulnerabilities and subsequent risk of data breaches if information security is not guaranteed.

Where big data relies on personal data, data controllers should pay additional attention to the following requirements:

- Verification of data accuracy, context and relevance of the data.
- Its use requires a high level of accountability.
- Its use shall be combined with methods of investigation which complement the conclusions drawn from the big data analysis. A decision affecting a person shall not be taken solely on automated processing of personal data.
- As for other types of data processing, it is of paramount importance that its use shall be ~~shall be be~~ necessary and proportionate for the fulfilment of police tasks described in Point 1, with special attention for the data processed to be adequate, relevant and non-excessive in relation to the purpose for which they are processed.
- Predictive analysis requires human intervention to assess the relevance of the analysis and conclusions.
- Ethical guidelines developed at national or at international level should be taken into consideration.
- As a principle and subject to restrictions and derogations mentioned in Point 7, transparency should be ensured by the data controller by explaining how the data are processed in accordance with privacy and data protection principles. If data collected for one purpose is used for another purpose, the data controller should in principle make the data subjects aware of this subsequent use.
- Even if complex methods are used, the lawfulness of the processing – including subsequent use of data - and compliance with the conditions set by Article 8 ECHR and Convention 108 should be demonstrated.
- An information security policy should be in place and implemented throughout the processing.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals and the administrative and judicial means exist for individuals to challenge those decisions. This implies data subjects' awareness of the reasoning of the algorythm used and the purposes for which it was used.

The above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones, are even more necessary when sensitive data are processed in Big Data analytics.

10. Storage of data

"As pointed out in Point 2" data shall be processed until they have served the purpose for which they were collected. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

There should be a clear distinction in how the police stores and processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses. This should also relate to the specific purpose for which the data was collected. Additional safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence. Clear rules have to be established in relation to the handling of different data bases with special attention to the analysis of multiple results.

The principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve the purpose of the prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where personal data is processed for the purpose of the maintenance of public order.

The grounds for retention and processing should be reviewed periodically. The unlawful processing of personal data outside of the legal framework allowed for the retention constitutes a severe violation of the

Comment [A9]: Overall: perhaps it would make sense to keep only recommendations specific to big data and replace those which apply to all kinds of processing with a general reminder?

Comment [A10]: Meaning: other than automated processing? Or other than "big data"? not very clear… and the recommendation (minimisation principle) seems applicable to all types of personal data processing, it is already made clear before. Is it necessary to repeat it here?

Comment [A11]: Reads strange: would the principle of lawfulness depend on complexity of methods?

Comment [A12]: Introducing various degrees of necessity might confuse the reader

Comment [A13]: Could be "otherwise processes" (processing include storing), but the title of this point suggests that only storing is discussed…

Comment [A14]: Is it lawful to differentiate between the two categories of innocent (not convicted) people?

Comment [A15]: What is the analysis of multiple results?

Comment [A16]: This is already included in the prevention, investigation and prosecution of criminal offences and execution of criminal penalties. If this notion is interpreted to go beyond these activities, it would excessively broaden the scope of the guide (referring to specific rules for police) to areas which should be covered by general data protection regime. We suggest deleting it.

Comment [A17]: Can it be lawful if it's "outside the legal framework allowed for the retention"?

right to protection of personal data. If the law in relation with a specific crime provides for a data retention period of 4 years and if
personal data are processed in relation with this crime by the police solely on this ground after 4 years have passed since the collection of the data in question and no other legal ground to process this data exists, the retention of this data could be considered as unlawful.

Comment [A18]: Isn't it already explained in the frame below?

General data retention periods are usually regulated in national or international law. In order to comply with the legislation while ensuring the effectiveness and the success of an investigation police bodies are strongly advised to develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data.

For example, in a case where the law prescribes a 4 year data retention period but the individual subject to an investigation is acquitted from all charges by the court after 2 years, her/his data shall be deleted (if the individual is not a recidivist or there is no information on her/him committing again the same category of crime) from the database, provided that all deadlines for the review of the case have expired. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judicial procedure terminates completely (which means all redress have been made or all deadline for redress have been passed).

The police should provide systems and mechanisms to ensure that the data that are stored are accurate and that their integrity is maintained.

International obligations, which include providing data to international bodies such as Europol, Eurojust and INTERPOL, bilateral agreements and mutual legal assistance between member states and third countries must be observed when shaping internal policies.

Data should be categorised according to the degree of accuracy and reliability in order to assist the police in their activities. It is recommended that handling codes are used to distinguish these categories. A classification system facilitates the assessment of the quality of the data and how reliable it is. Classification of data is also important when it is to be communicated to other police bodies or states.

Example - Information collected directly from a person's statement will be assessed differently than information collected from a person's hearsay statement. Data based on facts, or 'hard' data, will be assessed differently than data based on opinions or personal assessments, or 'soft' data.

Personal data collected by police for administrative purposes must be kept (as far as possible: logically and physically) separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by law.

Examples of administrative data include lists of data on licence holders or data on human resources and firearms certificates.

11. Communication of data within the police sector

A distinction should be made between domestic communication of data and international transfer of data. Within these two distinct operations different requirements apply, depending upon who is receiving the data, whether it is the police, another public body or a private party. The police can only communicate personal data within the police sector if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

There should be clear and transparent rules on how the police grant access to data held by it and on which grounds.

The police, domestically, should only share information (among police) when there is a legal basis for the request, e.g. an on-going criminal investigation or a shared law enforcement task and laws or agreements allowing the communication

The police can share data with other police organisations if the personal data are relevant for the purpose of prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where they are processed for the purpose of the maintenance of public order.

The communication of personal data in general should be in line with the general considerations described above.

Example: A police unit can share data on a suspect who presumably committed a tax fraud with another police unit investigating a murder case if there is indication that the suspect for this crime could be the same person or if doing so will materially assist the investigation.

12. Communication of data by the police to other public bodies

The communication of data outside police is permissible if it is provided for by law and the data are required by the recipient to enable them to fulfil their lawful task. Mutual assistance agreements foreseen by the law between law enforcement and public bodies allows the public bodies to have access to law enforcement data which would be essential in the fulfilment of their duties and tasks (for example in their investigations or other legal duties in accordance with national law).

Stricter principles than those set forth in Point 11 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the processing of personal data, which are considered sensitive, could result in adverse effects for the individual.

Communication of data to any other public authority may also be allowed if it is foreseen by law, is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to other persons or to public order or to public security.

The communicated data may only be used by the receiving body for the purposes for which the data were transferred.

Example - A claim for a residence permit made by a migrant. Police data may be required to verify if the person was ever involved in criminal activity. It would be in the interest of the Immigration Office and the claimant for this communication of data to take place.

13. Communication of data by the police to private parties

There may be occasions when, under strict conditions, the police can communicate data to private bodies. This communication has to be based in law and can only be done by the authority which is processing the data. Such communication can only be done for the purpose of the investigation or other important police tasks as described in Point 1, in the interest of the data subject, for humanitarian reasons or if it is necessary to prevent serious and imminent risk to public order or public security. For example, there might also be instances where police data may be communicated to humanitarian organisations based on international law, in the interest of the data subject or for humanitarian reasons.

Where the police shares data with media in respect of making information related to an investigation public, special consideration should be given to the assessment to determine that it is necessary and in the public interest that such publicity is allowed.

Comment [A19]: As explained in the comment to section 10, we suggest deleting it

Comment [A20]: Added value?

Such communication should only be on a case by case basis and in each case there must be a clear legal basis providing the necessary procedure (e.g. need for specific authorisation) to be followed for any such communication to occur.

Example - When the police communicate with the financial sector in relation to known fraud or theft offenders, when it communicates with an airline about stolen or lost travel documents or when the police releases details of wanted persons believed to pose a risk to the general public.

14. International transfer

Any transfer of police data internationally should be limited to police bodies and should be fit for purpose and in accordance with the law. For this, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data handling, regional legal frameworks such as EU and EU institutions' legislation (on Europol, Eurojust, Frontex, etc.) and subsequent agreements (operational bilateral agreements), bilateral treaties and in general, international agreements on mutual assistance, or other bilateral or multilateral agreements made regarding effective cooperation can be of use.

When considering sharing any data, consideration should be given as to whether the receiving authority is performing a function conferred to it in law related to the prevention, investigation, or prosecution of criminal offences, the execution of criminal penalties and the maintenance of public order, and whether the sharing of the data is necessary to perform its specific task.

Comment [A21]: As explained in the comment to section 10, we suggest deleting it

The sending authority should ascertain that there is an appropriate level of data protection in the receiving state and that the receiving state complies with the relevant rules of international transfers of personal data. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. This means of transfer should be used as a last resort option. International transfers framework such as "INTERPOL's Rule on the Processing of Data" and its "Statute of the Commission for the Control of INTERPOL's files" Rules on the Control of Information and access to INTERPOL's Files", the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185) may be taken into account[14] so as to ensure that any transfer of data is legally justified and has appropriate safeguards in place. The request should clearly state all the necessary elements from the requesting party to enable the receiving party to make a sound decision on the request. These details would be expected to include the reason for the request as well as the purpose for the transfer of data.

An appropriate level of data protection should be guaranteed (e.g. through ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments) if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

If there are conditions applied by the sending authority in relation to the use of the data in the receiving state these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout its lifecycle.

Example - Further transfer of data should only be allowed if this is necessary for the same police purpose as the original transfer and the second recipient is also a police body ensuring an appropriate level of data protection. The police body which originally sent the data must also consent to the onward transfer. If the police from country X sends personal data to the police of country Y it is only permissible for the country Y to transfer this data if above all requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) if country X consents to the transfer. If the data is sent to country Z which is a non-member of the Convention 108, then country Y should ascertain that this country provides an appropriate

[14] This is without prejudice to the right of the Committee of Convention 108 and other instances disposing such power to assess and to review if necessary the level of data protection guaranteed by those multilateral agreements

level of protection of personal data and effective means of exercise of the related data subject rights.

The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases if it is required for the performance of the task of the transferring authority and there is no effective means of transferring the data to a police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers.

Example: If tax authorities in country X requests the police in country Y about the whereabouts of a person involved in non-criminal tax evasion because they have evidence that the person is involved in criminal matters in country X, the police can transfer the personal data of the individual.

The international transfer of personal data between police and private bodies in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police as described in Point 1, provided by legal means, where the crime is of trans-border nature and where the involvement of the police would not be possible for objective reasons . Other facts as data security, the reassurance received as to the use of the data and the lawfulness of the data transfer in the receiving country have to be taken into account. In this context it is to be noted that in such a case, the data controller has a double obligation with respect to the protection of personal data: one imposed by the legal framework of the country where it resides and the one which is related to the data transfer. The local police should be informed afterwards. The police are required, wherever possible, to make use of existing international legal instruments, in respect of this type of data transfer.

Deleted: and

Deleted: emergency, the gravity of the

Deleted: ,

Deleted: t

Comment [A22]: who resides there and why is this two different legal regimes?

Example: In an investigation, carried out within the framework of an international multilateral agreement, into child sexual exploitation where the victim is in country Y and the police there have commenced an investigation, and the material has been made available on the internet by the suspect residing in another (country X) and there is a high risk that the suspect seeks to avoid justice by fleeing country X, the police in country Y can request, on an exceptional basis, that a service provider in country X provide the whereabouts of its customer. However, the police of country Y should inform the police in country X of its operation as soon as is possible and then seek to resolve the matter in cooperation.

15. Conditions for communications

Since there is a general obligation for the data controller to ensure a high level of data quality, it is advisable to have in place an additional check before sharing the data with others. When communicating or transferring data, it is always advisable to double-check the quality of data, if it is correct, up-to-date and complete. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated. It is required to establish secure channels of communication which ensure data security at the highest level possible. The quality of data can be assessed up to the moment of communication.

Example: If personal data that contain incorrect data (personal or otherwise) are sent they could adversely affect the investigation, cause harm to the individual concerned or others involved, or who may become involved as a result of the incorrect data being transferred. This can, as a result, leave the police in the transmitting and receiving states open to civil redress. In essence, if an individual is arrested based on a wrong communication of the suspect's name, it seriously harms several human rights of the individual concerned and can undermine any criminal investigation.

16. Safeguards for communication

It is of utmost importance that the necessity and purpose limitation principle should be applicable for any domestic communication or international transfer of personal data outside of police organisations.

Any data communicated should not be used for anything other than the purpose for which it was sent or received. The exceptions to this are when the sending authority, based on legal provisions, gives agreement

to any further use, and if it is necessary and vital for the recipient to fulfil their task. Data can also be communicated if it is in the interest of the data subject,for humanitarian reasons, is necessary to prevent serious and imminent risk to public order or public security or an appropriate level of data protection is guaranteed by the recipient by international, national legal instrument, ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments, as foreseen by Convention 108.

Example: Personal data sent by the police of country X to the police of country Y in a money laundering case cannot be used by the police as profiling on the given individual in respect of her/his religious beliefs or political activities (unless those are relevant to the crime committed and police in country X has given its consent for this use).

17. Interconnection of files and on-line access to files

In specific circumstances the police may seek to collect data by coordinating its information with other data controllers and processors. Furthermore, it may combine personal data stored in different files or in different databases that are held for different purposes, such as those held by other public bodies and/or private organisations. This may be in relation to an on-going criminal investigation or to identify thematic trends in relation to a certain type of crime.

In order for these actions to be legitimate they must be authorised or be underpinned by a legal obligation to comply with the purpose limitation principle.

If the relevant police body has direct access to files of other police or non-police bodies, ir must only access and use the data if domestic law, which should reflect the key data protection principles so permits.

Clear legislation and guidance, which adheres to the data protection principles, should exist for cross-referencing of databases. Such cross referencing should be necessary, purpose bound and proportionate. With relation to personal data stored in other data controllers' or processors' data base all conditions described in Point 2 have to be fulfilled and regularly checked.

Example - Data held for citizenship purposes can only be used in an investigation if the national legislation allows it and to the extent to which it is necessary for the purpose of the investigation to do so. For instance, the number of children a suspect has may not be relevant in an investigation, and should therefore not be processed by police. Access in this case to a database can be lawful if it respects the conditions laid down in the case-law of the European Court of Human Rights on law enforcement access to personal data collected for non-law enforcement purposes.

Deleted: but it can only be legitimate if it respects the principles of data protection if it respects the conditions laid down in the case-law of the European Court of Human Rights on law enforcement access to personal data collected for non-law enforcement purposes

18. Data security

The police must take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The controller must notify, without delay, at least, the competent supervisory authority of those data breaches which according to its assessment may seriously interfere with the rights and fundamental freedoms of data subjects. The information of data subjects of data breaches which may seriously interfere with their rights may also have to be ensured without undue delay, unless it jeopardisese the task of the police.

Information security is essential to data protection. It is a set of procedures to ensure the integrity, availability and confidentiality of all forms of information within the police organisation, with the aim of providing security of data and information, and limiting the impact of security incidents and data breaches to a predetermined level.

The level of protection given to a database and/or an information system or network is determined by a risk assessment. The more sensitive the data are, the greater protection is required.

Authorisation and authentication mechanisms are essential to protect the data, and sensitive information should always be encrypted. It is considered best practice to have in place an audit regime to regularly check that the level of security is appropriate.

Police authorities are advised, where necessary, to conduct DPIA (see Point4) to assess the privacy risks to individuals in respect of the collection, use and any disclosure of information. This will help to identify risks and develop solutions to ensure that concerns are addressed appropriately. Any such impact assessment should cover relevant systems and processes of processing operations, but not individual cases.

A Data Protection Officer (DPO) within the police can play an essential role in carrying out internal audits and assessing the legitimacy of the processing, which contributes to a higher level of data protection and data security within the organisation. Moreover, the DPO can facilitate the dialogue between the organisation and the data subjects, as well as the organisation and the supervisory authority which can add to the overall transparency of the police body.

An Identity & Access Management System (IAM) may be recommended to manage employees and third party access to information. This will require authentication and authorisation to access the system and set privilege rights to determine what can be viewed. IAM can be seen as a useful requirement to ensure safe and appropriate access to data.

The data controller, following an evaluation of the risks, should at implement measures in respect of:

- equipment access control,
- data media control,
- storage control,
- user control,
- data access control,
- communication control,
- input control,
- transport control,
- recovery and system integrity,
- reliability and integrity.

Privacy-by-Design

The concept of privacy-by-design is an integral part of data security. Data protection and security may be embedded directly into information systems and processes, using technical and organisational measures, to ensure a high level of data protection and security and, in particular, to minimise the likelihood of data breaches. This approach is known as Privacy–by–Design, promoting privacy and data protection compliance from the start. It can be achieved through software and/or hardware. It requires a threat analysis, a full life cycle approach and rigorous testing.

Data controllers should ensure that privacy and data protection is a key consideration in the early stages of any project and then through its life cycle. Specifically, when building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have privacy implications and embarking on an information sharing initiative using data for new purposes.

Privacy-by-Design requires the implementation of Privacy Enhancing Technologies (PETs) to enable a better protection of personal data. PETs prevent unnecessary processing of personal data, without losing functionality in the information system itself.

Example: Body scanners used for police purposes have to be designed to respect the privacy of the individuals being inspected while fulfilling the purpose of their use. Therefore the body image in such tools has to be blurred by default.

19. External control

There has to be, at least, one supervisory authority responsible for ensuring compliance of data processing to the international and national legislation within the law enforcement sector.

Certain states may require more than one supervisory authority, for instance a national or federal authority and a number of decentralised or regional authorities, whilst others will prefer to have a single supervisory authority, responsible for the entirety of the supervision of data processing operations.

The supervisory body should be completely independent, meaning that it does not belong to the law enforcement organisation, nor is it directed by another body whithin the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties and should not be instructed or forced to accept instructions from anybody. The personal independence of its chair/president including political, financial, functional and operational independence, are decisive factors when judging how independent the supervisory body is.

National law should provide for advisory, investigative and enforcement powers to enable it to investigate complaints, to have regulatory measures or to be able to impose sanctions where needed. The legal and administrative tools at its disposal shall be efficient and enforceable.

Supervisory authorities should have the ability to cooperate in law enforcement matters bilaterally and also via the Committee of Convention 108.

Example: The supervisory authority must be independent and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Comment [A23]: Rather: "should not accept instructions". If someone instructs it but it does not accept instructions, it's still independent. If it accepts instructions without being forced, it is not independent.

Comment [A24]: Can you say that a "tool" is enforceable? Maybe; "tools at its disposal shall be efficient and its decisions should be enforceable"?

Comment [A25]: I thought that Member States are free to decide who will represent them in the Committee… These can be supervisory authorities, but not necessarily.

Glossary/Definitions

For the purposes of this Guide:

a. “personal data” means any information relating to an identified or identifiable individual (“data subject”);

b. “genetic data” are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

c. “biometric data” are data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual;

d. “soft data” (evidence based on testimony or other personal assessment) means data acquired through testimony of person involved in the investigation;

e. “hard data “ (evidence based on documents or proven facts) means data acquired from official documents or other certified sources;

f. “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

g. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

h. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

i. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

j. Internet of Things (IoT): is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

k. “covert surveillance” means all measures aiming at monitoring discreetly the movements of persons, vehicles and containers, particularly those involved in organised or cross-border crime.

l. “special investigative techniques” techniques applied by the competent authorities in the context of criminal investigation for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person.

m. “privacy-enhancing technologies” (PETs) means a range of different technologies to protect personal data within information systems. The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.

EUROPEAN COMMITTEE ON CRIME PROBLEMS/COMITE EUROPEEN POUR LES PROBLEMES CRIMINELS

1. The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter "T-PD") prepared a "Draft practical guide on the use of personal data in the police sector" (hereinafter "the Draft practical guide") "to highlight the most important issues that may arise in the use of personal data in the police sector and to point out the key elements to be considered in that context".

2. The T-PD will discuss the "Draft practical guide on the use of personal data in the police sector" in view of its adoption at the forthcoming 35th Plenary Meeting (Strasbourg, 22-24 November 2017).

3. The T-PD Secretariat presented a revised version of the "Draft practical guide" to the Secretariat of the European Committee on Crime Problems (CDPC) and the Committee of Experts on Terrorism (CODEXTER) asking for comments on the draft from the two Steering Committees by 13 November 2017.

4. Replying to this request of the T-PD, the CDPC examined the text and adopted the present opinion following a written procedure:

5. The CDPC notes that Recommendation (87)15 clearly addresses the governments of the member States ("be guided in their domestic law and practice"). The "draft practical guide" is not quite clear in that respect. However, the "Introduction" seems to suggest that the guide should be used at an "operational level" thus by police authorities. Assuming that the latter is the intention, and while in many cases individual statements specifically refer to the applicable national law, it should be made clear, perhaps in the section on "general consideration", that the statements made in the handbook are subject to the rules of the applicable national law (or relevant international legal instruments) – c.f. e.g. use of the phrase "the police do not have an obligation…." in section 9 paragraph 3.

6. Furthermore, the CDPC finds that the relevant national law may not only be applicable data protection legislation, but may also include national criminal procedural law and legislation on judicial co-operation. The draft handbook focuses only on data protection aspects and on police authorities. However, it contains statements, especially in some of the ""Examples" given, on what the police may or may not do (c.f. e.g. Sections 11, 12 and 13, "Example" given in the last "box"). Data protection law, i.e. national law as well as the CoE Convention, however, does not necessarily give a final answer to the issues discussed. National criminal procedural law (or rules on judicial co-operation) may contain additional applicable obligations or provide a legal basis for the collection, processing and transmission of information including personal data (c.f. e.g. the issues discussed in sections 3, 5, 6, 8, 12, 13, 14, 16 and 17). And in respect of criminal investigations, national law may stipulate that when collecting, processing, or transmitting personal data or, for example, when informing the data subject, police authorities may do so only on behalf of and in line with instructions given by the competent prosecutor.

7. The CDPC further delivers the following remarks concerning specific sections of the revised draft:

    a. Section 3 paragraph 4: is it really helpful to the reader to merely state that it is "advisable for the police to look at existing international good practices"?
    b. Section 3: a) in paragraph 5 the sentence ", where applicable and as far as possible, should be added at the beginning after the words "There should be …" and b) in paragraph 13 the sentence ", as far as possible," should be added at the beginning after the words "Data should be …", in order the Council of Europe practical guide in line with the EU legislation.

c. Section 4 paragraph 1: in addition to the typical list of sensitive data, this paragraph also includes "personal data related to offences, criminal investigations…". While it is in principle appropriate to require appropriate safeguards also in respect of these types of data (c.f. also Article 6 of Convention 108 in respect of convictions), processing of such data is of course typical in any kind of criminal investigation.
d. Section 5 paragraph 4: The use of the term "shortly after it" may not only be rather vague, but it is also an example that the data protection law does not always necessarily provide a final answer to the question discussed: whether and when the data subject has to be informed about personal data obtained in the course of a telephone interception is to be regulated quite specifically in the applicable code on criminal procedure. Thus it is misleading and controversial to state here that the data subject should be informed "shortly after it".
e. Section 5 paragraph 6: "police functions or the rights of individuals" – what about causing prejudice to the prosecution services in charge of the criminal investigations?
f. Section 6 paragraph 2: this is another example of where the role of the prosecution services is not acknowledged. Also: what does "in principle" mean? Furthermore: the right to information is described here as a right which applies where so requested by the data subject. However, section 2.2 of Recommendation (87)15 seems to suggest a "proactive" information obligation.
g. Section 6 second paragraph on page 8 (starting with "In some cases"): the message here is not quite clear. If a data subject requests the rectification of (his/her) personal data contained in a witness testimony, the question of whether to rectify the data or to add additional information is not primarily a question of that witness's data protection rights. Also: what is meant by "soft police data" here?
h. Section 8: here again the issues discussed are not merely a question of data protection legislation but also, and above all, of criminal procedural law.
i. Section 14: this is an example of where the draft handbook does not acknowledge the role prosecutors (or investigating judges) frequently play in such "international transfers" (.c.f. e.g. the "Example" given in the first box on page 15) and that data protection rules do not necessarily give a final answer on the issues discussed (c.f. the "Example" in the second box on page 15).
j. Section 17: The statement in the "Example" (last sentence) according to which access "can be perfectly lawful but it can only be legitimate if it respects the principles of data protection" seems a bit unclear.

****

EUROPEAN DATA PROTECTION SUPERVISOR/LE CONTRÔLEUR EUROPEEN DE LA PROTECTION DES DONNEES (EDPS)

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied to ensure the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").
Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed application and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[15] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level.
The present Guide was therefore prepared to highlight the most important issues that may arise in the use of personal data in the police sector and to point out the key elements to be considered in that context.
This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance.
The overarching principles set out in Recommendation (87)15 and their practical implications aim to ensure that the use of personal data by the police is determined in full respect of the rights of the individual to privacy and data protection and that interferences with these rights are proportionate.
To facilitate the reading of the Guide, a glossary of the terms used is provided at the end of the document.

General considerations

The collection and use of personal data for law enforcement purposes constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and, as such, it *must* be based on law (clear, foreseeable and accessible), pursue a legitimate aim and be limited to what is necessary and proportionate to achieve that legitimate aim. (Former second paragraph moved upfront)

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data within the police should be processed on predefined, clear and legitimate purposes set in the law, they should be necessary and proportionate to these legitimate purposes and should always be in compliance with the original purpose. Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible.

1. Scope

The principles explained in the present guide apply to the processing of personal data for police purposes, primarily for the purposes of the prevention, investigation and prosecution of criminal offences, the execution of criminal penalties [and for the maintenance of public order by the police] (hereafter referred to as "tasks of the police"). Where 'police' is used in the text, it can be taken to mean wider law enforcement authorities, and/or other public and/or private bodies authorised by law to process personal data for the same purposes.

[15] See Report "Twenty–five years down the line" – by Joseph A. Cannataci

Deleted: for ensuring

Deleted: clear

Deleted: , aiming

Deleted: ing

Deleted: in the police

Deleted: are

Deleted: the a balance is struck between the essential objectives of general public interest (prevention, investigation and prosecution of criminal offences, the execution of criminal penalties and maintenance of public order), and the respect for

Deleted: processing

Deleted: based

Deleted: that it

Deleted: [in principle]

Deleted: The

Deleted: d

Deleted: It

Deleted: data which are processed within the police

Deleted: (Start) The collection and use of personal data for law enforcement purposes can constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and as such it *must* be based on law (clear and publicly available), pursue a legitimate aim/aim and be limited to what is necessary to achieve that legitimate /aimaim.

Deleted: specific

Deleted: offences and the

2. Collection of data and use of data

The collection and use of personal data for police purposes should be limited to what is necessary and be proportionate for the purpose of prevention, investigation and prosecution of criminal offences, the execution of criminal penalties (i.e. to a specific criminal offence(s) or the suspicion thereof) and for the purpose of the maintenance of public order. The police as data controller is responsible for all data processing it undertakes and is accountable for its data processing operations.

It is understood from Point 2.1 of the Recommendation that inforthe fulfilment of both of the main police tasks (prevention of a real danger and the suppression of a specific criminal offence), an evident and direct correlation should exist between the data processing carried out by the police and a situation where individuals have already committed or are likely to commit a crime.

The police should always choose the adequate legal basis to process personal data and should process personal data in a legitimate way. A careful assessment of the legal basis upon whichthe personal data is processed needs to consider the different operations during which the police is processing data.

The police should apply at all stages of the processing the relevant data protection principles (most importantly the principles of necessity, proportionality and purpose-bound data processing), and should not continue to process data which are not needed for the purposes. In this context, personal data collected at an early phase of the investigation, which then proves with the process of the investigation to be no longer relevant should no longer be processed (e.g. innocence of a suspect is confirmed), and should therefore either be blocked or deleted. This does not apply where subsequent use of the data is allowed.

Prior to and during the collection of such data, the question of whether the personal data collected is necessary for the investigation or for a task of the police as described in Point 1, should always be considered. One should note that once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific task of the police) should exist. This link together with compliance to the data protection principles as described in the Guide, must be demonstrated at all times. After the collection phase and at different stages of the investigation, a thorough analysis is needed to assess which data are to be retained and which are to be deleted.

Before collecting any personal data, investigators should ask themselves the question 'Why is it necessary to acquire the data?', 'What, exactly, do you seek to achieve?'.

Example – For personal data such as Telephone Billing: only the number(s) required for the time periods being investigated should be sought and only for those individuals suspected of having a link with the offence.

A list of phone numbers of the person(s) involved in the suspected offence can be collected if there are indications that such data serve the purpose of the investigation. It cannot be kept or processed after the analysis shows that the data are not strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for police purposes should be used for those purposes only and should not be used in any other way that is incompatible with the original purpose stated at the time of collection, unless this is provided for in law (see Art 9 of Convention 108) [In assessing the compatibility of the use of data for the same purpose, one should consider the following criteria: (i) relation between purposes; (ii) context of the collection and information given to data subjects; (iii) nature of personal data; (iv) consequences for data subjects of the intended subsequent use; (v) existence of appropriate safeguards.]

Subsequent use of data is considered for the purposes of this guide as a new data processing operation which has to fulfil all the criteria and conditions mentioned above. The subsequent use of data shall be lawful, undertaken for a legitimate aim and necessary and proportionate to this legitimate aim.

Deleted:
Deleted: and
Deleted: where personal data is processed
Deleted: therefore
Deleted: it can be
Deleted: held
Deleted: has to be reiterated that according to
Deleted: during
Deleted:
Deleted: The collection and use of personal data for law enforcement purposes can constitute an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and as such it *must* be based on law (clear and publicly available), pursue a legitimate aim and be limited to what is necessary to achieve that legitimate aim.
Deleted: P
Deleted: e
Deleted: n
Deleted: (law, consent, contract, vital interest of the individual, etc.)
Deleted:
Deleted: (e.g.: for testimonies consent seems to be adequate, but for cross-checking data in different data base legal provisions must exist). Legitimate data processing implies that the ...
Deleted: P
Deleted: -
Deleted: ,
Deleted: principle
Deleted: they should be
Deleted: permanently
Deleted: specific
Deleted: asked
Deleted: prnciples
Deleted: During collection, provided ...
Deleted: in order
Deleted: Police should apply the da ...
Deleted: the relevant people.
Comment [A26]: Previous version ...
Deleted: in law
Deleted:).
Deleted: use
Deleted: applicable to the collection ...

The police shall ensure at all stages of the data processing and for the subsequent use of data as stated in the General considerations that the personal data are accurate, up-to-date, adequate, relevant and not excessive in relation to the purposes for which they are processed.

Example: Police data collected for an investigation where the political affiliation is irrelevant, cannot then be used to determine the political affiliation of the concerned person unless provided for by law.

3. Subsequent use of data

Every subsequent processing of data by police (irrespective of the purposes of the original processing) for police purposes other than that the data were originally collected for, must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be undertaken for a legitimate aim and should be necessary and proportionate to the legitimate aim pursued.

Personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set out in Point 2. The general rule is that if data are likely to be used in a different case or in a different operation of the police, the assessment of compliance described in Point 2 shall be applied to this new processing as well. (This is not applicable if data are used for purely statistical or scientific purposes). Due to computerised and/or automated data processing and the large volume of personal data stored very often in different processing environments, the personal data collected and retained for police purposes should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

It should be noted, however, that any subsequent use of personal data of vulnerable individuals such as victims, minors, or of those enjoying international protection, should be subject to additional care and legal analysis with a special attention to the application of the principles of necessity and proportionality.

In cases such as trafficking in human beings, drug trafficking or sexual exploitation, where victims' data may subsequently be used also when they are considered as suspects, or where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to look at existing international good practice (in international or regional police bodies) and to enhance their exchange of information on the matter with other national police bodies. If all legal requirements as put forward in Point 2 are met, it should not represent any obstacle to the use of data of these persons for police purpose, but during these exchanges, confidentiality rules have to be followed.

Example - Data taken for tax purposes from a data subject can only be processed for law enforcement use by police () if the law allows it, if they are used for a legitimate aim and in a way that is necessary and proportionate to the aim pursued. In a concrete investigation of money laundering, the use of tax declarations' data of an individual can be envisaged to establish or deny a link between the individual and the money laundering operations.

4. Processing of special categories of data (sensitive data)[16]

Special categories of data, such as genetic data, personal data related to offences, criminal proceedings and convictions and related security measures, biometric data uniquely identifying a person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical nature, for instance additional security measures, and of an organisational nature, for instance having such sensitive data processed separately from the processing environment of the "ordinary" categories of data. Safeguards should be adjusted to each data processing operations taking into account their specificities and it is highly recommended to use multiple levels of protection for those categories of data (e.g.: separate main-frames, shorter data retention periods, etc.). It is of paramount importance to prevent unauthorised or unwanted access to those categories of data even with additional security measures.

[16] Paragraph removed from previous Point 8

Deleted: ¶
¶
Deleted: fact that the original processing has been carried out for a police purpose or for other purposes
Deleted: ~~same~~
Deleted: Due to the nature of data processing, it is possible to use personal data collected for one purpose for another, personal data collected and retained for police purposes should not be kept and processed in an unstructured manner unless there is a legitimate interest, a legal basis and operational reason within the legal powers of the police for this. This means that p
Deleted: specific, well-defined
Deleted: point
Deleted: a
Deleted: for
Deleted: the
Deleted: tests
Deleted: .
Deleted: all data held by police should have a link to a case or specific mission of the police and should be processed in relation with this
Deleted: isz
Deleted: the
Deleted: nature of data processing, it is possible to use personal data ...
Deleted: in an unstructured manne ...
Deleted: data, in particular in respe ...
Deleted: which shall include ...
Deleted: ,
Deleted: other
Deleted: This
Deleted: does
Deleted: if all legal requirements as ...
Deleted: .
Deleted: Biometric d
Deleted: immigration medical
Deleted: such as checks against ...
Deleted: allows
Deleted: it and appropriate ...
Deleted: Any such use should be ...
Deleted: The purpose of appropriat ...
Deleted: of
Deleted: its
Deleted: anonimisation,

A careful balance of interests taking into account the purpose of the investigation, the context and the nature of the data is necessary to determine whether or not, and to which extent, the police could process sensitive data. For instance, it would be advisable to differentiate when biometric data is processed by the police whether it is for identification purposes (where for instance 2 fingerprints could suffice) or it is for crime investigation purposes (where more fingerprints could be needed).

The use of Data Protection Impact Assessments (DPIA) is recommended in order to ensure that appropriate safeguards are put in place. The data controller should assess and demonstrate whether the purpose of the processing can be achieved in a manner that impacts less on the right to privacy and data protection and if the processing of special categories of data does not represent a risk of discrimination for the data subject.

Regarding these data the potential risk of negative discrimination or of adverse legal effect significantly affecting the data subject should be avoided, since all profiling based on sensitive data resulting in negative discrimination are prohibited. In this context, besides measures detailed above, the use of PETs and more frequent checks on the lawfulness of the processing can be recommended. This could, for example, translate into measures put in place to counter the assumption that individuals belong to a criminal organisation because of where they live, where a criminal organisation is active or where the individuals have the same ethnic origin.

Example - Targeting groups or individuals based solely on religious beliefs would not be allowed. However, in an investigation into a group of individuals engaging in possible terrorist activities that were attached to a particular religious group, it could be of importance to process data specific to the followers of this specific religious group (related to worshipping place, religious preachers, customs, teachings, members and structure of the religious community, etc. that was pertinent to the investigation). However, targeting all followers of a religion, purely because of their religious belief is strictly prohibited.

5. Providing information to data subjects

One of the most important obligations of a data controller is to provide information on data processing to data subjects. This obligation is two-fold: it requires the data controller to provide *general information* on the data processing that it carries out and to give *specific* information to data subjects if no restrictions or derogations apply to the data processing.

Information provided to the wider public, should promote awareness, inform them of their rights and provide clear guidance on exercising their rights regarding these files. The information provided should be effectively and broadly accessible. Moreover it should include details about the conditions under which exceptions apply to the data subject's rights and how they could submit an appeal to the DPA or to the judiciary.

Websites and other easily accessible media perform a role in informing the public. It is recommended to have in place letter templates on these websites or other media to help the data subjects exercise their rights. It is the responsibility of the data controller to provide information which adequately highlights data protection and data subjects' rights.

In order to comply with the second obligation of giving data subjects specific information regarding data processed, the police shall inform data subjects on the data processing envisaged or, if it is not possible, before the processing for objective reasons, shortly after it. This communication shall comprise information on the data processing, on the collection of the individuals' data and comprehensive information on their rights.

The obligation to provide specific information implies that, in principle, the data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.

Deleted: which takes
Deleted: can
Deleted: on the top of personal criminal data
Deleted: 8 to 10
Deleted: would
Deleted: A greater
Deleted: the
Deleted: adequately
Deleted: (i.e. tasks of the police)
Deleted: of the data subject
Deleted: as
Deleted: which
Deleted: a
Deleted: pseudo-anonymisation,
Deleted: legitimate
Deleted: (of these data
Deleted: can
Deleted: are from
Deleted: al
Deleted: There should be additional ...
Deleted: to
Deleted: they were members of that ...
Deleted: would
Deleted: be
Deleted: It should be noted that t
Deleted: ;
Deleted: prior
Deleted: and *upon request* on the ...
Deleted: The *general obligation* ...
Deleted: The i
Deleted: in respect of broader ...
Deleted: in general
Deleted: Information provided
Deleted: can
Deleted: against a decision of the ...
Deleted: as best practice
Deleted: in
Deleted: ing
Deleted: In respect of making ...
Deleted: According to the second ...
Deleted: this obligation
Deleted: it envisages undertaking
Deleted: undertook in relation to ...
Deleted: If there are objective ...

The information should be provided unless a restriction or derogation applies as described in Point 7 taking into account the specific nature of sensitive files, such as criminal intelligence files, files containing sensitive data, in order to avoid serious prejudice to the performance of police functions, or to the rights of individuals. Even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.

Very often data subjects, because of restrictions or derogations of their right to information, cannot receive complete information on the processing the police undertake with their data; this should not affect their exercise of the right of access.

Example - For the purpose of covert monitoring of a high risk sex offender, data processing and long-term data retention may be justified without informing the individuals under surveillance if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved, the data subject should be informed about the fact that she or he was subject to such measure.

6. Data subject's rights[17]

Accessing their personal data is a fundamental right for data subjects.
The right to information on request, the right of rectification and the right of erasure are interdependent rights.

The police [in principle] has to inform the individuals on the data processing activities carried out with their data. This means that in case an individual has her/his data collected during the course of an investigation or other tasks of the police as described in Point 1, as soon as circumstances safely permit, the police [in principle] should inform the individual of the data processing if there is such request. The information should be given upon request as soon as data are processed, for instance at the time of collection and it should be provided in clear and plain language. The communication has to contain the same information as described in point 5, unless data subjects wish otherwise.

The law can provide, under the strict conditions described in Point 7, that the right to be informed upon request may also be limited or excluded, should the provision of such information prejudice the investigation, or another important police task, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified.

The police should aim to answer even general questions arising from data subjects on the processing activities in relation to their personal data, but can use standardised forms to facilitate communication.

Example: If a data subject asks the police on data it processes on them, the police, if no exception is applicable, should provide a detailed answer with legal references, but should do so in a plain language, avoiding uncommon or specialised expressions.

The right of access should, in principle, be free of charge.

It is possible to charge a reasonable administrative fee for the request, if national law permits and the request is manifestly unfounded or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such refusal.

To ensure a fair exercise of the right of access, the communication "in an intelligible form" applies to the content as well as to the form of a standardised digital communication. It is, however, advisable to refer to national legislation to ensure consistency and to avoid suspects utilising this method to find out whether there is an on-going investigation into them.

[17] Paragraph removed from previous Point 17.

Deleted: of
Deleted: , etc
Deleted: police in performing theirits functions
Deleted: is
Deleted: t
Deleted: ing
Deleted: any more
Deleted: ¶
Deleted: a
Deleted: the
Deleted: in relation to their personal data
Deleted: , the right of access
Deleted: The right to access is a prerequisite for the exercise of other rightsinformation covered under Point 5 is a prerequisite to right of access; the data subject has the right to know about the data processing which is made on theirpersonal data and on the basis of this information, exercise other rights. It shall be noted nevertheless that there is no systematic link between access rights and the data controller's obligation to inform data subjects in specific cases *ex officio* or *upon request*. As a rule domestic law should, ideally, provide for direct access.
Deleted: ¶ ¶
Deleted: also
Deleted: as
Deleted: providing
Deleted: , for instance
Deleted: Very often data subjects, because of restrictions or derogations can not receive full information on the processing the police undertake with their data, it should exclude full exercise of their rights of access.¶ ¶
Deleted: P
Deleted: the
Deleted: using
Deleted: a
Deleted: of approach

In respect of direct access, the data subject can request access to the controller of the files. The data controller will assess the request and any possible restriction or derogation which can only be used if it is vital for the performance of a specific police task as described in Point 1, or it is necessary for the protection of the data subject or the rights and freedoms of others, and reply directly to the data subject. In case of a restriction, partial information, and in case of derogation, information on the use of derogation, shall be still given, with the motivation for using such measures in both cases, as well as information concerning redress.

Example: The access request can be refused if there is an on-going investigation on the person, and providing the data subject access to the data could compromise such investigation.

If restriction or derogation were to be used, any answer should take into consideration, according to national law or practice, all circumstances to which the restriction or the derogation is applicable.

As a rule, domestic law should, ideally, provide for direct access. If the right of access provided for is indirect, the data subjects may direct their request to the supervisory authority, which after being properly mandated, will carry out the request on their behalf and conduct checks regarding the availability and lawfulness of the processing of the data subject's personal data. The supervisory authority will then reply to the data subject (providing what data it is possible to release, subject to any legally allowed restrictions or derogation). In case of a restriction or derogation, the same communication should be made possible as in case of a direct access.

The data controller should assess the request and reply to the data subject within a reasonable time limit, as provided for by domestic law.

There should be arrangements in place to confirm the identity of the data subject before access to any data is granted as well as to obtain information on the processing activities to which the request refers. The same holds if the data subjects delegate the authority to someone else to exercise their rights.

It is an essential right of the data subjects to be able to amend any incorrect data held on them. If the data subject finds data that are incorrect or irrelevant, she/he should have the right to challenge it and ensure that they are amended.

In some cases, it may be appropriate to add additional or corrective information to the file. It is important to underline that this right can only be exercised with due respect to other individuals' rights, for instance to the rights related to a testimony in a criminal case (which does not preclude per se the exercise of the data subjects' rights related to soft police data).

If the data to be corrected or erased has been communicated elsewhere the relevant authorities should be informed of the changes to be made.

All proposed changes should be supported by evidence. If data subjects can prove by use of the official documentation that the data processed by police in respect to them are incorrect, the data controller shall not have the right of discretion whether to correct them.

It may be necessary for the police, as dealt with under Point 7, not to give information or grant the right of access, of deletion and of correction which might jeopardise an investigation and should therefore be excluded for its duration. Similar restrictions or derogation may be imposed by national law as described in Point 7.

Restrictions or derogations to the rights of data should only apply to the extent necessary and be interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis. Any decision to refuse a data subject's request should be provided in writing (including by electronic means). The response should provide clear justification of the decision making which can be verified by an independent authority or a court. It is possible that communicating the reasons for refusal could pose a risk to law enforcement or the

Deleted: of the police

Deleted: the

Deleted: s

Deleted: ,

Deleted: excessive

Deleted: or deleted

Deleted: Data subjects can ask for the deletion of their personal data where such processing is unlawful. ¶

Deleted: of

data subject or to the rights and freedoms of others. If this is the case, it should be documented and provided to the independent authority or court to be verified, if required.

Example - If person A submitted a declaration against person B accusing her/him of committing a serious offence and later it emerges that the accusation was false, it might be relevant for the police to retain the false statement and the information surrounding it.

Although the statement was proven to be false, if the police needs to retain the data in the interest of the investigation for instance, a clear corrective statement on the file, instead of removing the false statement, would be necessary.

The data subject should be informed of all available options following a refusal decision such as an appeal either to the supervisory authority, to court or to another independent administrative authority.
Depending upon national legislation, specifically whether there is a direct or an indirect right of access, the actual communication of the result of the review or appeal may differ. It is possible that the inspecting body cannot communicate the data to the individual even if there is no justification for refusing access. In this case the data subject should be informed that a verification of the police file has taken place. Alternatively, the inspecting body may request the police to release the data contained in the file to the data subject. The court or tribunal may have powers to enforce the access, correction or deletion of data from the file even in access-request cases referred to them by police or the supervisory authority.

Example: If police sends a refusal letter it should contain the name, address, web address, etc. of all possible forafor redress.

The data subject should have access to a court or tribunal in order to submit an appeal, and have the reasons for refusal verified if they are not satisfied with the reply given by the supervisory authority or the independent authority. The supervisory authority should have sufficient powers to examine the police file concerned and have the assessment communicated.

7. Exceptions from the application of data protection principles

Under the European Convention on Human Rights and Convention 108, exceptions can only be used if foreseen by law (the law should be public, open and transparent and, in addition, detailed enough) and they constitute a necessary and proportionate measure in a democratic society.

The exceptions which have to be incorporated into national legislation should serve a well-defined purpose.Exceptions can be applicable to those principles described under Points 2,3, 5 as well as to the data subjects' rights (Point 6) in case of some specific purposes in relation to which data processing activities are undertaken. In particular they concern, activities undertaken for the purpose of the protection of national security, defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest (which includes purposes in connection with the fulfilment of a state's international legal commitments or obligations, most prominently deriving from the binding decisions of United Nations' bodies, and humanitarian purposes,) or the protection of the rights and fundamental freedoms of others.

Example - If giving information to a data subject may endanger the safety of a witness or an informant; this right can be limited in light of such circumstances.

If the exception, as defined by national law providing specific safeguards is used by the police, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. The aim of using exceptions by the police should be limited to cases where the use of those rules and principles would endanger tasks of the police described under Point 1.

Example: If data collected for police purpose in an investigation are likely to serve national security purposes they can also be used to this latter purposes to the extent set forth by national legislation. If specific

Deleted: ¶
A data subject may be required, as per national legislation, to obtain a copy of their police file. However, to obtain a written copy or statement may not always be in their interest or feasible for the police and therefore in such cases domestic law may authorise oral communication of the contents.¶

Deleted: requires the retention of retaining the data

Deleted: um

Deleted: <#>¶

Deleted: should be

Deleted: exceptions

Deleted: and have to be incorporated into national legislation in a manner compatible with the ECtHR jurisprudence

Deleted: ¶
¶

Deleted: p

Deleted: 4

Deleted: 7

Deleted: p

Deleted: 17

Deleted: it

Deleted: affects

Deleted: s

Deleted: those

Deleted: from international

Deleted: obligations

Deleted: ,

Deleted: Other applicable exceptions are foreseen in Article 3 Convention 108.

Deleted: ¶

Deleted: ,

Deleted: based on

Deleted: the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police

Deleted: ¶

Example - If giving information to a data subject may endanger the safety of a witness or an informant; this right can be limited in light of such circumstances. ¶
¶

Example: Police data, if explicitly provided for by national law can be shared in compliance with stringent conditions set forth by the national law with national security agencies in respect of national security, for ...

intelligence proves that money laundering operations have been carried out to finance terrorist operations, data collected on individuals during the investigations on money laundering can be used for the purpose of eliminating the close and imminent terrorist risk.

8. Use of special investigative techniques

The police should always adopt the least intrusive means of data processing during its operations. If less intrusive methods can be used to achieve the desired ends, they should be preferred. The use of special investigative techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods. Regardless of the method of investigation or other operation led by the police, the police is obliged to comply with the general principles of data protection as described in General considerations, unless a law expressly exempts from it.

With increasingly sophisticated technological developments, electronic surveillance has become easier, however, the use of these techniques interferes with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the high potential of severe interference with the right to privacy has to be balanced with the efficiency of investigations.

Example: In an investigation, the evidence for communication between two suspects can be gathered in various ways. If, by the use of interrogations, testimonies, the obtaining of call data or discreet surveillance, the same result can be achieved without jeopardising the effectiveness of the investigation, it is to be preferred to the use of more intrusive surveillance measures, such as wiretapping.

9. Introduction of new data processing technologies

If the introduction of new technologies is likely to result in a high risk to the individual's rights, the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity. The relevance of the DPIA shall be checked at reasonable intervals.

It is also of great importance, that in terms of data security and safety of communications, the highest standard is taken into account when introducing such technologies.

Example - New data mining techniques may offer extended possibilities for identification of possible suspects and should be assessed carefully for their compliance with existing data protection law, including with regard to data security.

The data protection authority has an important role in advising which risks are involved for data protection and which safeguards should be provided to ensure that any technical means comply with data protection law. However, the police do not have an obligation to turn in every case to the supervisory authority where it introduces new technologies. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights.

The consultation between the supervisory authority and the data controller should provide the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.

Appropriate details should be provided to the supervisory authority, in particular regarding the type of file, the data controller, data processor, the legal basis and the purpose of the data processing, the type of data being processed and by whom the data is being accessed, as well as information on retention of data, log policy and access policy, and other relevant technical aspects of implementation.

Example: Detailed information on national reference files such as purpose, data controller etc. containing

Deleted: ¶
Other applicable underlying proposes for exceptions are foreseen in Article 3 of Convention 108.¶

Deleted: it must be remembered that

Deleted: can

Deleted: those considerations

Deleted: have

Deleted: cost-effectiveness, use of resources and

Deleted: covert

Deleted: Use

Deleted: It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance to existing privacy and data protection standards. It is also of great importance, that in terms of data security and safety of communication, the highest standard is taken into account when introducing such technologies.¶

Deleted: processing

Deleted: continuous (i.e.

Deleted:)

Deleted: should

Deleted: every

Deleted: by

Deleted: or the national legislation does not provide sufficient clarity on the implementation of these methods

Deleted: be defined in a way that

Deleted: s

Deleted: During the process with the supervisory authority the focus should be on mitigating the specific negative impacts that the data processing would represent to the right to privacy and to data protection.¶
¶
The consultation between the supervisory authority and the data controller should be defined in a way that provides the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.¶
¶
During the consultation process appropriate

Deleted: contained

Deleted: important

fingerprint data could be reported to or made available for consultation to the data protection authority.

Following consultation, the data controller should consider carefully to implement any necessary measures and safeguards that have been recommended by the data protection authority.

Example - Introducing an automatic facial recognition system or other system based on the automated processing of biometric data would be very likely to need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed and recommended by the data protection authority after being consulted on the issue, specific safeguards should be put in place (concerning the data retention time, the cross matching functionalities, the place of the storage of data and the access to data issues, etc.) to comply with data protection principles and provisions

Use of the Internet of Things (IoT) technology in police work

Data sent to and from police during operational activity via the internet are good examples of the IoT already in use. Due to potential security vulnerabilities, IoT requires measures such as data authentication, access control to ensure data security and resilience to (cyber) attacks.

Example: In light of their potential security vulnerabilities, smart glass used by police should not be directly connected to a national criminal record data base and data collected should be guaranteed a high level of security.

Big data analytics in the police

Technological advances in processing and analysing large and complex data sets leading to big data and big data analytics present opportunities and challenges to the police, who is turning to digital sources and profiling techniques to perform their tasks.

Big data technologies enable bulk collection and analysis of a vast quantity of data generated by electronic communications and devices aggregated with other bulk data. This could interfere with the right to privacy and data protection.

The Council of Europe's Recommendation CM/Rec(2010)13[18] on the protection of individuals with regard to automatic processing of personal data in the context of profiling and the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[19] can be of use in the context of Big Data analysis for police use too.

Big data technologies and analysis techniques may help assist detecting crime, but there are, however, considerable risks to this type of data processing that should be taken into account:

- Databases originating from one domain can be used in another domain and for another purpose, which changes the context and may lead to inaccurate conclusions and lack of valid legal basis, therefore to unlawful data processing with possibly serious consequences for the individuals involved.
- Profiling may lead to drawing discriminatory conclusions, which can result in the reinforcement of stereotypes, stigmatisation and discrimination.
- The increasing amount of personal data held in databases may lead to severe vulnerabilities and subsequent risk of data breaches if information security is not guaranteed.

Where big data relies on personal data, data controllers should pay additional attention to the following requirements:

[18] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[19] Document T-PD(2017)1 - Big Data Guidelines

Deleted: are to

Deleted: Data protection authority is preferably to be consulted during the legislative procedure.

Deleted: which is directly linked to relevant databases

Deleted: ; they should gather information which is to be downloaded to a secure IT environment for further analysis

Deleted: *and profiling*

Deleted: are

Deleted: legal

Deleted: way of processing data

Deleted: potentially and inadvertently

Deleted: ¶

Deleted: take

Deleted: due account of

- Verification of data accuracy, context and relevance of the data.
- Its use requires a high level of accountability.
- Its use shall be combined with methods of investigation which complement the conclusions drawn. A decision affecting a person shall not be taken solely on automated processing of personal data.
- As for other types of data processing, it is of paramount importance that its use shall be ~~shall be be~~ necessary and proportionate for the fulfilment of police tasks described in Point 1, with special attention for the data processed to be adequate, relevant and non-excessive in relation to the purpose for which they are processed.
- Predictive analysis requires human intervention to assess the relevance of the analysis and conclusions.
- Ethical guidelines developed at national or at international level should be taken into consideration.
- As a principle and subject to restrictions and derogations mentioned in Point 7, transparency should be ensured by the data controller by explaining how the data are processed in accordance with privacy and data protection principles. If data collected for one purpose is used for another purpose, the data controller should in principle make the data subjects aware of this subsequent use.
- Even if complex methods are used, the lawfulness of the processing – including subsequent use of data - and compliance with the conditions set by Article 8 ECHR and Convention 108 should be demonstrated.
- An information security policy should be in place and implemented throughout the processing.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals and the administrative and judicial means exist for individuals to challenge those decisions. This implies data subjects' awareness of the reasoning of the algorythm used and the purposes for which it was used.

The above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones, are even more necessary when sensitive data are processed in Big Data analytics.

10. Storage of data

"As pointed out in Point 2" data shall be processed until they have served the purpose for which they were collected. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

There should be a clear distinction in how the police stores and processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses. This should also relate to the specific purpose for which the data was collected. Additional safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence. Clear rules have to be established in relation to the handling of different data bases with special attention to the analysis of multiple results.

The principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve the purpose of the prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where personal data is processed for the purpose of the maintenance of public order.

The grounds for retention and processing should be reviewed periodically. The unlawful processing of personal data outside of the legal framework allowed for the retention constitutes a severe violation of the right to protection of personal data. If the law in relation with a specific crime provides for a data retention period of 4 years and if an individual is kept in custody by the police solely on this ground after 4 years have passed since the collection of the data in question and no legal ground to process this data exists, the retention of this data could be considered as unlawful.

General data retention periods are usually regulated in national or international law. In order to comply with the legislation while ensuring the effectiveness and the success of an investigation police bodies are strongly advised to develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data.

Deleted: traditional less intrusive other
Deleted: to
Deleted: such
Deleted: ized
Deleted: l
Deleted: use
Deleted:
Deleted: purpose
Deleted: notably
Deleted: Where possible
Deleted: provided
Deleted: compatible
Deleted: secondary
Deleted: and/or lengthy processing are undertaken L
Deleted: be
Deleted: allow the data subjects to know the
Deleted: ensure transparency
Deleted: h
Deleted: for to avoid any negative discriminatory action
Deleted: If data are no longer relevant for the purpose collected, they should be deleted, unless subsequent processing is possible on the grounds put forward in Point 3. S
Deleted: s
Deleted: S
Deleted: queries in
Deleted: can
Deleted: and evidence gathered in this way can be seen as unlawful
Deleted: retained
Deleted: , 4 years later the evidence based solely on
Deleted: and the measures undertaken by the police based solely on this data
Deleted: possibly
Deleted: by the court

For example, in a case where the law prescribes a 4 year data retention period but the individual subject to an investigation is acquitted from all charges by the court after 2 years, her/his data shall be deleted (if the individual is not a recidivist or there is no information on her/him committing again the same category of crime) from the database, provided that all deadlines for the review of the case have expired. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judicial procedure terminates completely (which means all redress have been made or all deadline for redress have been passed).

The police should provide systems and mechanisms to ensure that the data that are stored are accurate and that their integrity is maintained.

International obligations, which include providing data to international bodies such as Europol, Eurojust and INTERPOL, bilateral agreements and mutual legal assistance between member states and third countries must be observed when shaping internal policies.

Data should be categorised according to the degree of accuracy and reliability in order to assist the police in their activities. It is recommended that handling codes are used to distinguish these categories. A classification system facilitates the assessment of the quality of the data and how reliable it is. Classification of data is also important when it is to be communicated to other police bodies or states.

Example - Information collected directly from a person's statement will be assessed differently than information collected from a person's hearsay statement. Data based on facts, or 'hard' data, will be assessed differently than data based on opinions or personal assessments, or 'soft' data.

Personal data collected by police for administrative purposes must be kept (as far as possible: logically and physically) separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by law.

Examples of administrative data include lists of data on licence holders or data on human resources and firearms certificates.

11. Communication of data within the police sector

A distinction should be made between domestic communication of data and international transfer of data. Within these two distinct operations different requirements apply, depending upon who is receiving the data, whether it is the police, another public body or a private party. The police can only communicate personal data within the police sector if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

There should be clear and transparent rules on how the police grant access to data held by it and on which grounds.

The police, domestically, should only share information (among police) when there is a legal basis for the request, e.g. an on-going criminal investigation or a shared law enforcement task and laws or agreements allowing the communication

The police can share data with other police organisations if the personal data are relevant for the purpose of prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where they are processed for the purpose of the maintenance of public order.

The communication of personal data in general should be in line with the general considerations described above.

Deleted:

Deleted: revision

Deleted: also

Deleted: the

Deleted: of the data

Deleted: When shaping internal policies i

Deleted: This uses a

Deleted: to

Deleted: if feasible

Deleted: the

Deleted: ent

Deleted: As a general rule p

Deleted: that

Deleted: is

Deleted: personal data

Deleted: is

Deleted: subject to the principle of necessity and proportionality and has to serve the above mentioned purposes

Deleted: G

Example: A police unit can share data on a suspect who presumably committed a tax fraud with another police unit investigating a murder case if there is indication that the suspect for this crime could be the same person or if doing so will materially assist the investigation.

12. Communication of data by the police to other public bodies

The communication of data outside police is permissible if it is provided for by law and the data are required by the recipient to enable them to fulfil their lawful task. Mutual assistance agreements foreseen by the law between law enforcement and public bodies allows the public bodies to have access to law enforcement data which would be essential in the fulfilment of their duties and tasks (for example in their investigations or other legal duties in accordance with national law).

Stricter principles than those set forth in Point 11 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the processing of personal data, which are considered sensitive, could result in adverse effects for the individual.

Communication of data to any other public authority may also be allowed if it is foreseen by law, is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to other persons or to public order or to public security.

The communicated data may only be used by the receiving body for the purposes for which the data were transferred.

Example - A claim for a residence permit made by a migrant. Police data may be required to verify if the person was ever involved in criminal activity. It would be in the interest of the Immigration Office and the claimant for this communication of data to take place.

13. Communication of data by the police to private parties

There may be occasions when, under strict conditions, the police can communicate data to private bodies. This communication has to be based in law and can only be done by the authority which is processing the data. Such communication can only be done for the purpose of the investigation or other important police tasks as described in Point 1, in the interest of the data subject, for humanitarian reasons or if it is necessary to prevent serious and imminent risk to public order or public security. For example, there might also be instances where police data may be communicated to humanitarian organisations based on international law, in the interest of the data subject or for humanitarian reasons.

Where the police shares data with media in respect of making information related to an investigation public, special consideration should be given to the assessment to determine that it is necessary and in the public interest that such publicity is allowed.

Such communication should only be on a case by case basis and in each case there must be a clear legal basis providing the necessary procedure (e.g. need for specific authorisation) to be followed for any such communication to occur.

Example - When the police communicate with the financial sector in relation to known fraud or theft offenders, when it communicates with an airline about stolen or lost travel documents or when the police releases details of wanted persons believed to pose a risk to the general public.

14. International transfer

Deleted: is

Deleted: m

Deleted: 0

Deleted: criminal

Deleted: the communicated data

Deleted: be used for non-law enforcement purposes

Deleted: negative discrimination

Deleted: against

Deleted: In practice detailed ¶ ¶ As an exception, c

Deleted: as

Deleted: missions

Deleted: which should

Deleted: e

Deleted: they

Deleted: wanted who are

Any transfer of police data internationally should be limited to police bodies and should be fit for purpose and in accordance with the law. For this, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data handling, regional legal frameworks such as EU and EU institutions' legislation (on Europol, Eurojust, Frontex, etc.) and subsequent agreements (operational bilateral agreements), bilateral treaties and in general, international agreements on mutual assistance, or other bilateral or multilateral agreements made regarding effective cooperation can be of use.

When considering sharing any data, consideration should be given as to whether the receiving authority is performing a function conferred to it in law related to the prevention, investigation, or prosecution of criminal offences, the execution of criminal penalties and the maintenance of public order, and whether the sharing of the data is necessary to perform its specific task.

The sending authority should ascertain that there is an appropriate level of data protection in the receiving state and that the receiving state complies with the relevant rules of international transfers of personal data. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. This means of transfer should be used as a last resort option. International transfers framework such as "INTERPOL's Rule on the Processing of Data" and its "Statute of the Commission for the Control of INTERPOL's files" Rules on the Control of Information and access to INTERPOL's Files", the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185) may be taken into account[20] so as to ensure that any transfer of data is legally justified and has appropriate safeguards in place. The request should clearly state all the necessary elements from the requesting party to enable the receiving party to make a sound decision on the request. These details would be expected to include the reason for the request as well as the purpose for the transfer of data.

An appropriate level of data protection should be guaranteed (e.g. through ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments) if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

If there are conditions applied by the sending authority in relation to the use of the data in the receiving state these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout its lifecycle.

Example - Further transfer of data should only be allowed if this is necessary for the same police purpose as the original transfer and the second recipient is also a police body ensuring an appropriate level of data protection. The police body which originally sent the data must also consent to the onward transfer. If the police from country X sends personal data to the police of country Y it is only permissible for the country Y to transfer this data if above all requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) if country X consents to the transfer. If the data is sent to country Z which is a non-member of the Convention 108, then country Y should ascertain that this country provides an appropriate level of protection of personal data and effective means of exercise of the related data subject rights.

The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases if it is required for the performance of the task of the transferring authority and there is no effective means of transferring the data to a police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers.

Example: If tax authorities in country X requests the police in country Y about the whereabouts of a person involved in non-criminal tax evasion because they have evidence that the person is involved in criminal matters in country X, the police can transfer the personal data of the individual.

[20] This is without prejudice to the right of the Committee of Convention 108 and other instances disposing such power to assess and to review if necessary the level of data protection guaranteed by those multilateral agreements

Deleted: organisations

Deleted: contained within its legal framework

Deleted: ,

Deleted: in respect

Deleted: Interpol's "Rules Governing the Processing of Data

Deleted: can be applicable

Deleted: in place

Deleted: to

Deleted: its

Deleted: onward

Deleted: specific

Deleted: with

Deleted: has, in place, appropriate legal protection in terms of personal data processing and can guarantee an

Deleted: level for the

Deleted: it has

The international transfer of personal data between police and private bodies in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police as described in Point 1, provided by legal means and where the emergency, the gravity of the crime, its trans-border nature and where the involvement of the local police would compromise the purpose of the investigation for objective reasons. Other facts as data security, the reassurance received as to the use of the data and the lawfulness of the data transfer in the receiving country have to be taken into account. In this context it is to be noted that in such a case, the data controller has a double obligation with respect to the protection of personal data: one imposed by the legal framework of the country where it resides and the one which is related to the data transfer. The local police should be informed afterwards. The police are required, wherever possible, to make use of existing international legal instruments, in respect of this type of data transfer. International transfers may also exceptionally occur where the police communicates personal data for humanitarian purposes.

Example: In an investigation, carried out within the framework of an international multilateral agreement, into child sexual exploitation where the victim is in country Y and the police there have commenced an investigation, and the material has been made available on the internet by the suspect residing in another (country X) and there is a high risk that the suspect seeks to avoid justice by fleeing country X, the police in country Y can request, on an exceptional basis, that a service provider in country X provide the whereabouts of its customer. However, the police of country Y should inform the police in country X of its operation as soon as is possible and then seek to resolve the matter in cooperation.

15. Conditions for communications

Since there is a general obligation for the data controller to ensure a high level of data quality, it is advisable to have in place an additional check before sharing the data with others. When communicating or transferring data, it is always advisable to double-check the quality of data, if it is correct, up-to-date and complete. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated. It is required to establish secure channels of communication which ensure data security at the highest level possible. The quality of data can be assessed up to the moment of communication.

Example: If personal data that contain incorrect data (personal or otherwise) are sent they could adversely affect the investigation, cause harm to the individual concerned or others involved, or who may become involved as a result of the incorrect data being transferred. This can, as a result, leave the police in the transmitting and receiving states open to civil redress. In essence, if an individual is arrested based on a wrong communication of the suspect's name, it seriously harms several human rights of the individual concerned and can undermine any criminal investigation.

16. Safeguards for communication

It is of utmost importance that the necessity and purpose limitation principle should be applicable for any domestic communication or international transfer of personal data outside of police organisations.

Any data communicated should not be used for anything other than the purpose for which it was sent or received. The exceptions to this are when the sending authority, based on legal provisions, gives agreement to any further use, and if it is necessary and vital for the recipient to fulfil their task. Data can also be communicated if it is in the interest of the data subject for humanitarian reasons, is necessary to prevent serious and imminent risk to public order or public security or an appropriate level of data protection is guaranteed by the recipient by international, national legal instrument, ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments, as foreseen by Convention 108.

Example: Personal data sent by the police of country X to the police of country Y in a money laundering case cannot be used by the police as profiling on the given individual in respect of her/his religious beliefs or political activities (unless those are relevant to the crime committed and police in country X has given its consent for this use).

Deleted: police

Deleted: to

Deleted: a

Deleted: y

Deleted: residing

Deleted: the

Deleted: the fact that

Comment [A27]: Our comment has been partly taken into account but the presentation of the involvement of the police as a 'hindrance' in an investigation does not seem to be the appropriate wording to us.
The sentence could be shortened in a way such as "the involvement of the police would not be possible for objective reasons."

Deleted: because of the length of the procedure

Deleted: As

Deleted: or transferring

Deleted: ,

Deleted: and data based on opinions or personal assessments cheked at source before being communicated and their degree of accuracy or reliability indicated

Deleted: seems

Deleted: to be preferable

Deleted: transfers

Deleted: is sent

Deleted: s

Deleted: it can

Deleted: the

Deleted: only

Deleted: is

Deleted: and if the processing is based on law,

Deleted:

Deleted: safely

Deleted: ,

Deleted: or

Deleted: or

Deleted: and

Deleted: as well

17. Interconnection of files and on-line access to files

In specific circumstances the police may seek to collect data by coordinating its information with other data controllers and processors. Furthermore, it may combine personal data stored in different files or in different databases that are held for different purposes, such as those held by other public bodies and/or private organisations. This may be in relation to an on-going criminal investigation or to identify thematic trends in relation to a certain type of crime.

In order for these actions to be legitimate they must be authorised or be underpinned by a legal obligation to comply with the purpose limitation principle.

If the relevant police body has direct access to files of other police or non-police bodies, it must only access and use the data if domestic law, which should reflect the key data protection principles, so permits.

Clear legislation and guidance, which adheres to the data protection principles, should exist for cross-referencing of databases. Such cross referencing should be necessary, purpose bound and proportionate. With relation to personal data stored in other data controllers' or processors' data base all conditions described in Point 2 have to be fulfilled and regularly checked.

Example - Data held for citizenship purposes can only be used in an investigation if the national legislation allows it and to the extent to which it is necessary for the purpose of the investigation to do so. For instance, the number of children a suspect has may not be relevant in an investigation, and should therefore not be processed by police. Access in this case to a database can be perfectly lawful but it can only be legitimate if it respects the principles of data protection.

18. Data security

The police must take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The controller must notify, without delay, at least, the competent supervisory authority of those data breaches which according to its assessment may seriously interfere with the rights and fundamental freedoms of data subjects. The information of data subjects of data breaches which may seriously interfere with their rights may also have to be ensured without undue delay, unless it jeopardisese the task of the police.

Information security is essential to data protection. It is a set of procedures to ensure the integrity, availability and confidentiality of all forms of information within the police organisation, with the aim of providing security of data and information, and limiting the impact of security incidents and data breaches to a predetermined level.

The level of protection given to a database and/or an information system or network is determined by a risk assessment. The more sensitive the data are, the greater protection is required.

Authorisation and authentication mechanisms are essential to protect the data, and sensitive information should always be encrypted. It is considered best practice to have in place an audit regime to regularly check that the level of security is appropriate.

Police authorities are advised, where necessary, to conduct DPIA (see Point 4) to assess the privacy risks to individuals in respect of the collection, use and any disclosure of information. This will help to identify risks and develop solutions to ensure that concerns are addressed appropriately. Any such impact assessment should cover relevant systems and processes of processing operations, but not individual cases.

Deleted: crime

Deleted: have

Deleted: they

Deleted: in

Deleted: accordance with

Deleted: permits legislation

Deleted: ,

Deleted: of

Deleted: therefore

Comment [A28]: Note that this is not consistent with Article 33 of the GDPR according to which all data breaches shall be notified unless "the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

Deleted: any

Deleted: affect

Deleted: them

Deleted: shall also

Deleted: ing

Deleted: ¶

Deleted: ,

Deleted: …

A Data Protection Officer (DPO) within the police can play an essential role in carrying out internal audits and assessing the legitimacy of the processing, which contributes to a higher level of data protection and data security within the organisation. Moreover, the DPO can facilitate the dialogue between the organisation and the data subjects, as well as the organisation and the supervisory authority which can add to the overall transparency of the police body.

An Identity & Access Management System (IAM) may be recommended to manage employees and third party access to information. This will require authentication and authorisation to access the system and set privilege rights to determine what can be viewed. IAM can be seen as a useful requirement to ensure safe and appropriate access to data.

The data controller, following an evaluation of the risks, should at implement measures in respect of:

- equipment access control,
- data media control,
- storage control,
- user control,
- data access control,
- communication control,
- input control,
- transport control,
- recovery and system integrity,
- reliability and integrity.

Privacy-by-Design

The concept of privacy-by-design is an integral part of data security. Data protection and security may be embedded directly into information systems and processes, using technical and organisational measures, to ensure a high level of data protection and security and, in particular, to minimise the likelihood of data breaches. This approach is known as Privacy–by–Design, promoting privacy and data protection compliance from the start. It can be achieved through software and/or hardware. It requires a threat analysis, a full life cycle approach and rigorous testing.

Data controllers should ensure that privacy and data protection is a key consideration in the early stages of any project and then through its life cycle. Specifically, when building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have privacy implications and embarking on an information sharing initiative using data for new purposes.

Privacy-by-Design requires the implementation of Privacy Enhancing Technologies (PETs) to enable a better protection of personal data. PETs prevent unnecessary processing of personal data, without losing functionality in the information system itself.

Example: Body scanners used for police purposes have to be designed to respect the privacy of the individuals being inspected while fulfilling the purpose of their use. Therefore the body image in such tools has to be blurred by default.

19. External control

There has to be, at least, one supervisory authority responsible for ensuring compliance of data processing to the international and national legislation within the law enforcement sector.

Certain states may require more than one supervisory authority, for instance a national or federal authority and a number of decentralised or regional authorities, whilst others will prefer to have a single supervisory authority, responsible for the entirety of the supervision of data processing operations.

Deleted: P

Deleted:

Deleted: *Privacy-Enhancing Technologies (PETs)* ¶

Deleted: This is the common name for a range of different technologies to protect sensitive personal data within information systems.

Deleted: users to

Deleted: their

Deleted: The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.¶

The supervisory body should be completely independent, meaning that it does not belong to the law enforcement organisation, nor is it directed by another body whithin the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties and should not be instructed or forced to accept instructions from anybody. The personal independence of its chair/president including political, financial, functional and operational independence, are decisive factors when judging how independent the supervisory body is.

Deleted: organisation

Deleted:

National law should provide for advisory, investigative and enforcement powers to enable it to investigate complaints, to have regulatory measures or to be able to impose sanctions where needed. The legal and administrative tools at its disposal shall be efficient and enforceable.

Supervisory authorities should have the ability to cooperate in law enforcement matters bilaterally and also via the Committee of Convention 108.

Example: The supervisory authority must be independent and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

a. “personal data” means any information relating to an identified or identifiable individual (“data subject”);

b. “genetic data” are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

c. “biometric data” are data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual;

d. “soft data” (evidence based on testimony or other personal assessment) means data acquired through testimony of person involved in the investigation;

e. “hard data “ (evidence based on documents or proven facts) means data acquired from official documents or other certified sources;

f. “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

g. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

h. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

i. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

j. Internet of Things (IoT): is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

k. “covert surveillance” means all measures aiming at monitoring discreetly the movements of persons, vehicles and containers, particularly those involved in organised or cross-border crime.

l. “special investigative techniques” techniques applied by the competent authorities in the context of criminal investigation for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person.

m. “privacy-enhancing technologies” (PETs) means a range of different technologies to protect personal data within information systems. The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.

Deleted: g. “competent authority” means: public or private entity authorised by law having a competence in the prevention, investigation and prosecution of criminal offences and to the execution of criminal penalties;¶

Deleted: h

Deleted: i

Deleted: j

Deleted: k

Deleted: l

Deleted: m

Deleted: n

GERMANY/ALLEMAGNE

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied to ensure the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").
Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed application and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[21] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level.
The present Guide was therefore preparedto highlight the most important issues that may arise in the use of personal data in the police sector and to pointout the key elements to be considered in that context.
This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance.
The overarching principles set out in Recommendation (87)15 and their practical implications aim to ensure that the processing of personal data by the police is carried out in full respect of the rights of the individual to privacy and data protection.
To facilitate the reading of the Guide, a glossary of the terms used is provided at the end of the document.

Deleted: use
Deleted: determined

General considerations

The collection and use of personal data for law enforcement purposes constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and, as such, it *must* be based on law (clear, foreseeable and accessible), pursue a legitimate aim and be limited to what is necessary and proportionate to achieve that legitimate aim. (Former second paragraph moved upfront)

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data processing within the police should be based on predefined, clear and legitimate purposes set in the law; it should be necessary and proportionate to these legitimate purposes and should not be processed in a way incompatible with those purposes Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible.

Deleted: processed
Deleted: , they
Deleted: always
Deleted: compliance
Deleted: the original purpose.

1. Scope

The principles explained in the present guide apply to the processing of personal data for police purposes, for the purposes of the prevention, investigation and prosecution of criminal offences, the execution of criminal penalties [and for the maintenance of public order by the police] (hereafter referred to as "tasks of the police", ["police purposes"]). Where 'police' is used in the text, it can be taken to mean wider law enforcement authorities, and/or other public and/or private bodies authorised by law to process personal data for the same purposes.

Deleted: primarily
Deleted: ").

[21] See Report "Twenty–five years down the line" – by Joseph A. Cannataci

Field Code Changed

2. Collection of data and use of data

The police as data controller is responsible for all data processing it undertakes and is accountable for its data processing operations.

The collection of personal data for police purposes should be limited to what is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

It is understood from Point 2.1 of the Recommendation that inforthe fulfilment of both of the main police tasks (prevention of a real danger and the suppression of a specific criminal offence), an evident and direct correlation should exist between the data processing carried out by the police and a situation where individuals have already committed or are likely to commit a crime.

The police should always choose the adequate legal basis to process personal data and should process personal data in a legitimate way. A careful assessment should be carried out by police to make sure that the processing is based on an appropriate legislation and the procedures for data processing foreseen by it are fully respected.

The police should apply at all stages of the processing the relevant data protection principles (most importantly the principles of necessity, proportionality and purpose-bound data processing) and should not continue to process data which are not needed for the purposes. In this context, personal data collected at an early phase of the investigation, which then proves with the process of the investigation to be no longer relevant should no longer be processed (e.g. innocence of a suspect is confirmed), and should therefore either be blocked or deleted. This does not apply where subsequent use of the data is allowed (point 3).

Prior to and during the collection of such data, the question of whether the personal data collected is necessary for the investigation or for a task of the police as described in Point 1, should always be considered. One should note that once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific task of the police) should exist. This link together with compliance to the data protection principles as described in the Guide, must be demonstrable at all times. After the collection phase and at different stages of the investigation, a thorough analysis is needed to assess which data are to be retained and which are to be deleted.

Before collecting any personal data, investigators should ask themselves the question 'Why is it necessary to acquire the data?', 'What, exactly, do you seek to achieve?'.

Example – For personal data such as Telephone Billing: only the number(s) required for the time periods being investigated should be sought and only for those individuals suspected of having a link with the offence.

A list of phone numbers of the person(s) involved in the suspected offence can be collected if there are indications that such data serve the purpose of the investigation. It cannot be kept or processed after the analysis shows that the data are not strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for police purposes should be used for those purposes only and should not be used in any other way that is incompatible with the original purpose stated at the time of collection and is necessary for and proportionate to the pursuing of police purposes, unless this is provided for in law (see Article 9 of Convention 108) [In assessing the compatibility of the use of data for the same purpose, one should consider the following criteria: (i) relation between purposes; (ii) context of the collection and information given to data subjects; (iii) nature of personal data; (iv) consequences for data subjects of the intended subsequent use; (v) existence of appropriate safeguards.]

Deleted: The collection and use of personal data for police purposes should be limited to what is necessary and be proportionate for the purpose of prevention, investigation and prosecution of criminal offences, the execution of criminal penalties (i.e. to a specific criminal offence(s) or the suspicion thereof) and for the purpose of the maintenance of public order.

Deleted: of the legal basis upon whichthe personal data is processed needs to consider the different operations during which the

Deleted: is

Deleted: data

Deleted: .

Deleted: prnciples

Deleted: demonstrated

Deleted: Art

Subsequent use of data is considered for the purposes of this guide as a new data processing operation which has to fulfil all the criteria and conditions mentioned above. The subsequent use of data shall be lawful, undertaken for a legitimate aim and necessary and proportionate to this legitimate aim.

The police shall ensure at all stages of the data processing and for the subsequent use of data as stated in the General considerations that the personal data are accurate, up-to-date, adequate, relevant and not excessive in relation to the purposes for which they are processed.

Example: Police data collected for an investigation where the political affiliation is irrelevant, cannot then be used to determine the political affiliation of the concerned person.

Deleted: unless provided for by law

3. Subsequent use of data

Every subsequent processing of data for police purposes other than that the data were originally collected for, must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be undertaken for a legitimate aim and should be necessary and proportionate to the legitimate aim pursued.

Deleted: by police (irrespective of the purposes of the original processing)

Personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set out in Point 2. The general rule is that if data are likely to be used in a different case or in a different operation of the police, the assessment of compliance described in Point 2 shall be applied to this new processing as well (This is not applicable if data are used for purely statistical or scientific purposes). Notwithstanding thecomputerised and/or automated data processing and the large volume of personal data stored very often in different processing environments, the, personal data collected and retained for police purposes should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

Deleted: Due to computerised

It should be noted, moreover, that any subsequent use of personal data related to vulnerable individuals such as victims, minors, or of those enjoying international protection, should be subject to additional care and legal analysis with a special attention to the application of the principles of necessity and proportionality.

Deleted: however

Deleted: of

In cases such as trafficking in human beings, drug trafficking or sexual exploitation, where victims' data may subsequently be used also when they are considered as suspects, or where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to look at existing international good practice (in international or regional police bodies) and to enhance their exchange of information on the matter with other national police bodies.If all legal requirements as put forward in Point 2 are met, it should not represent any obstacle to the use of data of these persons for police purpose, but during these exchanges, confidentiality rules have to be followed.

Example - Data collected for tax purposes from a data subject can only be processed for law enforcement use by police () if the law allows it, if they are used for a legitimate aim and in a way that is necessary and proportionate to the aim pursued. In a concrete investigation of money laundering, the use of tax declarations' data of an individual can be envisaged to establish or deny a link between the individual and the money laundering operations. .

Deleted: taken

4. Processing of special categories of data (sensitive data)[22]

Special categories of data, such as genetic data, personal data related to offences, criminal proceedings and convictions and related security measures, biometric data uniquely identifying a person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical nature, for instance additional security measures, and of an organisational nature, for instance having such sensitive data processed separately from the processing environment of the "ordinary" categories of data. Safeguards should be adjusted to each data processing operations taking into account their specificities and it is highly recommended to use multiple

[22] Paragraph removed from previous Point 8

Formatted: English (U.K.)

levels of protection for those categories of data (e.g.: separate main-frames, shorter data retention periods, etc.). It is of paramount importance to prevent unauthorised or unwanted access to those categories of data even with additional security measures.

A careful balance of interests taking into account the purpose of the investigation, the context and the nature of the data is necessary to determine whether or not, and to which extent, the police could process sensitive data. For instance, it would be advisable to differentiate when biometric data is processed by the police whether it is for identification purposes (where for instance 2 fingerprints could suffice) or it is for crime investigation purposes (where more fingerprints could be needed).

The use of Data Protection Impact Assessments (DPIA) which is in general is to be carried out where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons can be recommended also in order to help to ensure that appropriate safeguards are put in place. The data controller should assess and demonstrate whether the purpose of the processing can be achieved in a manner that impacts less on the right to privacy and data protection and if the processing of special categories of data does not represent a risk of discrimination for the data subject.

Deleted: is recommended in order

Moreover, it should be recalled that the collection and processing of sensitive data in the context of profiling is prohibited (Principle 3.11 of Recommendation 2010 (13)[23] except if these data are necessary for and proportionate to the lawful and specific purposes of processing and as long as domestic law provides appropriate safeguards. In this context, besides measures detailed above, the use of PETs and more frequent checks on the lawfulness of the processing can be recommended. This could, for example, translate into measures put in place to counter the assumption that individuals belong to a criminal organisation because of where they live, where a criminal organisation is active or where the individuals have the same ethnic origin.

Deleted: Regarding these data the potential risk of negative discrimination or of adverse legal effect significantly affecting the data subject should be avoided, since all profiling based on sensitive data resulting in negative discrimination are prohibited.

Example - Targeting groups or individuals based solely on religious beliefs would not be allowed. In an investigation into a group of individuals engaging in possible terrorist activities that were attached to a particular religious group, it could nevertheless be of importance to process data specific to the followers of this specific religious group (related to worshipping place, religious preachers, customs, teachings, members and structure of the religious community, etc. that was pertinent to the investigation).

Deleted: However, in

Deleted: However, targeting all followers of a religion, purely because of their religious belief is strictly prohibited.

5. Providing information to data subjects

One of the most important obligations of a data controller is to provide information on data processing to data subjects. This obligation is two-fold: it requires the data controller to provide *general information* to the public on the data processing that it carries out, and to give *specific* information to data subjects if no restrictions or derogations apply to the data processing.

Information provided to the wider public, , should promote awareness, inform them of their rights and provide clear guidance on exercising their rights. The information provided should be effectively and broadly accessible. Moreover it should include details about the conditions under which exceptions apply to the data subject's rights and how they could submit an appeal to the DPA or to the judiciary..

Deleted: regarding these files.

Websites and other easily accessible media perform a role in informing the public. It is recommended to have in place letter templates on these websites or other media to help the data subjects exercise their rights. It is the responsibility of the data controller to provide information which adequately highlights data protection and data subjects' rights.

[23] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member stateson the protection of individuals with regard to automatic processing
of personal data in the context of profiling
(https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00)

In order to comply with the second obligation of giving data subjects specific information regarding data processed, the police shall inform data subjects on the data processing envisaged before the processing or, if it is not possible, for objective reasons, shortly after it. This communication shall comprise information on the data processing, on the collection of the individuals' data and comprehensive information on their rights.

The obligation to provide specific information implies that, in principle, the data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.

The information should be provided unless a restriction or derogation applies as described in Point 7 taking into account the specific nature of sensitive files, such as criminal intelligence files, files containing sensitive data. in order to avoid serious prejudice to the performance of police functions or to the rights of individuals. Even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.

Very often data subjects, because of restrictions or derogations of their right to information, cannot receive complete information on the processing the police undertake with their data; this should not affect their exercise of the right of access.

Example - For the purpose of covert monitoring of a high risk sex offender, data processing and long-term data retention may be justified without informing the individuals under surveillance if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved, the data subject should be informed about the fact that she or he was subject to such measure.

6. Data subject's rights[24]

Accessing their personal data is a fundamental right for data subjects as it allows them to be aware of the processing on data related to them. Moreover, it can also be a prerequisite to enable the exercise of further rights, such as the right of rectification and the right of erasure

In case an individual has her/his data collected during the course of an investigation or other tasks of the police as described in Point 1, as soon as circumstances safely permit, the police [in principle] should inform the individual of the data processing if there is such request. Specific information should be given in clear and plain language upon request . The communication has to contain the same information as described in point 5, unless data subjects wish otherwise.

The law can provide, under the strict conditions described in Point 7, that the right to be informed upon request may also be limited or excluded, should the provision of such information prejudice the investigation, or another important police task, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified.

The police should aim to answer even general questions arising from data subjects on the processing activities in relation to their personal data, but can use standardised forms to facilitate communication.

Example: If a data subject asks the police on data it processes on them, the police, if no exception is applicable, should provide a detailed answer with legal references, but should do so in a plain language, avoiding uncommon or specialised expressions.

The right of access should, in principle, be free of charge.

[24] Paragraph removed from previous Point 17.

Deleted: before the processing

Deleted:

Deleted: .

Comment [A29]: GER: This is not correct; it is part of the duties of the controller to inform the data subject (if no restrictions apply) and is not a right granted upon request; thus the right of access can only be a prerequisite of the mentioned rights of rectification and erasure.

Deleted: thethe right to information

Deleted: The right to information on request, the right of rectification and the right of erasure are interdependent rights. ¶
¶
The police [in principle] has to inform the individuals on the data processing activities carried out with their data. This means that in

Deleted: The

Deleted: upon request as soon as data are processed, for instance at the time of collection and it should be provided

Formatted: English (U.K.)

It is possible to charge a reasonable administrative fee for the request, if national law permits and the request is manifestly unfounded or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such refusal.

To ensure a fair exercise of the right of access, the communication "in an intelligible form" applies to the content as well as to the form of a standardised digital communication. It is, however, advisable to refer to national legislation to ensure consistency and to avoid suspects utilising this method to find out whether there is an on-going investigation into them.

In respect of direct access, the data subject can request access to the controller of the files. The data controller will assess the request and any possible restriction or derogation which can only be used if it is vital for the performance of a specific police task as described in Point 1, or it is necessary for the protection of the data subject or the rights and freedoms of others, and reply directly to the data subject. In case of a restriction, partial information, and in case of derogation, information on the use of derogation, shall be still given, with the motivation for using such measures in both cases, as well as information concerning redress.

Example: The access request can be refused if there is an on-going investigation on the person, and providing the data subject access to the data could compromise such investigation.

If restriction or derogation were to be used, any answer should take into consideration, according to national law or practice, all circumstances to which the restriction or the derogation is applicable.

As a rule, domestic law should, ideally, provide for direct access. If the right of access provided for is indirect, the data subjects may direct their request to the supervisory authority, which after being properly mandated, will carry out the request on their behalf and conduct checks regarding the availability and lawfulness of the processing of the data subject's personal data. The supervisory authority will then reply to the data subject (providing what data it is possible to release, subject to any legally allowed restrictions or derogation). In case of a restriction or derogation, the same communication should be made possible as in case of a direct access.

The data controller should assess the request and reply to the data subject within a reasonable time limit, as provided for by domestic law.

There should be arrangements in place to confirm the identity of the data subject before access to any data is granted as well as to obtain information on the processing activities to which the request refers. The same holds if the data subjects delegate the authority to someone else to exercise their rights.

It is an essential right of the data subjects to be able to have amended any incorrect data held on them or to have deleted data held on them whose processing is excessive, irrelevant or unlawful for another reason. If the data subject finds data that are incorrect , she/he should have the right to challenge it and ensure that they are amended. If the data subject finds data whose processing is excessive, irrelevant or unlawful for another reason, she/he should have the right to challenge it and ensure that they are deleted.

In some cases, it may be appropriate to add additional or corrective information to the file. It is important to underline that this right can only be exercised with due respect to other individuals' rights, for instance to the rights related to a testimony in a criminal case (which does not preclude per se the exercise of the data subjects' rights related to soft police data).

If the data to be corrected or erased has been communicated elsewhere the relevant authorities should be informed of the changes to be made.

All proposed changes should be supported by evidence. If data subjects can prove by use of the official documentation that the data processed by police in respect to them are incorrect, the data controller shall not have the right of discretion whether to correct them.

It may be necessary for the police, as dealt with under Point 7, not to give information or grant the right of access, of deletion and of correction which might jeopardise an investigation and should therefore be

Comment [A30]: GER: The inadequate mixture of the amendment/rectification of incorrect data with the deletion of excessive/irrelevand data can lead to misunderstandinds. See suggestion for clarification.

Deleted: It is an essential right of the data subjects to be able to amend any incorrect data held on them. If the data subject finds data that are incorrect or irrelevant, she/he should have the right to challenge it and ensure that they are amended or deleted. ¶

Comment [A31]: GER: the aspect of the right to have data deleted is - according to our suggestion - dealt with above

Deleted: Data subjects can ask for the deletion of their personal data where such processing is unlawful.

Deleted: ¶

excluded for its duration. Similar restrictions or derogation may be imposed by national law as described in Point 7.

Restrictions or derogations to the rights of data should only apply to the extent necessary and be interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis. Any decision to refuse a data subject's request should be provided in writing (including by electronic means). The response should provide clear justification of the decision making which can be verified by an independent authority or a court. It is possible that communicating the reasons for refusal could pose a risk to law enforcement or the data subject or to the rights and freedoms of others. If this is the case, it should be documented and provided to the independent authority or court to be verified, if required.

Example - If person A submitted a declaration against person B accusing her/him of committing a serious offence and later it emerges that the accusation was false, it might be relevant for the police to retain the false statement and the information surrounding it.

Although the statement was proven to be false, if the police needs to retain the data in the interest of the investigation for instance , a clear corrective statement on the file, instead of removing the false statement, would be necessary.

The data subject should be informed of all available options following a refusal decision such as an appeal either to the supervisory authority, to court or to another independent administrative authority.
Depending upon national legislation, specifically whether there is a direct or an indirect right of access, the actual communication of the result of the review or appeal may differ. In the case of indirect access the data subject should at least be informed that a verification of the police file has taken place. Alternatively, the supervisory body may request the police to release the data contained in the file to the data subject. The court or tribunal may have powers to enforce the access, correction or deletion of data from the file even in access-request cases referred to them by police or the supervisory authority.

If police sends a refusal letter it should contain the name, address, web address, etc. of all possible forafor redress.

The data subject should have access to a court or tribunal in order to submit an appeal, and have the reasons for refusal verified if they are not satisfied with the reply given by the supervisory authority or the independent authority. The supervisory authority should have sufficient powers to examine the police file concerned and have the assessment communicated.

7. Exceptions from the application of data protection principles

Exceptions can only be used for specific purposes foreseen by article 8 of European Convention on Human Rights and article 9 of Convention 108, if foreseen by law (the law should be public, open and transparent and, in addition, detailed enough) and if they constitute a necessary and proportionate measure in a democratic society.

The exceptions which have to be incorporated into national legislation should not be described in a general way, but should serve a well-defined purpose.Exceptions can be applicable to those principles described under Points 2,3,,5,as well as to the data subjects' rights (Point 6) in case of some specific purposes in relation to which data processing activities are undertaken. In particular they concern activities undertaken for the purpose of the protection of national security, defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest (which includes purposes in connection with the fulfilment of a state's international legal commitments or obligations, most prominently deriving from the binding decisions of United Nations' bodies, and humanitarian purposes.) or the protection of the rights and fundamental freedoms of others.

Example - If giving information to a data subject may endanger the safety of a witness or an informant; this right can be limited in light of such circumstances.

Deleted: requires the retention of the data

Deleted: It is possible that

Deleted: inspecting body cannot communicate the data to the individual even if there is no justification for refusing

Deleted: . In this case

Deleted: inspecting

Deleted: ¶
Example:

Formatted: Border: Top: (No border), Bottom: (No border), Left: (No border), Right: (No border)

Deleted: Under the

Deleted: exceptions can only be used

If the exception, as defined by national law providing specific safeguards is used by the police, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. The aim of using exceptions by the police should be limited to cases where the use of those rules and principles would endanger tasks of the police described under Point 1..

Example: If data collected for police purpose in an investigation are likely to serve national security purposes they can also be used to this latter purposes to the extent set forth by national legislation. If specific intelligence proves that money laundering operations have been carried out to finance terrorist operations, data collected on individuals during the investigations on money laundering can be used for the purpose of eliminating the close and imminent terrorist risk.

8. Use of special investigative techniques

The police should always adopt the least intrusive means of data processing during its operations. If less intrusive methods can be used to achieve the desired ends, they should be preferred. The use of special investigative techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods.

With increasingly sophisticated technological developments, electronic surveillance has become easier, however, the use of these techniques interferes with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the high potential of severe interference with the right to privacy has to be balanced with the efficiency of investigations.

Example: In an investigation, the evidence for communication between two suspects can be gathered in various ways. If, by the use of interrogations, testimonies, the obtaining of call data, the same result can be achieved without jeopardising the effectiveness of the investigation, it is to be preferred to the use of more intrusive surveillance measures, such as wiretapping.

Deleted: Regardless of the method of investigation or other operation led by the police, the police is obliged to comply with the general principles of data protection as described in General considerations, unless a law expressly exempts from it.

Deleted: ¶

Deleted: can interfere

Deleted: or discreet surveillance

9. Introduction of new data processing technologies

If the introduction of new technologies is likely to result in a high risk to the individual's rights, the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity. The relevance of the DPIA shall be checked at reasonable intervals.

It is also of great importance, that in terms of data security and safety of communications, the highest standard is taken into account when introducing such technologies.

Example - New data mining techniques may offer extended possibilities for identification of possible suspects and should be assessed carefully for their compliance with existing data protection law, together with assessment of the risks it may represent to individual's rights and suggestions for the adoption of safeguards to ensure the protection of data, including with regard to data security.

The data protection authority has an important role in advising which risks are involved for data protection and which safeguards should be provided to ensure that any technical means comply with data protection law. However, the police do not have an obligation to turn in every case to the supervisory authority where it introduces new technologies. It may do so if the DPIA it previously conducted demonstrates a significantly persisting high risk to the individual's rights notwithstanding the adoption of specific safeguards.

The consultation between the supervisory authority and the data controller should provide the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.

Comment [A32]: GER: The added sentence (in a nutshell: mandatory DPIA w/ new technologies) contradicts the first one (in a nutshell: DPIA w/ new technologies when there is likely risk for individual´s rights) and should therefore be deleted.

Deleted: The introduction of new data processing technologies is considered to be subject to a DPIA as probability of risks to the individual's rights is usually high

. Appropriate details should be provided to the supervisory authority, in particular regarding the type of file, the data controller, data processor, the legal basis and the purpose of the data processing, the type of data being processed and by whom the data is being accessed, as well as information on retention of data, log policy and access policy, and other relevant technical aspects of implementation.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data could be reported to or made available for consultation to the data protection authority.

Following consultation, the data controller should consider carefully to implement any necessary measures and safeguards that have been recommended by the data protection authority.

Example - Introducing an automatic facial recognition system or other system based on the automated processing of biometric data would be very likely to need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed and recommended by the data protection authority after being consulted on the issue, specific safeguards should be put in place (concerning the data retention time, the cross matching functionalities, the place of the storage of data and the access to data issues, etc.) to comply with data protection principles and provisions

Use of the Internet of Things (IoT) technology in police work

Data sent to and from police during operational activity via the internet are good examples of the IoT already in use. Due to potential security vulnerabilities, IoT requires measures such as data authentication, access control to ensure data security and resilience to (cyber) attacks.

Example: In light of their potential security vulnerabilities, smart glass used by police should not be directly connected to a national criminal record data base and data collected should be guaranteed a high level of security.

Big data analytics in the police

Technological advances in processing and analysing large and complex data sets leading to big data and big data analytics present opportunities and challenges to the police, who is turning to digital sources and profiling techniques to perform their tasks.

Big data technologies enable bulk collection and analysis of a vast quantity of data generated by electronic communications and devices aggregated with other bulk data. This could interfere with the right to privacy and data protection.

The Council of Europe's Recommendation CM/Rec(2010)13[25] on the protection of individuals with regard to automatic processing of personal data in the context of profiling and the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[26] can be of use in the context of Big Data analysis for police use too.

Big data technologies and analysis techniques may help assist detecting crime, but there are, however, considerable risks to this type of data processing that should be taken into account:

- Databases originating from one domain can be used in another domain and for another purpose, which changes the context and may lead to inaccurate conclusions and lack of valid legal basis, therefore to unlawful data processing with possibly serious consequences for the individuals involved.
- Profiling may lead to drawing discriminatory conclusions, which can result in the reinforcement of stereotypes, stigmatisation and discrimination.

[25] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[26] Document T-PD(2017)1 - Big Data Guidelines

Field Code Changed

Formatted: English (U.K.)

- The increasing amount of personal data held in databases may lead to severe vulnerabilities and subsequent risk of data breaches if information security is not guaranteed.

Where big data relies on personal data, data controllers should pay additional attention to the following requirements:

- Verification of data accuracy, context and relevance of the data.
- Its use requires a high level of accountability.
- Its use shall be combined with methods of investigation which complement the conclusions drawn from the big data analysis. A decision affecting a person shall not be taken solely on automated processing of personal data.
- As for other types of data processing, it is of paramount importance that its use shall be ~~shall be be~~ necessary and proportionate for the fulfilment of police tasks described in Point 1, with special attention for the data processed to be adequate, relevant and non-excessive in relation to the purpose for which they are processed.
- Predictive analysis requires human intervention to assess the relevance of the analysis and conclusions.
- Ethical guidelines developed at national or at international level should be taken into consideration.
- As a principle and subject to restrictions and derogations mentioned in Point 7, transparency should be ensured by the data controller by explaining how the data are processed in accordance with privacy and data protection principles. If data collected for one purpose is used for another purpose, the data controller should in principle make the data subjects aware of this subsequent use.
- Even if complex methods are used, the lawfulness of the processing – including subsequent use of data - and compliance with the conditions set by Article 8 ECHR and Convention 108 should be demonstrated.
- An information security policy should be in place and implemented throughout the processing.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals and the administrative and judicial means exist for individuals to challenge those decisions. This implies data subjects' awareness of the reasoning of the algorythm used and the purposes for which it was used.

The above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones, are even more necessary when sensitive data are processed in Big Data analytics.

10. Storage of data

"As pointed out in Point 2" data shall be processed until they have served the purpose for which they were collected. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

There should be a clear distinction in how the police stores and processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses. This should also relate to the specific purpose for which the data was collected. Additional safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence. Clear rules have to be established in relation to the handling of different data bases with special attention to the analysis of multiple results.

The principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve the purpose of the prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where personal data is processed for the purpose of the maintenance of public order.

The grounds for retention and processing should be reviewed periodically. The unlawful processing of personal data outside of the legal framework allowed for the retention constitutes a severe violation of the right to protection of personal data. If the law in relation with a specific crime provides for a data retention period of 4 years and if

Deleted: .

Deleted:

Deleted: an individual is kept

personal data are processed in relation with this crime by the police solely on this ground after 4 years have passed since the collection of the data in question and no other legal ground to process this data exists, the retention of this data could be considered as unlawful.

Deleted: custody

General data retention periods are usually regulated in national or international law. In order to comply with the legislation while ensuring the effectiveness and the success of an investigation police bodies are strongly advised to develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data.

For example, in a case where the law prescribes a 4 year data retention period but the individual subject to an investigation is acquitted from all charges by the court after 2 years, her/his data shall be deleted (if the individual is not a recidivist or there is no information on her/him committing again the same category of crime) from the database, provided that all deadlines for the review of the case have expired. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judicial procedure terminates completely (which means all redress have been made or all deadline for redress have been passed).

The police should provide systems and mechanisms to ensure that the data that are stored are accurate and that their integrity is maintained.

International obligations, which include providing data to international bodies such as Europol, Eurojust and INTERPOL, bilateral agreements and mutual legal assistance between member states and third countries must be observed when shaping internal policies.

Data should be categorised according to the degree of accuracy and reliability in order to assist the police in their activities. It is recommended that handling codes are used to distinguish these categories. A classification system facilitates the assessment of the quality of the data and how reliable it is. Classification of data is also important when it is to be communicated to other police bodies or states.

Example - Information collected directly from a person's statement will be assessed differently than information collected from a person's hearsay statement. Data based on facts, or 'hard' data, will be assessed differently than data based on opinions or personal assessments, or 'soft' data.

Personal data collected by police for administrative purposes must be kept (as far as possible: logically and physically) separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by law.

Examples of administrative data include lists of data on licence holders or data on human resources and firearms certificates.

11. Communication of data within the police sector

A distinction should be made between domestic communication of data and international transfer of data. Within these two distinct operations different requirements apply, depending upon who is receiving the data, whether it is the police, another public body or a private party. The police can only communicate personal data within the police sector if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

There should be clear and transparent rules on how the police grant access to data held by it and on which grounds.

The police, domestically, should only share information (among police) when there is a legal basis for the request, e.g. an on-going criminal investigation or a shared law enforcement task and laws or agreements allowing the communication

The police can share data with other police organisations if the personal data are relevant for the purpose of prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where they are processed for the purpose of the maintenance of public order.

The communication of personal data in general should be in line with the general considerations described above.

Example: A police unit can share data on a suspect who presumably committed a tax fraud with another police unit investigating a murder case if there is indication that the suspect for this crime could be the same person or if doing so will materially assist the investigation.

12. Communication of data by the police to other public bodies

The communication of data outside police is permissible if it is provided for by law and the data are required by the recipient to enable them to fulfil their lawful task. Mutual assistance agreements foreseen by the law between law enforcement and public bodies allows the public bodies to have access to law enforcement data which would be essential in the fulfilment of their duties and tasks (for example in their investigations or other legal duties in accordance with national law).

Stricter principles than those set forth in Point 11 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the processing of personal data, which are considered sensitive, could result in adverse effects for the individual.

Communication of data to any other public authority may also be allowed if it is foreseen by law, is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to other persons or to public order or to public security.

The communicated data may only be used by the receiving body for the purposes for which the data were transferred.

Example - A claim for a residence permit made by a migrant. Police data may be required to verify if the person was ever involved in criminal activity. It would be in the interest of the Immigration Office and the claimant for this communication of data to take place.

13. Communication of data by the police to private parties

There may be occasions when, under strict conditions, the police can communicate data to private bodies. This communication has to be based in law and can only be done by the authority which is processing the data. Such communication can only be done for the purpose of the investigation or other important police tasks as described in Point 1, in the interest of the data subject, for humanitarian reasons or if it is necessary to prevent serious and imminent risk to public order or public security. For example, there might also be instances where police data may be communicated to humanitarian organisations based on international law, in the interest of the data subject or for humanitarian reasons.

Where the police shares data with media in respect of making information related to an investigation public, special consideration should be given to the assessment to determine that it is necessary and in the public interest that such publicity is allowed.

Such communication should only be on a case by case basis and in each case there must be a clear legal basis providing the necessary procedure (e.g. need for specific authorisation) to be followed for any such communication to occur.

Example - When the police communicate with the financial sector in relation to known fraud or theft offenders, when it communicates with an airline about stolen or lost travel documents or when the police releases details of wanted persons believed to pose a risk to the general public.

14. International transfer

Any transfer of police data internationally should be limited to police bodies and should be fit for purpose and in accordance with the law. For this, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data handling, regional legal frameworks such as EU and EU institutions' legislation (on Europol, Eurojust, Frontex, etc.) and subsequent agreements (operational bilateral agreements), bilateral treaties and in general, international agreements on mutual assistance, or other bilateral or multilateral agreements made regarding effective cooperation can be of use.

When considering sharing any data, consideration should be given as to whether the receiving authority is performing a function conferred to it in law related to the prevention, investigation, or prosecution of criminal offences, the execution of criminal penalties and the maintenance of public order, and whether the sharing of the data is necessary to perform its specific task.

The sending authority should ascertain that there is an appropriate level of data protection in the receiving state and that the receiving state complies with the relevant rules of international transfers of personal data. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. This means of transfer should be used as a last resort option. International transfers framework such as "INTERPOL's Rule on the Processing of Data" and its "Statute of the Commission for the Control of INTERPOL's files" Rules on the Control of Information and access to INTERPOL's Files", the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185) may be taken into account[27] so as to ensure that any transfer of data is legally justified and has appropriate safeguards in place. The request should clearly state all the necessary elements from the requesting party to enable the receiving party to make a sound decision on the request. These details would be expected to include the reason for the request as well as the purpose for the transfer of data.

An appropriate level of data protection should be guaranteed (e.g. through ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments) if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

If there are conditions applied by the sending authority in relation to the use of the data in the receiving state these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout its lifecycle.

Example - Further transfer of data should only be allowed if this is necessary for the same police purpose as the original transfer and the second recipient is also a police body ensuring an appropriate level of data protection. The police body which originally sent the data must also consent to the onward transfer. If the police from country X sends personal data to the police of country Y it is only permissible for the country Y to transfer this data if above all requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) if country X consents to the transfer. If the data is sent to country Z which is a non-member of the Convention 108, then country Y should ascertain that this country provides an appropriate

[27] This is without prejudice to the right of the Committee of Convention 108 and other instances disposing such power to assess and to review if necessary the level of data protection guaranteed by those multilateral agreements

Formatted: English (U.K.)

level of protection of personal data and effective means of exercise of the related data subject rights.

The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases if it is required for the performance of the task of the transferring authority and there is no effective means of transferring the data to a police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers.

Example: If tax authorities in country X requests the police in country Y about the whereabouts of a person involved in non-criminal tax evasion because they have evidence that the person is involved in criminal matters in country X, the police can transfer the personal data of the individual.

The international transfer of personal data between police and private bodies in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police as described in Point 1, provided by legal means and where the emergency, the gravity of the crime, its trans-border nature and where the involvement of the police would not be possible for objective reasons . Other facts as data security, the reassurance received as to the use of the data and the lawfulness of the data transfer in the receiving country have to be taken into account. In this context it is to be noted that in such a case, the data controller has a double obligation with respect to the protection of personal data: one imposed by the legal framework of the country where it resides and the one which is related to the data transfer. The local police should be informed afterwards. The police are required, wherever possible, to make use of existing international legal instruments, in respect of this type of data transfer. International transfers may also exceptionally occur where the police communicates personal data for humanitarian purposes.

Deleted: local

Comment [A33]: GER: The new wording is not adequate because it is always generally possible to contact the police. We should get back to the original text or - as a compromise - stick to the wording of Art 39 DPD: ...."involvement of police would be ineffective or inappropriate."

Deleted: compromise the purpose of the investigation

Example: In an investigation, carried out within the framework of an international multilateral agreement, into child sexual exploitation where the victim is in country Y and the police there have commenced an investigation, and the material has been made available on the internet by the suspect residing in another (country X) and there is a high risk that the suspect seeks to avoid justice by fleeing country X, the police in country Y can request, on an exceptional basis, that a service provider in country X provide the whereabouts of its customer. However, the police of country Y should inform the police in country X of its operation as soon as is possible and then seek to resolve the matter in cooperation.

15. Conditions for communications

Since there is a general obligation for the data controller to ensure a high level of data quality, it is advisable to have in place an additional check before sharing the data with others. When communicating or transferring data, it is always advisable to double-check the quality of data, if it is correct, up-to-date and complete. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated. It is required to establish secure channels of communication which ensure data security at the highest level possible. The quality of data can be assessed up to the moment of communication.

Example: If personal data that contain incorrect data (personal or otherwise) are sent they could adversely affect the investigation, cause harm to the individual concerned or others involved, or who may become involved as a result of the incorrect data being transferred. This can, as a result, leave the police in the transmitting and receiving states open to civil redress. In essence, if an individual is arrested based on a wrong communication of the suspect's name, it seriously harms several human rights of the individual concerned and can undermine any criminal investigation.

16. Safeguards for communication

It is of utmost importance that the necessity and purpose limitation principle should be applicable for any domestic communication or international transfer of personal data outside of police organisations.

Any data communicated should not be used for anything other than the purpose for which it was sent or received. The exceptions to this are when the sending authority, based on legal provisions, gives agreement to any further use, and if it is necessary and vital for the recipient to fulfil their task. Data can also be communicated if it is in the interest of the data subject,for humanitarian reasons, is necessary to prevent serious and imminent risk to public order or public security or an appropriate level of data protection is guaranteed by the recipient by international, national legal instrument, ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments, as foreseen by Convention 108.

Example: Personal data sent by the police of country X to the police of country Y in a money laundering case cannot be used by the police as profiling on the given individual in respect of her/his religious beliefs or political activities (unless those are relevant to the crime committed and police in country X has given its consent for this use).

17. Interconnection of files and on-line access to files

In specific circumstances the police may seek to collect data by coordinating its information with other data controllers and processors. Furthermore, it may combine personal data stored in different files or in different databases that are held for different purposes, such as those held by other public bodies and/or private organisations. This may be in relation to an on-going criminal investigation or to identify thematic trends in relation to a certain type of crime.

In order for these actions to be legitimate they must be authorised or be underpinned by a legal obligation to comply with the purpose limitation principle.

If the relevant police body has direct access to files of other police or non-police bodies, ir must only access and use the data if domestic law, which should reflect the key data protection principles so permits.

Clear legislation and guidance, which adheres to the data protection principles, should exist for cross-referencing of databases. Such cross referencing should be necessary, purpose bound and proportionate. With relation to personal data stored in other data controllers' or processors' data base all conditions described in Point 2 have to be fulfilled and regularly checked.

Example - Data held for citizenship purposes can only be used in an investigation if the national legislation allows it and to the extent to which it is necessary for the purpose of the investigation to do so. For instance, the number of children a suspect has may not be relevant in an investigation, and should therefore not be processed by police. Access in this case to a database can be perfectly lawful but it can only be legitimate if it respects the principles of data protection.

18. Data security

The police must take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The controller must notify, without delay, at least, the competent supervisory authority of those data breaches which according to its assessment may seriously interfere with the rights and fundamental freedoms of data subjects. The information of data subjects of data breaches which may seriously interfere with their rights may also have to be ensured without undue delay, unless it jeopardisese the task of the police.

Information security is essential to data protection. It is a set of procedures to ensure the integrity, availability and confidentiality of all forms of information within the police organisation, with the aim of providing security of data and information, and limiting the impact of security incidents and data breaches to a predetermined level.

The level of protection given to a database and/or an information system or network is determined by a risk assessment. The more sensitive the data are, the greater protection is required.

Authorisation and authentication mechanisms are essential to protect the data, and sensitive information should always be encrypted. It is considered best practice to have in place an audit regime to regularly check that the level of security is appropriate.

Police authorities are advised, where necessary, to conduct DPIA (see Point4) to assess the privacy risks to individuals in respect of the collection, use and any disclosure of information. This will help to identify risks and develop solutions to ensure that concerns are addressed appropriately. Any such impact assessment should cover relevant systems and processes of processing operations, but not individual cases.

A Data Protection Officer (DPO) within the police can play an essential role in carrying out internal audits and assessing the legitimacy of the processing, which contributes to a higher level of data protection and data security within the organisation. Moreover, the DPO can facilitate the dialogue between the organisation and the data subjects, as well as the organisation and the supervisory authority which can add to the overall transparency of the police body.

An Identity & Access Management System (IAM) may be recommended to manage employees and third party access to information. This will require authentication and authorisation to access the system and set privilege rights to determine what can be viewed. IAM can be seen as a useful requirement to ensure safe and appropriate access to data.

The data controller, following an evaluation of the risks, should at implement measures in respect of:

- equipment access control,
- data media control,
- storage control,
- user control,
- data access control,
- communication control,
- input control,
- transport control,
- recovery and system integrity,
- reliability and integrity.

Privacy-by-Design

The concept of privacy-by-design is an integral part of data security. Data protection and security may be embedded directly into information systems and processes, using technical and organisational measures, to ensure a high level of data protection and security and, in particular, to minimise the likelihood of data breaches. This approach is known as Privacy–by–Design, promoting privacy and data protection compliance from the start. It can be achieved through software and/or hardware. It requires a threat analysis, a full life cycle approach and rigorous testing.

Data controllers should ensure that privacy and data protection is a key consideration in the early stages of any project and then through its life cycle. Specifically, when building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have privacy implications and embarking on an information sharing initiative using data for new purposes.

Privacy-by-Design requires the implementation of Privacy Enhancing Technologies (PETs) to enable a better protection of personal data. PETs prevent unnecessary processing of personal data, without losing functionality in the information system itself.

Example: Body scanners used for police purposes have to be designed to respect the privacy of the individuals being inspected while fulfilling the purpose of their use. Therefore the body image in such tools has to be blurred by default.

19. External control

There has to be, at least, one supervisory authority responsible for ensuring compliance of data processing to the international and national legislation within the law enforcement sector.

Certain states may require more than one supervisory authority, for instance a national or federal authority and a number of decentralised or regional authorities, whilst others will prefer to have a single supervisory authority, responsible for the entirety of the supervision of data processing operations.

The supervisory body should be completely independent, meaning that it does not belong to the law enforcement organisation, nor is it directed by another body whithin the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties and should not be instructed or forced to accept instructions from anybody. The personal independence of its chair/president including political, financial, functional and operational independence, are decisive factors when judging how independent the supervisory body is.

National law should provide for advisory, investigative and enforcement powers to enable it to investigate complaints, to have regulatory measures or to be able to impose sanctions where needed. The legal and administrative tools at its disposal shall be efficient and enforceable.

Supervisory authorities should have the ability to cooperate in law enforcement matters bilaterally and also via the Committee of Convention 108.

Example: The supervisory authority must be independent and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

a. “personal data” means any information relating to an identified or identifiable individual (“data subject”);

b. “genetic data” are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

c. “biometric data” are data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual;

d. “soft data” (evidence based on testimony or other personal assessment) means data acquired through testimony of person involved in the investigation;

e. “hard data “ (evidence based on documents or proven facts) means data acquired from official documents or other certified sources;

f. “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

g. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

Deleted: h

h. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

Deleted: i

i. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

Deleted: j

j. Internet of Things (IoT): is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

Deleted: k

k. “covert surveillance” means all measures aiming at monitoring discreetly the movements of persons, vehicles and containers, particularly those involved in organised or cross-border crime.

Deleted: l

l. “special investigative techniques” techniques applied by the competent authorities in the context of criminal investigation for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person.

Deleted: m

m. “privacy-enhancing technologies” (PETs) means a range of different technologies to protect personal data within information systems. The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.

Deleted: n

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied to ensure the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").
Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed both its application and its relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[28] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level.
The present Guide was therefore prepared to highlight the most important issues that may arise in the use of personal data in the police sector and to point out the key elements to be considered in that context.
This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance.
The overarching principles set out in Recommendation (87)15 and their practical implications aim to ensure that the use of personal data by the police is determined in full respect of the rights of the individual to privacy and data protection.
To facilitate the reading of the Guide, a glossary of the terms used is provided at the end of the document.

General considerations

The collection and use of personal data for law enforcement purposes constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and, as such, it *must* be based on law (clear, foreseeable and accessible), pursue a legitimate aim and be limited to what is necessary and proportionate to achieve that legitimate aim. (Former second paragraph moved upfront)

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data within the police should be processed on predefined, clear and legitimate purposes set out in the law, they should be necessary and proportionate to these legitimate purposes and should always be in compliance with the original purpose. Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible.

1. Scope

The principles explained in the present guide apply to the processing of personal data for police purposes, primarily for the purposes of the prevention, investigation and prosecution of criminal offences, the execution of criminal penalties and for the maintenance of public order by the police (hereafter referred to as "tasks of the police"). Where 'police' is used in the text, it can be taken to mean wider law enforcement authorities, and/or other public and/or private bodies authorised by law to process personal data for the same purposes.

2. Collection of data and use of data

[28] See Report "Twenty–five years down the line" – by Joseph A. Cannataci

Deleted: for ensuring

Deleted: clear

Deleted: , aiming

Deleted: ing

Deleted: in the police

Deleted: are

Deleted: the a balance is struck between the essential objectives of general public interest (prevention, investigation and prosecution of criminal offences, the execution of criminal penalties and maintenance of public order), and the respect for

Deleted: processing

Deleted: based

Deleted: that it

Deleted: [in principle]

Deleted: The

Deleted: d

Deleted: It

Deleted: data which are processed within the police

Deleted: (Start) The collection and use of personal data for law enforcement purposes can constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and as such it *must* be based on law (clear and publicly available), pursue a legitimate aim/aim and be limited to what is necessary to achieve that legitimate /aimaim.

Deleted: specific

Deleted: offences and the

Comment [A34]: GER: DE sees no reason for putting this addition in parantheses pointing out that this could be a point for further discussion. This wording simply reflects Recommendation 87(15) which this Guide wants to give practical relevance.

Deleted: [

Deleted:]

The collection and use of personal data for police purposes should be limited to what is necessary and proportionate for the purpose of prevention, investigation and prosecution of criminal offences, the execution of criminal penalties (i.e. to a specific criminal offence(s) or the suspicion thereof) and for the purpose of the maintenance of public order. The police as data controller is responsible for all data processing it undertakes and is accountable for its data processing operations.

It is understood from Point 2.1 of the Recommendation that for the fulfilment of both of the main police tasks (prevention of a real danger and the suppression of a specific criminal offence), an evident and direct correlation should exist between the data processing carried out by the police and a situation where individuals have already committed or are likely to commit a crime.

The police should always choose the adequate legal basis to process personal data and should process personal data in a legitimate way. A careful assessment of the legal basis upon which the personal data is processed needs to consider the different operations during which the police is processing data.

The police should apply at all stages of the processing the relevant data protection principles (most importantly the principles of necessity, proportionality and purpose-bound data processing) and should not continue to process data which are not needed for the purposes. In this context, personal data collected at an early phase of the investigation, which then proves with the process of the investigation to be no longer relevant should no longer be processed (e.g. innocence of a suspect is confirmed), and should therefore either be blocked or deleted. This does not apply where subsequent use of the data is allowed.

Prior to and during the collection of data, the question of whether the personal data collected is necessary for the investigation or for a task of the police as described in Point 1, should always be considered. One should note that once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific task of the police) should exist. This link together with compliance with the data protection principles as described in this Guide must be demonstrated at all times. After the collection phase and at different stages of the investigation, a thorough analysis is needed to assess which data are to be retained and which are to be deleted.

Before collecting any personal data, investigators should ask themselves the question 'Why is it necessary to acquire the data?', 'What, exactly, do you seek to achieve?'

Example – For personal data such as Telephone Billing: only the number(s) required for the time periods being investigated should be sought and only for those individuals suspected of having a link with the offence.

A list of phone numbers of the person(s) involved in the suspected offence can be collected if there are indications that such data serve the purpose of the investigation. It cannot be kept or processed after the analysis shows that the data are not necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for police purposes should be used for those purposes only and should not be used for any other purpose that is incompatible with the original purpose stated at the time of collection, unless this is provided for in law (see Art 9 of Convention 108). [In assessing the compatibility of the use of data, one should consider the following criteria: (i) relation between purposes; (ii) context of the collection and information given to data subjects; (iii) nature of personal data; (iv) consequences for data subjects of the intended subsequent use; (v) existence of appropriate safeguards.]

Subsequent use of data is considered for the purposes of this guide as a new data processing operation which has to fulfil all the criteria and conditions mentioned above. The subsequent use of data shall be lawful, undertaken for a legitimate aim and necessary and proportionate to this legitimate aim.

The police shall ensure at all stages of the data processing and for the subsequent use of data as stated in the General considerations that the personal data are accurate, up-to-date, adequate, relevant and not excessive in relation to the purposes for which they are processed.

Deleted:
Deleted: be
Deleted: and
Deleted: where personal data is processed
Deleted: therefore
Deleted: it can be
Deleted: held
Deleted: has to be reiterated that according to
Deleted: in during
Deleted:
Deleted: The collection and use of personal data for law enforcement ...
Deleted: P
Deleted: e
Deleted: n
Deleted: (law, consent, contract, vit ...
Deleted:
Deleted: (e.g.: for testimonies cons ...
Deleted: P
Deleted: -
Deleted: ,
Deleted: principle
Deleted: they should be
Deleted: permanently
Deleted: such
Deleted: specific
Deleted: asked
Deleted: to
Deleted: e
Deleted: ,
Deleted: During collection, provided ...
Deleted: in order
Comment [A35]: DE: At the Paris ...
Deleted: Police should apply the da ...
Deleted: ¶
Deleted: .
Deleted: the relevant people.
Deleted: in any other way
Deleted: in law
Deleted:).
Deleted: for the same purpose,
Comment [A36]: DE: It is still not cl ...
Deleted: use
Deleted: applicable to the collection ...

Example: Police data collected for an investigation where the political affiliation is irrelevant, cannot then be used to determine the political affiliation of the concerned person unless provided for by law.

3. Subsequent use of data

Every subsequent processing of data by police (irrespective of the purposes of the original processing) for police purposes other than that the data were originally collected for, must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be undertaken for a legitimate aim and should be necessary and proportionate to the legitimate aim pursued.

Personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set out in Point 2. The general rule is that if data are likely to be used in a different case or in a different operation of the police, the assessment of compliance described in Point 2 shall be applied to this new processing as well. (This is not applicable if data are used for purely statistical or scientific purposes). Due to computerised and/or automated data processing and the large volume of personal data stored very often in different processing environments, the personal data collected and retained for police purposes should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

It should be noted, however, that any subsequent use of personal data of vulnerable individuals such as victims, minors, or of those enjoying international protection, should be subject to additional care and legal analysis with a special attention to the application of the principles of necessity and proportionality.

In cases such as trafficking in human beings, drug trafficking or sexual exploitation, where victims' data may subsequently be used also when they are considered as suspects, or where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to look at existing international good practice (in international or regional police bodies) and to enhance their exchange of information on the matter with other national police bodies. If all legal requirements as put forward in Point 2 are met, it should not represent any obstacle to the use of data of these persons for police purpose, but during these exchanges, confidentiality rules have to be followed.

Example - Data taken for tax purposes from a data subject can only be processed for law enforcement use by police () if the law allows it, if they are used for a legitimate aim and in a way that is necessary and proportionate to the aim pursued. In a concrete investigation of money laundering, the use of tax declarations' data of an individual can be envisaged to establish or deny a link between the individual and the money laundering operations.

4. Processing of special categories of data (sensitive data)[29]

Special categories of data, such as genetic data, personal data related to offences, criminal proceedings and convictions and related security measures, biometric data uniquely identifying a person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical nature, for instance additional security measures, and of an organisational nature, for instance having such sensitive data processed separately from the processing environment of the "ordinary" categories of data. Safeguards should be adjusted to each data processing operations taking into account their specificities and it is highly recommended to use multiple levels of protection for those categories of data (e.g.: separate main-frames, shorter data retention periods, etc.). It is of paramount importance to prevent unauthorised or unwanted access to those categories of data even with additional security measures.

A careful balance of interests taking into account the purpose of the investigation, the context and the nature of the data is necessary to determine whether or not, and to which extent, the police could process sensitive data. For instance, it would be advisable to differentiate when biometric data is processed by the police

[29] Paragraph removed from previous Point 8

Deleted: ¶
¶
Deleted: fact that the original processing has been carried out for a police purpose or for other purposes
Deleted: ~~same~~
Deleted: Due to the nature of data processing, it is possible to use personal data collected for one purpose for another, personal data collected and retained for police purposes should not be kept and processed in an ...
Deleted: specific, well-defined
Deleted: point
Deleted: a
Deleted: for
Comment [A37]: DE: see comment ...
Deleted: the
Deleted: tests
Deleted: .
Deleted: all data held by police shou ...
Deleted: isz
Deleted: the
Deleted: nature of data processing ...
Deleted: in an unstructured manne ...
Deleted: data, in particular in respe ...
Deleted: which shall include ...
Deleted: ,
Deleted: other
Deleted: This
Deleted: does
Comment [A38]: DE: This paragrapl ...
Deleted: if all legal requirements as ...
Deleted: .
Deleted: Biometric d
Deleted: immigration medical
Deleted: such as checks against ...
Deleted: allows
Deleted: it and appropriate ...
Deleted: Any such use should be ...
Deleted: The purpose of appropriate ...
Deleted: of
Deleted: its
Deleted: anonimisation,
Deleted: which takes
Deleted: can
Deleted: on the top of personal ...

whether it is for identification purposes (where for instance 2 fingerprints could suffice) or it is for crime investigation purposes (where more fingerprints could be needed).

The use of Data Protection Impact Assessments (DPIA) is recommended in order to ensure that appropriate safeguards are put in place. The data controller should assess and demonstrate whether the purpose of the processing can be achieved in a manner that impacts less on the right to privacy and data protection and if the processing of special categories of data does not represent a risk of discrimination for the data subject.

Regarding these data the potential risk of negative discrimination or of adverse legal effect significantly affecting the data subject should be avoided, since all profiling based on sensitive data resulting in negative discrimination are prohibited. In this context, besides measures detailed above, the use of PETs and more frequent checks on the lawfulness of the processing can be recommended. This could, for example, translate into measures put in place to counter the assumption that individuals belong to a criminal organisation because of where they live, where a criminal organisation is active or where the individuals have the same ethnic origin.

Example - Targeting groups or individuals based solely on religious beliefs would not be allowed. However, in an investigation into a group of individuals engaging in possible terrorist activities that were attached to a particular religious group, it could be of importance to process data specific to the followers of this specific religious group (related to worshipping place, religious preachers, customs, teachings, members and structure of the religious community, etc. that was pertinent to the investigation). However, targeting all followers of a religion, purely because of their religious belief is strictly prohibited.

5. Providing information to data subjects

One of the most important obligations of a data controller is to provide information on data processing to data subjects. This obligation is two-fold: it requires the data controller to provide *general information* on the data processing that it carries out and to give *specific* information to data subjects if no restrictions or derogations apply to the data processing.

Information provided to the wider public, should promote awareness, inform them of their rights and provide clear guidance on exercising their rights regarding these files. The information provided should be effectively and broadly accessible. Moreover it should include details about the conditions under which exceptions apply to the data subject's rights and how they could submit an appeal to the DPA or to the judiciary.

Websites and other easily accessible media perform a role in informing the public. It is recommended to have in place letter templates on these websites or other media to help the data subjects exercise their rights. It is the responsibility of the data controller to provide information which adequately highlights data protection and data subjects' rights.

In order to comply with the second obligation of giving data subjects specific information regarding data processed, the police shall inform data subjects on the data processing envisaged or, if it is not possible, before the processing for objective reasons, shortly after it. This communication shall comprise information on the data processing, on the collection of the individuals' data and comprehensive information on their rights.

The obligation to provide specific information implies that, in principle, the data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.

The information should be provided unless a restriction or derogation applies as described in Point 7. When applying the provisions allowing for restrictions and derogations account should be taken of the specific nature of sensitive files, such as criminal intelligence files, files containing sensitive data, in order to avoid prejudice to the performance of police functions or to the rights of individuals. Even if restrictions or derogations to the

Deleted: 8 to 10…ore fingerprints ...

Deleted: A greater…he use of Data ...

Deleted: as…all profiling based on ...

Deleted: to…targeting all followers ...

Deleted: It should be noted that t…l ...

Deleted: The *general obligation* implies that, in principle, the data subjects are provided with, details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights. The information provided should strike the balance between all interests concerned and also, most importantly, take account of the specific nature of ad hoc or temporary files and other particularly sensitive files, such as criminal intelligence files, in order to avoid serious prejudice to police in performing their functions.¶

Deleted: The i…nformation provide ...

Deleted: as best practice …o have i ...

Deleted: According to the second obligation of giving data subjects specific information regarding their data processed by police *ex officio*, it responds to the general principle that an individual should always be in control of her/his data. …n order to ...

Deleted: taking into …ccount shou ...

Comment [A39]: DE:It is assumed that the suggested changes reflect better what is meant. Clarity is crucial here.

Comment [A40]: DE: this conflicts with the approach in the DPD.

Deleted: serious

Deleted: …rejudice to the ...

right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.

Very often data subjects, because of restrictions or derogations of their right to information, cannot receive complete information on the processing the police undertake with their data; this should not affect the possibility of their exercise of the right of access which can have restrictions on its own merits.

Example - For the purpose of covert monitoring of a high risk sex offender, data processing and long-term data retention may be justified without informing the individuals under surveillance if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved, the data subject should be informed about the fact that she or he was subject to such measure.

6. Data subject's rights[30]

Accessing their personal data is a fundamental right for data subjects.
The right to access their personal data on request, the right of rectification and the right of erasure are interdependent rights.

In case an individual´s data is collected during the course of an investigation or other tasks of the police as described in Point 1, as soon as circumstances safely permit, the police [in principle] should grant the individual access to the data processed if there is such request. The access should be provided in clear and plain language. The communication has to contain the same information as described in point 5, unless data subjects wish otherwise.

The law can provide, under the strict conditions described in Point 7, that the right of access upon request may also be limited or excluded, should the provision of such information prejudice the investigation or another important police task, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified.

The police should aim to answer even general questions arising from data subjects on the processing activities in relation to their personal data, but can use standardised forms to facilitate communication.

Example: If a data subject asks the police on data it processes on them, the police, if no exception is applicable, should provide a detailed answer with legal references, but should do so in a plain language, avoiding uncommon or specialised expressions.

The right of access should, in principle, be free of charge.

It is possible to charge a reasonable administrative fee for the request, if national law permits and the request is manifestly unfounded or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such refusal.

To ensure a fair exercise of the right of access, the communication "in an intelligible form" applies to the content as well as to the form of a standardised digital communication. It is, however, advisable to refer to national legislation to ensure consistency and to avoid suspects utilising this method to find out whether there is an on-going investigation into them.

In respect of direct access, the data subject can request access to the controller of the files. The data controller will assess the request and any possible restriction or derogation which can only be used if it is vital for the performance of a specific police task as described in Point 1, or it is necessary for the protection of the data subject or the rights and freedoms of others, and reply directly to the data subject. In case of a

[30] Paragraph removed from previous Point 17.

Deleted: is
Deleted: t
Deleted: s
Deleted: ing
Deleted: any more
Comment [A41]: DE: attempt to clarify.
Deleted: ¶
Deleted: a
Deleted: the
Deleted: in relation to their personal data
Comment [A42]: DE: assuming that the Guide now wants to turn to the rights of access, erasure and rectification.
Deleted: to information
Deleted: , the right of access
Deleted: The right to access is a prerequisite for the exercise of other rightsinformation covered under Point 5 is a prerequisite to right of access; the data subject has the right to know about the data processing which is made on theirpersonal data and on the basis of this information, exercise other rights. It shall be noted nevertheless that there is no systematic link between access rights and the data controller's obligation to inform data subjects in ...
Comment [A43]: DE: That has alred ...
Deleted: ¶ ...
Deleted: i
Deleted: has her/his
Deleted: inform
Deleted: of
Deleted: ing
Deleted: information
Deleted: given upon request as soo ...
Comment [A44]: DE: There is, as it ...
Deleted: as
Deleted: to be informed
Deleted: providing
Deleted: , for instance
Deleted: ,
Deleted: Very often data subjects, ...
Deleted: P
Deleted: the
Deleted: using
Deleted: a
Deleted: of approach
Deleted: of the police

restriction, partial information, and in case of derogation, information on the use of derogation, shall be still given, with the motivation for using such measures in both cases, as well as information concerning redress.

Example: The access request can be refused if there is an on-going investigation on the person, and providing the data subject access to the data could compromise such investigation.

If restriction or derogation were to be used, any answer should take into consideration, according to national law or practice, all circumstances to which the restriction or the derogation is applicable.

As a rule, domestic law should, ideally, provide for direct access. If the right of access provided for is indirect, the data subjects may direct their request to the supervisory authority, which after being properly mandated, will carry out the request on their behalf and conduct checks regarding the availability and lawfulness of the processing of the data subject's personal data. The supervisory authority will then reply to the data subject (providing what data it is possible to release, subject to any legally allowed restrictions or derogation). In case of a restriction or derogation, the same communication should be made possible as in case of a direct access.

The data controller should consider the request and reply to the data subject within a reasonable time limit, as provided for by domestic law.

There should be arrangements in place to confirm the identity of the data subject before access to any data is granted as well as to obtain information on the processing activities to which the request refers. The same holds if the data subjects delegate the authority to someone else to exercise their rights.

It is an essential right of the data subjects to be able to amend any incorrect data held on them. If the data subject finds data that are incorrect or irrelevant, she/he should have the right to challenge it and ensure that they are amended.

In some cases, it may be appropriate to add additional or corrective information to the file. It is important to underline that this right can only be exercised with due respect to other individuals' rights, for instance to the rights related to a testimony in a criminal case (which does not preclude per se the exercise of the data subjects' rights related to soft police data).

If the data to be corrected or erased has been communicated elsewhere the relevant authorities should be informed of the changes to be made.

All proposed changes should be supported by evidence. If data subjects can prove by use of the official documentation that the data processed by police in respect to them are incorrect, the data controller shall not have the right of discretion whether to correct them.

It may be necessary for the police, as dealt with under Point 7, not to give information or grant the right of access, of deletion and of correction which might jeopardise an investigation and should therefore be excluded for its duration. Similar restrictions or derogation may be imposed by national law as described in Point 7.

Restrictions or derogations to the rights of data subjects should only apply to the extent necessary and be interpreted narrowly. Every data subject's request should be considered carefully on a case-by-case basis. Any decision to refuse a data subject's request should be provided in writing (including by electronic means). The response should provide clear justification of the decision making which can be verified by an independent authority or a court. It is possible that communicating the reasons for refusal could pose a risk to law enforcement or the data subject or to the rights and freedoms of others. If this is the case, it should be documented and provided to the independent authority or court to be verified, if required.

Example - If person A submitted a declaration against person B accusing her/him of committing a serious offence and later it emerges that the accusation was false, it might be relevant for the police to retain the

Deleted: the

Comment [A45]: DE: Suggestion to use the term "consider" in order to avoid an understanding of the "assessment" process as a process in which the controller checks if the request is relevant etc. - which is not the case. The controller has no discretion regarding the request (except in order to apply derogations and excemptions).

Deleted: assess

Deleted: s

Deleted: ,

Deleted: excessive

Deleted: or deleted

Deleted: Data subjects can ask for the deletion of their personal data where such processing is unlawful. ¶

Deleted: of

Deleted: assessed

Deleted: ¶
A data subject may be required, as per national legislation, to obtain a copy of their police file. However, to obtain a written copy or statement may not always be in their interest or feasible for the police and therefore in such cases domestic law may authorise oral communication of the contents.¶

false statement and the personal data surrounding it.

Although the statement was proven to be false, if the police requires the retention of the surrounding data, a clear corrective statement on the file, instead of removing the data surrounding false statement, would be necessary.

The data subject should be informed of all available options following a decision to refuse and/or to restrict granting data subject´s rights such as an appeal either to the supervisory authority, to court or to another independent administrative authority.
Depending upon national legislation, specifically whether there is a direct or an indirect right of access, the actual communication of the result of the review or appeal may differ. It is possible that the inspecting body cannot communicate the data to the individual even if there is no justification for refusing access. In this case the data subject should be informed that a verification of the police file has taken place. Alternatively, the inspecting body may request the police to release the data contained in the file to the data subject. The court or tribunal may have powers to enforce the access, correction or deletion of data from the file even in access-request cases referred to them by police or the supervisory authority.

Example: If police sends a refusal letter it should contain the name, address, web address, etc. of all possible fora for redress.

The data subject should have access to a court or tribunal in order to submit an appeal, and have the reasons for refusal verified if they are not satisfied with the reply given by the supervisory authority or the independent authority. The supervisory authority should have sufficient powers to examine the police file concerned and have the assessment communicated.

7. Exceptions from the application of data protection principles

Under the European Convention on Human Rights and Convention 108, exceptions can only be used if foreseen by law (the law should be public, open and transparent and, in addition, detailed enough) and they constitute a necessary and proportionate measure in a democratic society.

Exceptions can be applicable to those principles described under Points 2,3,,5,as well as to the data subjects' rights (Point 6). The exceptions which have to be incorporated into national legislation should serve a well-defined purpose, in particular to avoid obstruction of activities undertaken for the purpose of the protection of national security, or for the purposes of defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest (which includes purposes in connection with the fulfilment of a state's international legal commitments or obligations, most prominently deriving from the binding decisions of United Nations' bodies, and humanitarian purposes,) or the protection of the rights and fundamental freedoms of others.

Example - If giving information to a data subject may endanger the safety of a witness or an informant; this right can be limited in light of such circumstances.

If the exception, as defined by national law providing specific safeguards is used by the police, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. The aim of using exceptions by the police should be limited to cases where the use of those rules and principles would endanger tasks of the police described under Point 1.

Example: If data collected for a police purpose in an investigation are likely to serve national security purposes they can also be used to this latter purposes to the extent set forth by national legislation. If specific intelligence proves that money laundering operations have been carried out to finance terrorist operations, data collected on individuals during the investigations on money laundering can be used for the purpose of eliminating the close and imminent terrorist risk.

8. Use of special investigative techniques

Comment [A46]: DE: It has to be made clearer that in this example it is not the personal data that is false but the statement.

Deleted: information

Comment [A47]: DE: Suggestion to make it even clearer that it is not the personal data processed are false but the accusation itself.

Deleted: retaining

Deleted: refusal decision

Deleted: um

Deleted: ¶

Deleted: should be

Deleted: exceptions

Comment [A48]: DE: Is this supposed to mean now that exceptions can only take effect in cases where the data processing (deviating from the dp principles) serves one of the following purposes? In my understanding the following purposes shall be the underlying reasons for invoking exceptions from the data protection principles themselves. That has to be made clearer (see suggestion).

Deleted: and have to be incorporated into national legislation in a manner compatible with the ECtHR jurisprudence

Deleted: ¶
¶
Exceptions can be applicable to those principles described under Ppoints 2,3,4,5,7 as well as to the data subjects' rights (Ppoint 176)

Deleted: in case of some specific purposes in relation to which data processing activities are undertaken. In particular it they affectsconcerns those

Deleted: from international

Deleted: obligations

Deleted: ,

Deleted: Other applicable exceptions are foreseen in Article 3 Convention 108.

Deleted: ¶

Deleted: ,

Deleted: based on

Deleted: the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police

Deleted: ¶
Example - If giving information to a data subject may endanger the safety of a witness or an informant; ...

Formatted: Highlight

Deleted: ¶ ...

The police should always adopt the least intrusive means of data processing during its operations. If less intrusive methods can be used to achieve the desired ends, they should be preferred. The use of special investigative techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods. Regardless of the method of investigation or other operation led by the police, the police is obliged to comply with the general principles of data protection as described in General considerations, unless a law expressly exempts from it.

With increasingly sophisticated technological developments, electronic surveillance has become easier, however, the use of these techniques can interfere with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the high potential of severe interference with the right to privacy has to be balanced with the efficiency of investigations.

Example: In an investigation, the evidence for communication between two suspects can be gathered in various ways. If, by the use of interrogations, testimonies, the obtaining of call data or discreet surveillance, the same result can be achieved without jeopardising the effectiveness of the investigation, it is to be preferred to the use of more intrusive surveillance measures, such as wiretapping.

9. Introduction of new data processing technologies

If the introduction of new technologies is likely to result in a high risk to the individual's rights, the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity. The relevance of the DPIA shall be checked at reasonable intervals.

It is also of great importance, that in terms of data security and safety of communications, the highest standard is taken into account when introducing such technologies.

Example - New data mining techniques may offer extended possibilities for identification of possible suspects and should be assessed carefully for their compliance with existing data protection law, including with regard to data security.

The data protection authority has an important role in advising which risks are involved for data protection and which safeguards should be provided to ensure that any technical means comply with data protection law. However, the police do not have an obligation to turn in every case to the supervisory authority where it introduces new technologies. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights.

The consultation between the supervisory authority and the data controller should provide the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.

Appropriate details should be provided to the supervisory authority, in particular regarding the type of file, the data controller, data processor, the legal basis and the purpose of the data processing, the type of data being processed and by whom the data is being accessed, as well as information on retention of data, log policy and access policy, and other relevant technical aspects of implementation.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data could be reported to or made available for consultation to the data protection authority.

Following consultation, the data controller should consider carefully to implement any necessary measures and safeguards that have been recommended by the data protection authority.

Deleted: it must be remembered that

Deleted: those considerations

Deleted: have

Deleted: cost-effectiveness, use of resources and

Deleted: covert

Deleted: Use

Deleted: It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance to existing privacy and data protection standards. It is also of great importance, that in terms of data security and safety of communication, the highest standard is taken into account when introducing such technologies.¶

Deleted: processing

Deleted: continuous (i.e.

Deleted:)

Deleted: should

Deleted: every

Deleted: by

Deleted: or the national legislation does not provide sufficient clarity on the implementation of these methods

Deleted: be defined in a way that

Deleted: s

Deleted: During the process with the supervisory authority the focus should be on mitigating the specific negative impacts that the data processing would represent to the right to privacy and to data protection.¶
¶
The consultation between the supervisory authority and the data controller should be defined in a way that provides the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.¶
¶
During the consultation process appropriate

Deleted: contained

Deleted: important

Deleted: are to

Deleted: Data protection authority is preferably to be consulted during the legislative procedure.

Example - Introducing an automatic facial recognition system or other system based on the automated processing of biometric data would be very likely to need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed and recommended by the data protection authority after being consulted on the issue, specific safeguards should be put in place (concerning the data retention time, the cross matching functionalities, the place of the storage of data and the access to data issues, etc.) to comply with data protection principles and provisions

Use of the Internet of Things (IoT) technology in police work

Data sent to and from police during operational activity via the internet are good examples of the IoT already in use. Due to potential security vulnerabilities, IoT requires measures such as data authentication, access control to ensure data security and resilience to (cyber) attacks.

Example: In light of their potential security vulnerabilities, smart glass used by police should not be directly connected to a national criminal record data base and data collected should be guaranteed a high level of security.

Big data analytics in the police

Technological advances in processing and analysing large and complex data sets leading to big data and big data analytics present opportunities and challenges to the police, who is turning to digital sources and profiling techniques to perform their tasks.

Big data technologies enable bulk collection and analysis of a vast quantity of data generated by electronic communications and devices aggregated with other bulk data. This could interfere with the right to privacy and data protection.

The Council of Europe's Recommendation CM/Rec(2010)13[31] on the protection of individuals with regard to automatic processing of personal data in the context of profiling and the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[32] can be of use in the context of Big Data analysis for police use too.

Big data technologies and analysis techniques may help assist detecting crime, but there are, however, considerable risks to this type of data processing that should be taken into account:

- Databases originating from one domain can be used in another domain and for another purpose, which changes the context and may lead to inaccurate conclusions and lack of valid legal basis, therefore to unlawful data processing with possibly serious consequences for the individuals involved.
- Profiling may lead to drawing discriminatory conclusions, which can result in the reinforcement of stereotypes, stigmatisation and discrimination.
- The increasing amount of personal data held in databases may lead to severe vulnerabilities and subsequent risk of data breaches if information security is not guaranteed.

Where big data relies on personal data, data controllers should pay additional attention to the following requirements:

- Verification of data accuracy, context and relevance of the data.
- Its use requires a high level of accountability.
- Its use shall be combined with methods of investigation which complement the conclusions drawn. A decision affecting a person shall not be taken solely on automated processing of personal data.
- As for other types of data processing, it is of paramount importance that its use shall be ~~shall be be~~ necessary and proportionate for the fulfilment of police tasks described in Point 1, with special attention

[31] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[32] Document T-PD(2017)1 - Big Data Guidelines

Deleted: which is directly linked to relevant databases

Deleted: ; they should gather information which is to be downloaded to a secure IT environment for further analysis

Deleted: *and profiling*

Deleted: are

Deleted: legal

Deleted: way of processing data

Deleted: potentially and inadvertently

Deleted: ¶

Deleted: take

Deleted: due account of

Deleted: traditional less intrusive other

Deleted: to

Deleted: such

Deleted: ized

Deleted: l

Deleted: use

Deleted:

for the data processed to be adequate, relevant and non-excessive in relation to the purpose for which they are processed.

- Predictive analysis requires human intervention to assess the relevance of the analysis and conclusions.
- Ethical guidelines developed at national or at international level should be taken into consideration.
- As a principle and subject to restrictions and derogations mentioned in Point 7, transparency should be ensured by the data controller by explaining how the data are processed in accordance with privacy and data protection principles. If data collected for one purpose is used for another purpose, the data controller should in principle make the data subjects aware of this subsequent use.
- Even if complex methods are used, the lawfulness of the processing – including subsequent use of data - and compliance with the conditions set by Article 8 ECHR and Convention 108 should be demonstrated.
- An information security policy should be in place and implemented throughout the processing.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals and the administrative and judicial means exist for individuals to challenge those decisions. This implies data subjects' awareness of the reasoning of the algorythm used and the purposes for which it was used.

The above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones, are even more necessary when sensitive data are processed in Big Data analytics.

10. Storage of data

"As pointed out in Point 2" data shall be processed until they have served the purpose for which they were collected. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

There should be a clear distinction in how the police stores and processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses. This should also relate to the specific purpose for which the data was collected. Additional safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence. Clear rules have to be established in relation to the handling of different data bases with special attention to the analysis of multiple results.

The principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve the purpose of the prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where personal data is processed for the purpose of the maintenance of public order.

The grounds for retention and processing should be reviewed periodically. The unlawful processing of personal data outside of the legal framework allowed for the retention constitutes a severe violation of the right to protection of personal data. If the law in relation with a specific crime provides for a data retention period of 4 years and if an individual is kept in custody by the police solely on this ground after 4 years have passed since the collection of the data in question and no legal ground to process this data exists, the retention of this data could be considered as unlawful.

General data retention periods are usually regulated in national or international law. In order to comply with the legislation while ensuring the effectiveness and the success of an investigation police bodies are strongly advised to develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data.

For example, in a case where the law prescribes a 4 year data retention period but the individual subject to an investigation is acquitted from all charges by the court after 2 years, her/his data shall be deleted (if the individual is not a recidivist or there is no information on her/him committing again the same category of crime) from the database, provided that all deadlines for the review of the case have expired. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

Deleted: purpose
Deleted: notably
Deleted: Where possible
Deleted: provided
Deleted: compatible
Deleted: secondary
Deleted: and/or lengthy processing are undertaken L
Deleted: be
Deleted: allow the data subjects to know the
Deleted: ensure transparency
Deleted: h
Deleted: for to avoid any negative discriminatory action
Deleted: If data are no longer relevant for the purpose collected, they should be deleted, unless subsequent processing is possible on the grounds put forward in Point 3. S
Deleted: s
Deleted: S
Deleted: queries in
Deleted: can
Deleted: and evidence gathered in this way can be seen as unlawful
Deleted: retained
Deleted: , 4 years later the evidence based solely on
Deleted: and the measures undertaken by the police based solely on this data
Deleted: possibly
Deleted: by the court
Deleted:
Deleted: revision
Deleted: also

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judicial procedure terminates completely (which means all redress have been made or all deadline for redress have been passed).

The police should provide systems and mechanisms to ensure that the data that are stored are accurate and that their integrity is maintained.

International obligations, which include providing data to international bodies such as Europol, Eurojust and INTERPOL, bilateral agreements and mutual legal assistance between member states and third countries must be observed when shaping internal policies.

Data should be categorised according to the degree of accuracy and reliability in order to assist the police in their activities. It is recommended that handling codes are used to distinguish these categories. A classification system facilitates the assessment of the quality of the data and how reliable it is. Classification of data is also important when it is to be communicated to other police bodies or states.

Example - Information collected directly from a person's statement will be assessed differently than information collected from a person's hearsay statement. Data based on facts, or 'hard' data, will be assessed differently than data based on opinions or personal assessments, or 'soft' data.

Personal data collected by police for administrative purposes must be kept (as far as possible: logically and physically) separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by law.

Examples of administrative data include lists of data on licence holders or data on human resources and firearms certificates.

11. Communication of data within the police sector

A distinction should be made between domestic communication of data and international transfer of data. Within these two distinct operations different requirements apply, depending upon who is receiving the data, whether it is the police, another public body or a private party. The police can only communicate personal data within the police sector if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

There should be clear and transparent rules on how the police grant access to data held by it and on which grounds.

The police, domestically, should only share information (among police) when there is a legal basis for the request, e.g. an on-going criminal investigation or a shared law enforcement task and laws or agreements allowing the communication

The police can share data with other police organisations if the personal data are relevant for the purpose of prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where they are processed for the purpose of the maintenance of public order.

The communication of personal data in general should be in line with the general considerations described above.

Example: A police unit can share data on a suspect who presumably committed a tax fraud with another police unit investigating a murder case if there is indication that the suspect for this crime could be the same person or if doing so will materially assist the investigation.

Deleted: the

Deleted: of the data

Deleted: When shaping internal policies i

Deleted: This uses a

Deleted: to

Deleted: if feasible

Deleted: the

Deleted: ent

Deleted: As a general rule p

Deleted: that

Deleted: is

Deleted: personal data

Deleted: is

Deleted: subject to the principle of necessity and proportionality and has to serve the above mentioned purposes

Deleted: G

12. Communication of data by the police to other public bodies

The communication of data outside police is permissible if it is provided for by law and the data are required by the recipient to enable them to fulfil their lawful task. Mutual assistance agreements foreseen by the law between law enforcement and public bodies allows the public bodies to have access to law enforcement data which would be essential in the fulfilment of their duties and tasks (for example in their investigations or other legal duties in accordance with national law).

Stricter principles than those set forth in Point 11 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the processing of personal data, which are considered sensitive, could result in adverse effects for the individual.

Communication of data to any other public authority may also be allowed if it is foreseen by law, is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to other persons or to public order or to public security.

The communicated data may only be used by the receiving body for the purposes for which the data were transferred.

Example - A claim for a residence permit made by a migrant. Police data may be required to verify if the person was ever involved in criminal activity. It would be in the interest of the Immigration Office and the claimant for this communication of data to take place.

13. Communication of data by the police to private parties

There may be occasions when, under strict conditions, the police can communicate data to private bodies. This communication has to be based in law and can only be done by the authority which is processing the data. Such communication can only be done for the purpose of the investigation or other important police tasks as described in Point 1, in the interest of the data subject, for humanitarian reasons or if it is necessary to prevent serious and imminent risk to public order or public security. For example, there might also be instances where police data may be communicated to humanitarian organisations based on international law, in the interest of the data subject or for humanitarian reasons.

Where the police shares data with media in respect of making information related to an investigation public, special consideration should be given to the assessment to determine that it is necessary and in the public interest that such publicity is allowed.

Such communication should only be on a case by case basis and in each case there must be a clear legal basis providing the necessary procedure (e.g. need for specific authorisation) to be followed for any such communication to occur.

Example - When the police communicate with the financial sector in relation to known fraud or theft offenders, when it communicates with an airline about stolen or lost travel documents or when the police releases details of wanted persons believed to pose a risk to the general public.

14. International transfer

Any transfer of police data internationally should be limited to police bodies and should be fit for purpose and in accordance with the law. For this, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data handling, regional legal frameworks such as EU and EU institutions' legislation (on Europol, Eurojust, Frontex, etc.) and subsequent agreements (operational bilateral agreements), bilateral treaties and in general, international agreements on

Deleted: is

Deleted: m

Deleted: 0

Deleted: criminal

Deleted: the communicated data

Deleted: be used for non-law enforcement purposes

Deleted: negative discrimination

Deleted: against

Deleted: In practice detailed ¶ ¶ As an exception, c

Deleted: as

Deleted: missions

Deleted: which should

Deleted: e

Deleted: they

Deleted: wanted who are

Deleted: organisations

Deleted: contained within its legal framework

mutual assistance, or other bilateral or multilateral agreements made regarding effective cooperation can be of use.

When considering sharing any data, consideration should be given as to whether the receiving authority is performing a function conferred to it in law related to the prevention, investigation, or prosecution of criminal offences, the execution of criminal penalties and the maintenance of public order, and whether the sharing of the data is necessary to perform its specific task.

The sending authority should ascertain that there is an appropriate level of data protection in the receiving state and that the receiving state complies with the relevant rules of international transfers of personal data. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. This means of transfer should be used as a last resort option. International transfers framework such as "INTERPOL's Rule on the Processing of Data" and its "Statute of the Commission for the Control of INTERPOL's files" Rules on the Control of Information and access to INTERPOL's Files", the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185) may be taken into account[33] so as to ensure that any transfer of data is legally justified and has appropriate safeguards in place. The request should clearly state all the necessary elements from the requesting party to enable the receiving party to make a sound decision on the request. These details would be expected to include the reason for the request as well as the purpose for the transfer of data.

An appropriate level of data protection should be guaranteed (e.g. through ad hoc or - if this condition applies in the relevant domestic law - approved safeguards or guarantees provided by the recipient or entailed in legally binding and enforceable instruments) if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

If there are conditions applied by the sending authority in relation to the use of the data in the receiving state these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout its lifecycle.

Example - Further transfer of data should only be allowed if this is necessary for the same police purpose as the original transfer and the second recipient is also a police body ensuring an appropriate level of data protection. The police body which originally sent the data must also consent to the onward transfer. If the police from country X sends personal data to the police of country Y it is only permissible for the country Y to transfer this data if above all requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) if country X consents to the transfer. If the data is sent to country Z which is a non-member of the Convention 108, then country Y should ascertain that this country provides an appropriate level of protection of personal data including the existence of effective means of exercise of the related data subject rights

The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases if it is required for the performance of the task of the transferring authority and there is no effective means of transferring the data to a competent police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers.

Example: If tax authorities in country X requests the police in country Y about the whereabouts of a person involved in non-criminal tax evasion because they have evidence that the person is involved in criminal matters in country X, the police can transfer the personal data of the individual.

The international transfer of personal data between police and private bodies in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police as described in Point 1, provided by legal means and where

[33] This is without prejudice to the right of the Committee of Convention 108 and other instances disposing such power to assess and to review if necessary the level of data protection guaranteed by those multilateral agreements

Deleted: ,
Deleted: in respect
Deleted: Interpol's "Rules Governing the Processing of Data
Deleted: can be applicable
Deleted: in place
Deleted: to
Deleted: standardised
Comment [A49]: DE: Here the wording has to distinguish between ad hoc safeguards on the one hand and safeguards provided by legally....instruments. Furthermore, in the police area there are not always approvals of safeguards.
Deleted: its
Deleted: onward
Deleted: specific
Deleted: with
Deleted: has, in place, appropriate legal protection in terms of personal data processing and can guarantee an
Deleted: level for the
Deleted: and
Comment [A50]: DE: That is part of the assessment on if there is an appropriate level of dp.
Deleted: .
Deleted: it has
Deleted: police
Deleted: to
Deleted: a
Deleted: y
Deleted: residing

the emergency, the gravity of the crime, its trans-border nature and where the involvement of the local police would compromise the purpose of the investigation for objective reasons. Other facts as data security, the reassurance received as to the use of the data and the lawfulness of the data transfer in the receiving country have to be taken into account. In this context it is to be noted that in such a case, the data controller has a double obligation with respect to the protection of personal data: one imposed by the legal framework of the country where it resides and the one which is related to the data transfer. The local police should be informed afterwards. The police are required, wherever possible, to make use of existing international legal instruments, in respect of this type of data transfer. International transfers to private bodies may also exceptionally occur where the police communicates personal data for humanitarian purposes.

Example: In an investigation, carried out within the framework of an international multilateral agreement, into child sexual exploitation where the victim is in country Y and the police there have commenced an investigation, and the material has been made available on the internet by the suspect residing in another (country X) and there is a high risk that the suspect seeks to avoid justice by fleeing country X, the police in country Y can request, on an exceptional basis, that a service provider in country X provide the whereabouts of its customer. However, the police of country Y should inform the police in country X of its operation as soon as is possible and then seek to resolve the matter in cooperation.

15. Conditions for communications

Since there is a general obligation for the data controller to ensure a high level of data quality, it is advisable to have in place an additional check before sharing the data with others. When communicating or transferring data, it is always advisable to double-check the quality of data, if it is correct, up-to-date and complete. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated. It is required to establish secure channels of communication which ensure data security at the highest level possible. The quality of data can be assessed up to the moment of communication.

Example: If personal data that contain incorrect data (personal or otherwise) are sent they could adversely affect the investigation, cause harm to the individual concerned or others involved, or who may become involved as a result of the incorrect data being transferred. This can, as a result, leave the police in the transmitting and receiving states open to civil redress. In essence, if an individual is arrested based on a wrong communication of the suspect's name, it seriously harms several human rights of the individual concerned and can undermine any criminal investigation.

16. Safeguards for communication

It is of utmost importance that the necessity and purpose limitation principle should be applicable for any domestic communication or international transfer of personal data outside of police organisations.

Any data communicated should not be used for anything other than the purpose for which it was sent or received. The exceptions to this are when the sending authority, based on legal provisions, gives agreement to any further use, and if it is necessary and vital for the recipient to fulfil their task. Data can also be communicated if it is in the interest of the data subject for humanitarian reasons, is necessary to prevent serious and imminent risk to public order or public security or an appropriate level of data protection is guaranteed by the recipient or entailed in a legally binding instrument, as foreseen by Convention 108.

Example: Personal data sent by the police of country X to the police of country Y in a money laundering case cannot be used by the police as profiling on the given individual in respect of her/his religious beliefs or political activities (unless those are relevant to the crime committed and police in country X has given its consent for this use).

17. Interconnection of files and on-line access to files

Deleted: the

Deleted: the fact that

Deleted: because of the length of the procedure

Comment [A51]: DE: clarification.

Deleted: As

Deleted: or transferring

Deleted: ,

Deleted: and data based on opinions or personal assessments cheked at source before being communicated and their degree of accuracy or reliability indicated

Deleted: seems

Deleted: to be preferable

Deleted: transfers

Deleted: is sent

Deleted: s

Deleted: it can

Deleted: the

Deleted: only

Deleted: is

Deleted: and if the processing is based on law,

Deleted:

Deleted: safely

Deleted: ,

Deleted: or

Deleted: or

Deleted: and

Comment [A52]: DE: see comment above.

Deleted: by international, national

Deleted: ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments

Deleted: as well

In specific circumstances the police may seek to collect data by coordinating its information with other data controllers and processors. Furthermore, it may combine personal data stored in different files or in different databases that are held for different purposes, such as those held by other public bodies and/or private organisations. This may be in relation to an on-going criminal investigation or to identify thematic trends in relation to a certain type of crime.

In order for these actions to be legitimate they must be authorised or be underpinned by a legal obligation to comply with the purpose limitation principle.

If the relevant police body has direct access to files of other police or non-police bodies, it must only access and use the data if domestic law, which should reflect the key data protection principles, so permits.

Clear legislation and guidance, which adheres to the data protection principles, should exist for cross-referencing of databases. Such cross referencing should be necessary, purpose bound and proportionate. With relation to personal data stored in other data controllers' or processors' data base all conditions described in Point 2 have to be fulfilled and regularly checked.

Example - Data held for citizenship purposes can only be used in an investigation if the national legislation allows it and to the extent to which it is necessary for the purpose of the investigation to do so. For instance, the number of children a suspect has may not be relevant in an investigation, and should therefore not be processed by police. Access in this case to a database can be perfectly lawful but it can only be legitimate if it respects the principles of data protection.

18. Data security

The police must take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The controller must notify, without delay, at least, the competent supervisory authority of those data breaches which according to its assessment may seriously interfere with the rights and fundamental freedoms of data subjects. The information of data subjects of data breaches which may seriously interfere with their rights may also have to be ensured without undue delay, unless it jeopardisese the task of the police.

Information security is essential to data protection. It is a set of procedures to ensure the integrity, availability and confidentiality of all forms of information within the police organisation, with the aim of providing security of data and information, and limiting the impact of security incidents and data breaches to a predetermined level.

The level of protection given to a database and/or an information system or network is determined by a risk assessment. The more sensitive the data are, the greater protection is required.

Authorisation and authentication mechanisms are essential to protect the data, and sensitive information should always be encrypted. It is considered best practice to have in place an audit regime to regularly check that the level of security is appropriate.

Police authorities are advised, where necessary, to conduct DPIA (see Point 4) to assess the privacy risks to individuals in respect of the collection, use and any disclosure of information. This will help to identify risks and develop solutions to ensure that concerns are addressed appropriately. Any such impact assessment should cover relevant systems and processes of processing operations, but not individual cases.

A Data Protection Officer (DPO) within the police can play an essential role in carrying out internal audits and assessing the legitimacy of the processing, which contributes to a higher level of data protection and data security within the organisation. Moreover, the DPO can facilitate the dialogue between the organisation and the data subjects, as well as the organisation and the supervisory authority which can add to the overall transparency of the police body.

Deleted: crime

Deleted: have

Deleted: r they

Deleted: in

Deleted: accordance with

Deleted: permits legislation

Deleted: ,

Deleted: of

Deleted: therefore

Deleted: any

Deleted: affect

Deleted: them

Deleted: shall also

Deleted: ing

Deleted: ¶

Deleted: ,

Deleted: …

An Identity & Access Management System (IAM) may be recommended to manage employees and third party access to information. This will require authentication and authorisation to access the system and set privilege rights to determine what can be viewed. IAM can be seen as a useful requirement to ensure safe and appropriate access to data.

The data controller, following an evaluation of the risks, should at implement measures in respect of:

- equipment access control,
- data media control,
- storage control,
- user control,
- data access control,
- communication control,
- input control,
- transport control,
- recovery and system integrity,
- reliability and integrity.

Privacy-by-Design

The concept of privacy-by-design is an integral part of data security. Data protection and security may be embedded directly into information systems and processes, using technical and organisational measures, to ensure a high level of data protection and security and, in particular, to minimise the likelihood of data breaches. This approach is known as Privacy–by–Design, promoting privacy and data protection compliance from the start. It can be achieved through software and/or hardware. It requires a threat analysis, a full life cycle approach and rigorous testing.

Data controllers should ensure that privacy and data protection is a key consideration in the early stages of any project and then through its life cycle. Specifically, when building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have privacy implications and embarking on an information sharing initiative using data for new purposes.

Privacy-by-Design requires the implementation of Privacy Enhancing Technologies (PETs) to enable a better protection of personal data. PETs prevent unnecessary processing of personal data, without losing functionality in the information system itself.

Example: Body scanners used for police purposes have to be designed to respect the privacy of the individuals being inspected while fulfilling the purpose of their use. Therefore the body image in such tools has to be blurred by default.

19. External control

There has to be, at least, one supervisory authority responsible for ensuring and overseeing the correct application of the international and national legislation applicable to the data processing within the law enforcement sector.

Certain states may require more than one supervisory authority, for instance a national or federal authority and a number of decentralised or regional authorities, whilst others will prefer to have a single supervisory authority, responsible for the entirety of the supervision of data processing operations.

The supervisory body should be completely independent, meaning that it does not belong to the law enforcement organisation, nor is it directed by another body whithin the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties and should not be instructed or forced to accept instructions from anybody. The personal independence of its chair/president including

Deleted: P

Deleted:

Deleted: *Privacy-Enhancing Technologies (PETs)* ¶

Deleted: This is the common name for a range of different technologies to protect sensitive personal data within information systems.

Deleted: users to

Deleted: their

Deleted: The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.¶

Deleted: compliance of

Deleted: to the international and national legislation

Comment [A53]: DE: Suggestion to make it clearer that it is not the DPA´s job to ensure compliance (this is for the controller) but to ensure oversight and application).

Deleted: organisation

political, financial, functional and operational independence, are decisive factors when judging how independent the supervisory body is.

Deleted:

National law should provide for advisory, investigative and enforcement powers to enable it to investigate complaints, to have regulatory measures or to be able to impose sanctions where needed. The legal and administrative tools at its disposal shall be efficient and enforceable.

Supervisory authorities should have the ability to cooperate in law enforcement matters bilaterally and also via the Committee of Convention 108.

Example: The supervisory authority must be independent and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

a. “personal data” means any information relating to an identified or identifiable individual (“data subject”);

b. “genetic data” are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

c. “biometric data” are data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual;

d. “soft data” (evidence based on testimony or other personal assessment) means data acquired through testimony of person involved in the investigation;

e. “hard data “ (evidence based on documents or proven facts) means data acquired from official documents or other certified sources;

f. “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

h. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

Deleted: g. “competent authority” means: public or private entity authorised by law having a competence in the prevention, investigation and prosecution of criminal offences and to the execution of criminal penalties;¶

i. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

j. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

k. Internet of Things (IoT): is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

l. “covert surveillance” means all measures aiming at monitoring discreetly the movements of persons, vehicles and containers, particularly those involved in organised or cross-border crime.

m. “special investigative techniques” techniques applied by the competent authorities in the context of criminal investigation for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person.

n. “privacy-enhancing technologies” (PETs) means a range of different technologies to protect personal data within information systems. The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.

ITALY/ITALIE

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied to ensure the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").
Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed application and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[34] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level.
The present Guide was therefore prepared to highlight the most important issues that may arise in the use of personal data in the police sector and to point out the key elements to be considered in that context.
This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance.
The overarching principles set out in Recommendation (87)15 and their practical implications aim to ensure that the processing of personal data by the police is carried out in full respect of the rights of the individual to privacy and data protection.
To facilitate the reading of the Guide, a glossary of the terms used is provided at the end of the document.

General considerations

The collection and use of personal data for law enforcement purposes constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108 and, as such, it *must* be based on law (clear, foreseeable and accessible), pursue a legitimate aim and be limited to what is necessary and proportionate to achieve that legitimate aim. (Former second paragraph moved upfront)

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data processing within the police should be based on predefined, clear and legitimate purposes set in the law; it should be necessary and proportionate to these legitimate purposes and should not be processed in a way incompatible with those purposes. Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible.

1. Scope

The principles explained in the present guide apply to the processing of personal data for police purposes, namely for the purposes of the prevention, investigation and prosecution of criminal offences, the execution of criminal penalties [and for the maintenance of public order by the police] (hereafter referred to as "tasks of the police", ["police purposes"]). Where 'police' is used in the text, it can be taken to mean wider law enforcement authorities, and/or other public and/or private bodies authorised by law to process personal data for the same purposes.

[34] See Report "Twenty–five years down the line" – by Joseph A. Cannataci

2. Collection of data and use of data

The police as data controller is responsible for all data processing it undertakes and is accountable for its data processing operations.

The collection of personal data for police purposes should be limited to what is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

It is understood from Point 2.1 of the Recommendation that for the fulfilment of both of the main police tasks (prevention of a real danger and the suppression of a specific criminal offence), an evident and direct correlation should exist between the data processing carried out by the police and a situation where individuals have already committed or are likely to commit a crime.

Deleted: in

The police should always choose the adequate legal basis to process personal data and should process personal data in a legitimate way. A careful assessment should be carried out by police to make sure that the processing is based on an appropriate legislation and the procedures for data processing foreseen by it are fully respected.

The police should apply at all stages of the processing the relevant data protection principles (most importantly the principles of necessity, proportionality and purpose-bound data processing) and should not continue to process data which are not needed for the purposes. In this context, personal data collected at an early phase of the investigation, which then proves with the process of the investigation to be no longer relevant should no longer be processed (e.g. innocence of a suspect is confirmed), and should therefore either be blocked or deleted. This does not apply where subsequent use of the data is allowed (point 3).

Prior to and during the collection of such data, the question of whether the personal data collected is necessary for the investigation or for a task of the police as described in Point 1, should always be considered. One should note that once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific task of the police) should exist. This link together with compliance to the data protection principles as described in the Guide, must be demonstrable at all times. After the collection phase and at different stages of the investigation, a thorough analysis is needed to assess which data are to be retained and which are to be deleted.

Before collecting any personal data, investigators should ask themselves the question 'Why is it necessary to acquire the data?', 'What, exactly, do you seek to achieve?'.

Example – For personal data such as Telephone Billing: only the number(s) required for the time periods being investigated should be sought and only for those individuals suspected of having a link with the offence.

A list of phone numbers of the person(s) involved in the suspected offence can be collected if there are indications that such data serve the purpose of the investigation. It cannot be kept or processed after the analysis shows that the data are not strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for police purposes should be used for those purposes only and should not be used in any other way that is incompatible with the original purpose stated at the time of collection and is necessary for and proportionate to the pursuing of police purposes, unless this is provided for in law (see Article 9 of Convention 108) [In assessing the compatibility of the use of data for the same purpose, one should consider the following criteria: (i) relation between purposes; (ii) context of the collection and information given to data subjects; (iii) nature of personal data; (iv) consequences for data subjects of the intended subsequent use; (v) existence of appropriate safeguards.]

Subsequent use of data is considered for the purposes of this guide as a new data processing operation which has to fulfil all the criteria and conditions mentioned above. The subsequent use of data shall be lawful, undertaken for a legitimate aim and necessary and proportionate to this legitimate aim.

The police shall ensure at all stages of the data processing and for the subsequent use of data as stated in the General considerations that the personal data are accurate, up-to-date, adequate, relevant and not excessive in relation to the purposes for which they are processed.

Example: Police data collected for an investigation where the political affiliation is irrelevant, cannot then be used to determine the political affiliation of the concerned person.

3. Subsequent use of data

Every subsequent processing of data for police purposes other than that the data were originally collected for, must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be undertaken for a legitimate aim and should be necessary and proportionate to the legitimate aim pursued.

Comment [A54]: Is this sufficient? Shouldn't we refer to the specific legitimate aims identified by Article 8.2 of ECHR and Article 9 of Convention 108?

Personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set out in Point 2. The general rule is that if data are likely to be used in a different case or in a different operation of the police, the assessment of compliance described in Point 2 shall be applied to this new processing as well (This is not applicable if data are used for purely statistical or scientific purposes). Notwithstanding the computerised and/or automated data processing and the large volume of personal data stored very often in different processing environments, the, personal data collected and retained for police purposes should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

It should be noted, moreover, that any subsequent use of personal data related to vulnerable individuals such as victims, minors, or of those enjoying international protection, should be subject to additional care and legal analysis with a special attention to the application of the principles of necessity and proportionality.

In cases such as trafficking in human beings, drug trafficking or sexual exploitation, where victims' data may subsequently be used also when they are considered as suspects, or where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to look at existing international good practice (in international or regional police bodies) and to enhance their exchange of information on the matter with other national police bodies.If all legal requirements as put forward in Point 2 are met, it should not represent any obstacle to the use of data of these persons for police purpose, but during these exchanges, confidentiality rules have to be followed.

Example - Data collected for tax purposes from a data subject can only be processed for law enforcement use by police if the law allows it, if they are used for a legitimate aim and in a way that is necessary and proportionate to the aim pursued. In a concrete investigation of money laundering, the use of tax declarations' data of an individual can be envisaged to establish or deny a link between the individual and the money laundering operations.

Deleted: ()

Deleted: .

4. Processing of special categories of data (sensitive data)[35]

Special categories of data, such as genetic data, personal data related to offences, criminal proceedings and convictions and related security measures, biometric data uniquely identifying a person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical nature, for instance additional security measures, and of an organisational nature, for instance having such sensitive data processed separately from the processing environment of the "ordinary" categories of data. Safeguards should be adjusted to each data processing operations taking into account their specificities and it is highly recommended to use multiple

[35] Paragraph removed from previous Point 8

levels of protection for those categories of data (e.g.: separate main-frames, shorter data retention periods, etc.). It is of paramount importance to prevent unauthorised or unwanted access to those categories of data even with additional security measures.

A careful balance of interests taking into account the purpose of the investigation, the context and the nature of the data is necessary to determine whether or not, and to which extent, the police could process sensitive data. For instance, it would be advisable to differentiate when biometric data is processed by the police whether it is for identification purposes (where for instance 2 fingerprints could suffice) or it is for crime investigation purposes (where more fingerprints could be needed).

The use of Data Protection Impact Assessments (DPIA) which is in general is to be carried out where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons can be recommended also in order to help to ensure that appropriate safeguards are put in place. The data controller should assess and demonstrate whether the purpose of the processing can be achieved in a manner that impacts less on the right to privacy and data protection and if the processing of special categories of data does not represent a risk of discrimination for the data subject.

Moreover, it should be recalled that the collection and processing of sensitive data in the context of profiling is prohibited (Principle 3.11 of Recommendation 2010 (13)[36] except if these data are necessary for and proportionate to the lawful and specific purposes of processing and as long as domestic law provides appropriate safeguards. In this context, besides measures detailed above, the use of PETs and more frequent checks on the lawfulness of the processing can be recommended. This could, for example, translate into measures put in place to counter the assumption that individuals belong to a criminal organisation because of where they live, where a criminal organisation is active or where the individuals have the same ethnic origin.

Example - Targeting groups or individuals based solely on religious beliefs would not be allowed. In an investigation into a group of individuals engaging in possible terrorist activities that were attached to a particular religious group, it could nevertheless be of importance to process data specific to the followers of this specific religious group (related to worshipping place, religious preachers, customs, teachings, members and structure of the religious community, etc. that was pertinent to the investigation).

5. Providing information to data subjects

One of the most important obligations of a data controller is to provide information on data processing to data subjects. This obligation is two-fold: it requires the data controller to provide *general information* to the public on the data processing that it carries out, and to give *specific* information to data subjects if no restrictions or derogations apply to the data processing.

Information provided to the wider public should promote awareness, inform them of their rights and provide clear guidance on exercising their rights. The information provided should be effectively and broadly accessible. Moreover it should include details about the conditions under which exceptions apply to the data subject's rights and how they could submit an appeal to the DPA or to the judiciary.

Deleted: , ,

Deleted: .

Websites and other easily accessible media perform a role in informing the public. It is recommended to have in place letter templates on these websites or other media to help the data subjects exercise their rights. It is the responsibility of the data controller to provide information which adequately highlights data protection and data subjects' rights.

[36] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing
of personal data in the context of profiling
(https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00)

In order to comply with the second obligation of giving data subjects specific information regarding data processed, the police shall inform data subjects on the data processing envisaged before the processing or, if it is not possible, for objective reasons, shortly after it. This communication shall comprise information on the data processing, on the collection of the individuals' data and comprehensive information on their rights.

The obligation to provide specific information implies that, in principle, the data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.

The information should be provided unless a restriction or derogation applies as described in Point 7 taking into account the specific nature of sensitive files, such as criminal intelligence files, files containing sensitive data. in order to avoid serious prejudice to the performance of police functions or to the rights of individuals. Even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.

Very often data subjects, because of restrictions or derogations of their right to information, cannot receive complete information on the processing the police undertake with their data; this should not affect their exercise of the right of access.

Example - For the purpose of covert monitoring of a high risk sex offender, data processing and long-term data retention may be justified without informing the individuals under surveillance if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved, the data subject should be informed about the fact that she or he was subject to such measure.

6. Data subject's rights[37]

Accessing their personal data is a fundamental right for data subjects as it allows them to be aware of the processing on data related to them, Moreover, it can also be a prerequisite to enable the exercise of further rights, such as the right to information, the right of rectification and the right of erasure

Deleted: the

In case an individual has her/his data collected during the course of an investigation or other tasks of the police as described in Point 1, as soon as circumstances safely permit, the police [in principle] should inform the individual of the data processing if there is such request. Specific information should be given in clear and plain language upon request . The communication has to contain the same information as described in point 5, unless data subjects wish otherwise.

The law can provide, under the strict conditions described in Point 7, that the right to access may also be limited or excluded, should the provision of such information prejudice the investigation, or another important police task, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified.

Deleted:

Deleted: be informed

Deleted: upon request

The police should aim to answer even general questions arising from data subjects on the processing activities in relation to their personal data, but can use standardised forms to facilitate communication.

Example: If a data subject asks the police on data it processes on them, the police, if no exception is applicable, should provide a detailed answer with legal references, but should do so in a plain language, avoiding uncommon or specialised expressions.

Comment [A55]: Not sure this is an example

The right of access should, in principle, be free of charge.

[37] Paragraph removed from previous Point 17.

It is possible to charge a reasonable administrative fee for the request, if national law permits and the request is manifestly unfounded or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such refusal.

To ensure a fair exercise of the right of access, the communication "in an intelligible form" applies to the content as well as to the form of a standardised digital communication. It is, however, advisable to refer to national legislation to ensure consistency and to avoid suspects utilising this method to find out whether there is an on-going investigation into them.

In respect of direct access, the data subject can request access to the controller of the files. The data controller will assess the request and any possible restriction or derogation which can only be used if it is vital for the performance of a specific police task as described in Point 1, or it is necessary for the protection of the data subject or the rights and freedoms of others, and reply directly to the data subject. In case of a restriction, partial information, and in case of derogation, information on the use of derogation, shall be still given, with the motivation for using such measures in both cases, as well as information concerning redress.

Example: The access request can be refused if there is an on-going investigation on the person, and providing the data subject access to the data could compromise such investigation.

If restriction or derogation were to be used, any answer should take into consideration, according to national law or practice, all circumstances to which the restriction or the derogation is applicable.

As a rule, domestic law should, ideally, provide for direct access. If the right of access provided for is indirect, the data subjects may direct their request to the supervisory authority, which after being properly mandated, will carry out the request on their behalf and conduct checks regarding the availability and lawfulness of the processing of the data subject's personal data. The supervisory authority will then reply to the data subject (providing what data it is possible to release, subject to any legally allowed restrictions or derogation). In case of a restriction or derogation, the same communication should be made possible as in case of a direct access.

The data controller should assess the request and reply to the data subject within a reasonable time limit, as provided for by domestic law.

There should be arrangements in place to confirm the identity of the data subject before access to any data is granted as well as to obtain information on the processing activities to which the request refers. The same holds if the data subjects delegate the authority to someone else to exercise their rights.

It is an essential right of the data subjects to be able to amend any incorrect data held on them. If the data subject finds data that are incorrect or irrelevant, she/he should have the right to challenge it and ensure that they are amended or deleted.

In some cases, it may be appropriate to add additional or corrective information to the file. It is important to underline that this right can only be exercised with due respect to other individuals' rights, for instance to the rights related to a testimony in a criminal case (which does not preclude per se the exercise of the data subjects' rights related to soft police data).

Data subjects can ask for the deletion of their personal data where such processing is unlawful.

If the data to be corrected or erased has been communicated elsewhere the relevant authorities should be informed of the changes to be made.

All proposed changes should be supported by evidence. If data subjects can prove by use of the official documentation that the data processed by police in respect to them are incorrect, the data controller shall not have the right of discretion whether to correct them.

It may be necessary for the police, as dealt with under Point 7, not to give information or grant the right of access, of deletion and of correction which might jeopardise an investigation and should therefore be

excluded for its duration. Similar restrictions or derogation may be imposed by national law as described in Point 7.

Restrictions or derogations to the rights of data should only apply to the extent necessary and be interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis. Any decision to refuse a data subject's request should be provided in writing (including by electronic means). The response should provide clear justification of the decision making which can be verified by an independent authority or a court. It is possible that communicating the reasons for refusal could pose a risk to law enforcement or the data subject or to the rights and freedoms of others. If this is the case, it should be documented and provided to the independent authority or court to be verified, if required.

Example - If person A submitted a declaration against person B accusing her/him of committing a serious offence and later it emerges that the accusation was false, it might be relevant for the police to retain the false statement and the information surrounding it.

Although the statement was proven to be false, if the police needs to retain the data in the interest of the investigation for instance, a clear corrective statement on the file, instead of removing the false statement, would be necessary.

Deleted:

Comment [A56]: This examples seems to have more to do with accuracy of data than data subject's rights

The data subject should be informed of all available options following a refusal decision such as an appeal either to the supervisory authority, to court or to another independent administrative authority.
Depending upon national legislation, specifically whether there is a direct or an indirect right of access, the actual communication of the result of the review or appeal may differ. In the case of indirect access the data subject should at least be informed that a verification of the police file has taken place. Alternatively, the supervisory body may request the police to release the data contained in the file to the data subject. The court or tribunal may have powers to enforce the access, correction or deletion of data from the file even in access-request cases referred to them by police or the supervisory authority.

If police sends a refusal letter it should contain the name, address, web address, etc. of all possible fora for redress.

Deleted: fora

The data subject should have access to a court or tribunal in order to submit an appeal, and have the reasons for refusal verified if they are not satisfied with the reply given by the supervisory authority or the independent authority. The supervisory authority should have sufficient powers to examine the police file concerned and have the assessment communicated.

7. Exceptions from the application of data protection principles

Exceptions can only be used for specific purposes foreseen by article 8 of European Convention on Human Rights and article 9 of Convention 108, if foreseen by law (the law should be public, open and transparent and, in addition, detailed enough) and if they constitute a necessary and proportionate measure in a democratic society for the purposes of….

Comment [A57]: See next comment

The exceptions which have to be incorporated into national legislation should not be described in a general way, but should serve a well-defined purpose. Exceptions can be applicable to those principles described under Points 2,3,,5,as well as to the data subjects' rights (Point 6) in case of some specific purposes in relation to which data processing activities are undertaken. In particular they concern activities undertaken for the purpose of the protection of national security, defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest (which includes purposes in connection with the fulfilment of a state's international legal commitments or obligations, most prominently deriving from the binding decisions of United Nations' bodies, and humanitarian purposes.) or the protection of the rights and fundamental freedoms of others.

Deleted:

Comment [A58]: We may move this part at the end of the 1st paragraph

Example - If giving information to a data subject may endanger the safety of a witness or an informant; this right can be limited in light of such circumstances.

If the exception, as defined by national law providing specific safeguards is used by the police, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. The aim of using exceptions by the police should be limited to cases where the use of those rules and principles would endanger tasks of the police described under Point 1.

Deleted: .

Example: If data collected for police purpose in an investigation are likely to serve national security purposes they can also be used to this latter purposes to the extent set forth by national legislation. If specific intelligence proves that money laundering operations have been carried out to finance terrorist operations, data collected on individuals during the investigations on money laundering can be used for the purpose of eliminating the close and imminent terrorist risk.

8. Use of special investigative techniques

The police should always adopt the least intrusive means of data processing during its operations. If less intrusive methods can be used to achieve the desired ends, they should be preferred. The use of special investigative techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods.
With increasingly sophisticated technological developments, electronic surveillance has become easier, however, the use of these techniques interferes with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the need to ensure efficiency of investigations has to be balanced with the high potential of severe interference with the right to privacy and fundamental rights.

Deleted:

Deleted: has to be balanced with the efficiency of investigations

Example: In an investigation, the evidence for communication between two suspects can be gathered in various ways. If, by the use of interrogations, testimonies, the obtaining of call data, the same result can be achieved without jeopardising the effectiveness of the investigation, it is to be preferred to the use of more intrusive surveillance measures, such as wiretapping which, moreover, must be carried out in due respect of the specific requirements and conditions set forth by law.

9. Introduction of new data processing technologies

If the introduction of new technologies is likely to result in a high risk to the individual's rights, the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. The introduction of new data processing technologies is considered to be subject to a DPIA as probability of risks to the individual's rights is usually high. It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity. The relevance of the DPIA shall be checked at reasonable intervals.

It is also of great importance, that in terms of data security and safety of communications, the highest standard is taken into account when introducing such technologies.

Example - New data mining techniques may offer extended possibilities for identification of possible suspects and should be assessed carefully for their compliance with existing data protection law, together with assessment of the risks it may represent to individual's rights and suggestions for the adoption of safeguards to ensure the protection of data, including with regard to data security.

The data protection authority has an important role in advising which risks are involved for data protection and which safeguards should be provided to ensure that any technical means comply with data protection law. However, the police do not have an obligation to turn in every case to the supervisory authority where it introduces new technologies. It may do so if the DPIA it previously conducted demonstrates a significantly persisting high risk to the individual's rights notwithstanding the adoption of specific safeguards.

The consultation between the supervisory authority and the data controller should provide the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.

Appropriate details should be provided to the supervisory authority, in particular regarding the type of file, the data controller, data processor, the legal basis and the purpose of the data processing, the type of data being processed and by whom the data is being accessed, as well as information on retention of data, log policy and access policy, and other relevant technical aspects of implementation.

Example: Detailed information on national reference files containing fingerprint data such as purpose, data controller etc. could be reported to or made available for consultation to the data protection authority.

Following consultation, the data controller must consider carefully to implement any necessary measures and safeguards that have been recommended by the data protection authority.

Example - Introducing an automatic facial recognition system or other system based on the automated processing of biometric data would be very likely to need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed and recommended by the data protection authority after being consulted on the issue, specific safeguards should be put in place (concerning the data retention time, the cross matching functionalities, the place of the storage of data and the access to data issues, etc.) to comply with data protection principles and provisions.

Deleted: .

Deleted: containing fingerprint data

Deleted: should

Deleted:

Use of the Internet of Things (IoT) technology in police work

Data sent to and from police during operational activity via the internet are good examples of the IoT already in use. Due to potential security vulnerabilities, IoT requires measures such as data authentication, access control to ensure data security and resilience to (cyber) attacks.

Example: In light of their potential security vulnerabilities, smart glass used by police should not be directly connected to a national criminal record data base and data collected should be guaranteed a high level of security.

Big data analytics in the police

Technological advances in processing and analysing large and complex data sets leading to big data and big data analytics present opportunities and challenges to the police, who is turning to digital sources and profiling techniques to perform their tasks.

Big data technologies enable bulk collection and analysis of a vast quantity of data generated by electronic communications and devices aggregated with other bulk data. This could interfere with the right to privacy and data protection.

The Council of Europe's Recommendation CM/Rec(2010)13[38] on the protection of individuals with regard to automatic processing of personal data in the context of profiling and the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[39] can be of use in the context of Big Data analysis for police use too.

Big data technologies and analysis techniques may help assist detecting crime, but there are, however, considerable risks to this type of data processing that should be taken into account:

[38] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[39] Document T-PD(2017)1 - Big Data Guidelines

- Databases originating from one domain can be used in another domain and for another purpose, which changes the context and may lead to inaccurate conclusions and lack of valid legal basis, therefore to unlawful data processing with possibly serious consequences for the individuals involved.
- Profiling may lead to drawing discriminatory conclusions, which can result in the reinforcement of stereotypes, stigmatisation and discrimination.
- The increasing amount of personal data held in databases may lead to severe vulnerabilities and subsequent risk of data breaches if information security is not guaranteed.

Where big data relies on personal data, data controllers should pay additional attention to the following requirements:

- Verification of data accuracy, context and relevance of the data.
- Its use requires a high level of accountability.
- Its use shall be combined with methods of investigation which complement the conclusions drawn from the big data analysis. A decision affecting a person shall not be taken solely on automated processing of personal data.
- As for other types of data processing, it is of paramount importance that its use shall be ~~shall be be~~ necessary and proportionate for the fulfilment of police tasks described in Point 1, with special attention for the data processed to be adequate, relevant and non-excessive in relation to the purpose for which they are processed.
- Predictive analysis requires human intervention to assess the relevance of the analysis and conclusions.
- Ethical guidelines developed at national or at international level should be taken into consideration.
- As a principle and subject to restrictions and derogations mentioned in Point 7, transparency should be ensured by the data controller by explaining how the data are processed in accordance with privacy and data protection principles. If data collected for one purpose is used for another purpose, the data controller should in principle make the data subjects aware of this subsequent use.
- Even if complex methods are used, the lawfulness of the processing – including subsequent use of data - and compliance with the conditions set by Article 8 ECHR and Convention 108 should be demonstrated.
- An information security policy should be in place and implemented throughout the processing.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals and the administrative and judicial means exist for individuals to challenge those decisions. This implies data subjects' awareness of the reasoning of the algorythm used and the purposes for which it was used.

The above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones, are even more necessary when sensitive data are processed in Big Data analytics.

10. Storage of data

"As pointed out in Point 2" data shall be processed until they have served the purpose for which they were collected. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

There should be a clear distinction in how the police stores and processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses. This should also relate to the specific purpose for which the data was collected. Additional safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence. Clear rules have to be established in relation to the handling of different data bases with special attention to the analysis of multiple results.

The principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve police purposes as defined in Section 1.

Deleted: the

Deleted: of the prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where personal data is processed for the purpose of the maintenance of public orde

Deleted: r

The grounds for retention and processing should be reviewed periodically. The unlawful processing of personal data outside of the legal framework allowed for the retention constitutes a severe violation of the right to protection of personal data. If the law in relation with a specific crime provides for a data retention period of 4 years and if
personal data are processed in relation with this crime by the police solely on this ground after 4 years have passed since the collection of the data in question and no other legal ground to process this data exists, the retention of this data could be considered as unlawful.

Comment [A59]: Would?

General data retention periods are usually regulated in national or international law. In order to comply with the legislation while ensuring the effectiveness and the success of an investigation police bodies are strongly advised to develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data.

For example, in a case where the law prescribes a 4 year data retention period but the individual subject to an investigation is acquitted from all charges by the court after 2 years, her/his data shall be deleted (if the individual is not a recidivist or there is no information on her/him committing again the same category of crime) from the database, provided that all deadlines for the review of the case have expired. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

Comment [A60]: Are we sure that data should be deleted in the presence of a law providing for a longer retention (provided that of course the law has the necessary requirements of necessity and proportionality?)

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judicial procedure terminates completely (which means all redress have been made or all deadline for redress have been passed).

The police should provide systems and mechanisms to ensure that the data that are stored are accurate and that their integrity is maintained.

International obligations, which include providing data to international bodies such as Europol, Eurojust and INTERPOL, bilateral agreements and mutual legal assistance between member states and third countries must be observed when shaping internal policies.

Data should be categorised according to the degree of accuracy and reliability in order to assist the police in their activities. It is recommended that handling codes are used to distinguish these categories. A classification system facilitates the assessment of the quality of the data and how reliable it is. Classification of data is also important when it is to be communicated to other police bodies or states.

Example - Information collected directly from a person's statement will be assessed differently than information collected from a person's hearsay statement. Data based on facts, or 'hard' data, will be assessed differently than data based on opinions or personal assessments, or 'soft' data.

Personal data collected by police for administrative purposes must be kept (as far as possible: logically and physically) separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by law.

Examples of administrative data include lists of data on licence holders or data on human resources and firearms certificates.

11. Communication of data within the police sector

A distinction should be made between domestic communication of data and international transfer of data. Within these two distinct operations different requirements apply, depending upon who is receiving the data, whether it is the police, another public body or a private party. The police can only communicate personal data within the police sector if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

Comment [A61]: Relationship with the next underlined sentence?

There should be clear and transparent rules on how the police grant access to data held by it and on which grounds.

The police, domestically, should only share information (among police) when there is a legal basis for the request, e.g. an on-going criminal investigation or a shared law enforcement task and laws or agreements allowing the communication

Comment [A62]: See previous comment

The police can share data with other police organisations if the personal data are relevant for the purpose of prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where they are processed for the purpose of the maintenance of public order.

The communication of personal data in general should be in line with the general considerations described above.

Example: A police unit can share data on a suspect who presumably committed a tax fraud with another police unit investigating a murder case if there is indication that the suspect for this crime could be the same person or if doing so will materially assist the investigation.

12. Communication of data by the police to other public bodies

The communication of data outside police is permissible if it is provided for by law and the data are required by the recipient to enable them to fulfil their lawful task. Mutual assistance agreements foreseen by the law between law enforcement and public bodies allows the public bodies to have access to law enforcement data which would be essential in the fulfilment of their duties and tasks (for example in their investigations or other legal duties in accordance with national law).

Stricter principles than those set forth in Point 11 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the processing of personal data, which are considered sensitive, could result in adverse effects for the individual.

Communication of data to any other public authority may also be allowed if it is foreseen by law, is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to other persons or to public order or to public security.

The communicated data may only be used by the receiving body for the purposes for which the data were transferred.

Example - A claim for a residence permit made by a migrant. Police data may be required to verify if the person was ever involved in criminal activity. It would be in the interest of the Immigration Office and the claimant for this communication of data to take place.

13. Communication of data by the police to private parties

There may be occasions when, under strict conditions, the police can communicate data to private bodies. This communication has to be based in law and can only be done by the authority which is processing the data. Such communication can only be done for the purpose of the investigation or other important police tasks as described in Point 1, in the interest of the data subject, for humanitarian reasons or if it is necessary to prevent serious and imminent risk to public order or public security. For example, there might also be instances where police data may be communicated to humanitarian organisations based on international law, in the interest of the data subject or for humanitarian reasons.

Where the police shares data with media in respect of making information related to an investigation public, special consideration should be given to the assessment to determine that it is necessary and in the public

interest that such publicity is allowed and to appropriate safeguards to ensure respect for the rights of the individuals involved in the case.
Such communication should only be on a case by case basis and in each case there must be a clear legal basis providing the necessary procedure (e.g. need for specific authorisation) to be followed for any such communication to occur.

Deleted: . ¶

Example - When the police communicate with the financial sector in relation to known fraud or theft offenders, when it communicates with an airline about stolen or lost travel documents or when the police releases details of wanted persons believed to pose a risk to the general public.

14. International transfer

Any transfer of police data internationally should be limited to police bodies and should be fit for purpose and in accordance with the law. For this, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data handling, regional legal frameworks such as EU and EU institutions' legislation (on Europol, Eurojust, Frontex, etc.) and subsequent agreements (operational bilateral agreements), bilateral treaties and in general, international agreements on mutual assistance, or other bilateral or multilateral agreements made regarding effective cooperation can be of use.

When considering sharing any data, consideration should be given as to whether the receiving authority is performing a function conferred to it in law related to police purposes as defined in Section 1, and whether the sharing of the data is necessary to perform its specific task.

Deleted: the prevention, investigation, or prosecution of criminal offences, the execution of criminal penalties and the maintenance of public order

The sending authority should ascertain that there is an appropriate level of data protection in the receiving state and that the receiving state complies with the relevant rules of international transfers of personal data. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. This means of transfer should be used as a last resort option. International transfers framework such as "INTERPOL's Rule on the Processing of Data" and its "Statute of the Commission for the Control of INTERPOL's files" Rules on the Control of Information and access to INTERPOL's Files", the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185) may be taken into account[40] so as to ensure that any transfer of data is legally justified and has appropriate safeguards in place. The request should clearly state all the necessary elements from the requesting party to enable the receiving party to make a sound decision on the request. These details would be expected to include the reason for the request as well as the purpose for the transfer of data.

An appropriate level of data protection should be guaranteed (e.g. through ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments) if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

If there are conditions applied by the sending authority in relation to the use of the data in the receiving state these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout its lifecycle.

Example - Further transfer of data should only be allowed if this is necessary for the same police purpose as the original transfer and the second recipient is also a police body ensuring an appropriate level of data protection. The police body which originally sent the data must also consent to the onward transfer. If the police from country X sends personal data to the police of country Y it is only permissible for the country Y to transfer this data if above all requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) if country X consents to the transfer. If the data is sent to country Z which is a non-

[40] This is without prejudice to the right of the Committee of Convention 108 and other instances disposing such power to assess and to review if necessary the level of data protection guaranteed by those multilateral agreements

member of the Convention 108, then country Y should ascertain that this country provides an appropriate level of protection of personal data and effective means of exercise of the related data subject rights.

The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases if it is required for the performance of the task of the transferring authority and there is no effective means of transferring the data to a police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers.

Example: If tax authorities in country X requests the police in country Y about the whereabouts of a person involved in non-criminal tax evasion because they have evidence that the person is involved in criminal matters in country X, the police can transfer the personal data of the individual.

Comment [A63]: Is this enough?

The international transfer of personal data between police and private bodies in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police as described in Point 1, provided by legal means and where the emergency, the gravity of the crime, its trans-border nature and where the involvement of the police would not be possible for objective reasons . Other facts as data security, the reassurance received as to the use of the data and the lawfulness of the data transfer in the receiving country have to be taken into account. In this context it is to be noted that in such a case, the data controller has a double obligation with respect to the protection of personal data: one imposed by the legal framework of the country where it resides and the one which is related to the data transfer. The local police should be informed afterwards. The police are required, wherever possible, to make use of existing international legal instruments, in respect of this type of data transfer. International transfers may also exceptionally occur where the police communicates personal data for humanitarian purposes.

Example: In an investigation, carried out within the framework of an international multilateral agreement, into child sexual exploitation where the victim is in country Y and the police there have commenced an investigation, and the material has been made available on the internet by the suspect residing in another (country X) and there is a high risk that the suspect seeks to avoid justice by fleeing country X, the police in country Y can request, on an exceptional basis, that a service provider in country X provide the whereabouts of its customer. However, the police of country Y should inform the police in country X of its operation as soon as is possible and then seek to resolve the matter in cooperation.

15. Conditions for communications

Since there is a general obligation for the data controller to ensure a high level of data quality, it is advisable to have in place an additional check before sharing the data with others. When communicating or transferring data, it is always advisable to double-check the quality of data, if it is correct, up-to-date and complete. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated. It is required to establish secure channels of communication which ensure data security at the highest level possible. The quality of data can be assessed up to the moment of communication.

Example: If personal data that contain incorrect data (personal or otherwise) are sent they could adversely affect the investigation, cause harm to the individual concerned or others involved, or who may become involved as a result of the incorrect data being transferred. This can, as a result, leave the police in the transmitting and receiving states open to civil redress. In essence, if an individual is arrested based on a wrong communication of the suspect's name, it seriously harms several human rights of the individual concerned and can undermine any criminal investigation.

16. Safeguards for communication

It is of utmost importance that the necessity and purpose limitation principle should be applicable for any domestic communication or international transfer of personal data outside of police organisations.

Any data communicated should not be used for anything other than the purpose for which it was sent or received. The exceptions to this are when the sending authority, based on legal provisions, gives agreement to further use, and if it is necessary and vital for the recipient to fulfil their task. Data can also be communicated if it is in the interest of the data subject, for humanitarian reasons, is necessary to prevent serious and imminent risk to public order or public security or an appropriate level of data protection is guaranteed by the recipient by international, national legal instrument, ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments, as foreseen by Convention 108.

Deleted: any

Example: Personal data sent by the police of country X to the police of country Y in a money laundering case cannot be used by the police as profiling on the given individual in respect of her/his religious beliefs or political activities (unless those are relevant to the crime committed and police in country X has given its consent for this use).

17. Interconnection of files and on-line access to files

In specific circumstances the police may seek to collect data by coordinating its information with other data controllers and processors. Furthermore, it may combine personal data stored in different files or in different databases that are held for different purposes, such as those held by other public bodies and/or private organisations. This may be in relation to an on-going criminal investigation or to identify thematic trends in relation to a certain type of crime.

In order for these actions to be legitimate they must be authorised or be underpinned by a legal obligation to comply with the purpose limitation principle.

If the relevant police body has direct access to files of other police or non-police bodies, it must only access and use the data if domestic law, which should reflect the key data protection principles so permits.

Deleted: ir

Clear legislation and guidance, which adheres to the data protection principles, should exist for cross-referencing of databases. Such cross referencing should be necessary, purpose bound and proportionate. With relation to personal data stored in other data controllers' or processors' data base all conditions described in Point 2 have to be fulfilled and regularly checked.

Example - Data held for citizenship purposes can only be used in an investigation if the national legislation allows it and to the extent to which it is necessary for the purpose of the investigation to do so. For instance, the number of children a suspect has may not be relevant in an investigation, and should therefore not be processed by police. Access in this case to a database can be perfectly lawful but it can only be legitimate if it respects the principles of data protection.

18. Data security

The police must take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The controller must notify, without delay, at least, the competent supervisory authority of those data breaches which according to its assessment may seriously interfere with the rights and fundamental freedoms of data subjects. The information of data subjects of data breaches which may seriously interfere with their rights may also have to be ensured without undue delay, unless it jeopardise the task of the police.

Comment [A64]: I am afraid we can't we use "must" as data breach notification is only provided by the modernised convention not finalised yet..

Deleted: se

Information security is essential to data protection. It is a set of procedures to ensure the integrity, availability and confidentiality of all forms of information within the police organisation, with the aim of providing security of data and information, and limiting the impact of security incidents and data breaches to a predetermined level.

The level of protection given to a database and/or an information system or network is determined by a risk assessment. The more sensitive the data are, the greater protection is required.

Authorisation and authentication mechanisms are essential to protect the data, and sensitive information should always be encrypted. It is considered best practice to have in place an audit regime to regularly check that the level of security is appropriate.

Police authorities are advised, where necessary, to conduct DPIA (see Point4) to assess the privacy risks to individuals in respect of the collection, use and any disclosure of information. This will help to identify risks and develop solutions to ensure that concerns are addressed appropriately. Any such impact assessment should cover relevant systems and processes of processing operations, but not individual cases.

A Data Protection Officer (DPO) within the police can play an essential role in carrying out internal audits and assessing the legitimacy of the processing, which contributes to a higher level of data protection and data security within the organisation. Moreover, the DPO can facilitate the dialogue between the organisation and the data subjects, as well as the organisation and the supervisory authority which can add to the overall transparency of the police body.

An Identity & Access Management System (IAM) may be recommended to manage employees and third party access to information. This will require authentication and authorisation to access the system and set privilege rights to determine what can be viewed. IAM can be seen as a useful requirement to ensure safe and appropriate access to data.

The data controller, following an evaluation of the risks, should at implement appropriate measures in respect of different elements such as:

Comment [A65]: Can we avoid the exhaustive list of measures?

- equipment access control,
- data media control,
- storage control,
- user control,
- data access control,
- communication control,
- input control,
- transport control,
- recovery and system integrity,
- reliability and integrity.

Privacy-by-Design

The concept of privacy-by-design is an integral part of data security. Data protection and security may be embedded directly into information systems and processes, using technical and organisational measures, to ensure a high level of data protection and security and, in particular, to minimise the likelihood of data breaches. This approach is known as Privacy–by–Design, promoting privacy and data protection compliance from the start. It can be achieved through software and/or hardware. It requires a threat analysis, a full life cycle approach and rigorous testing.

Data controllers should ensure that privacy and data protection is a key consideration in the early stages of any project and then through its life cycle. Specifically, when building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have privacy implications and embarking on an information sharing initiative using data for new purposes.

Privacy-by-Design requires the implementation of Privacy Enhancing Technologies (PETs) to enable a better protection of personal data. PETs prevent unnecessary processing of personal data, without losing functionality in the information system itself.

Example: Body scanners used for police purposes have to be designed to respect the privacy of the individuals being inspected while fulfilling the purpose of their use. Therefore the body image in such tools has to be blurred by default.

19. External control

There has to be, at least, one supervisory authority responsible for ensuring compliance of data processing to the international and national legislation within the law enforcement sector.

Certain states may require more than one supervisory authority, for instance a national or federal authority and a number of decentralised or regional authorities, whilst others will prefer to have a single supervisory authority, responsible for the entirety of the supervision of data processing operations.

The supervisory body should be completely independent, meaning that it does not belong to the law enforcement organisation, nor is it directed by another body within the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties and should not be instructed or forced to accept instructions from anybody. The personal independence of its chair/president including political, financial, functional and operational independence, are decisive factors when judging how independent the supervisory body is.

Deleted: h

National law should provide for advisory, investigative and enforcement powers to enable it to investigate complaints, to have regulatory measures or to be able to impose sanctions where needed. The legal and administrative tools at its disposal shall be efficient and enforceable.

Supervisory authorities should have the ability to cooperate in law enforcement matters bilaterally and also via the Committee of Convention 108.

Example: The supervisory authority must be independent and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

a. “personal data” means any information relating to an identified or identifiable individual (“data subject”);

b. “genetic data” are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

c. “biometric data” are data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual;

d. “soft data” (evidence based on testimony or other personal assessment) means data acquired through testimony of person involved in the investigation;

e. “hard data “ (evidence based on documents or proven facts) means data acquired from official documents or other certified sources;

f. “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

g. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

h. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

i. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

j. Internet of Things (IoT): is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

k. “covert surveillance” means all measures aiming at monitoring discreetly the movements of persons, vehicles and containers, particularly those involved in organised or cross-border crime.

l. “special investigative techniques” techniques applied by the competent authorities in the context of criminal investigation for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person.

m. “privacy-enhancing technologies” (PETs) means a range of different technologies to protect personal data within information systems. The most important aspect for the use of PETs is to determine if identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.

MAURITIUS/ILE MAURICE

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied to ensure the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").
Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed application and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[41] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level.
The present Guide was therefore prepared to highlight the most important issues that may arise in the use of personal data in the police sector and to point out the key elements to be considered in that context.
This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance.
The overarching principles set out in Recommendation (87)15 and their practical implications aim to ensure that the processing of personal data by the police is carried out in full respect of the rights of the individual to privacy and data protection.
To facilitate the reading of the Guide, a glossary of the terms used is provided at the end of the document.

General considerations

The collection and use of personal data for law enforcement purposes constitutes an interference with the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by Convention 108... As such, it *must* be based on law (clear, foreseeable and accessible), pursue a legitimate aim and be limited to what is necessary and proportionate to achieve that legitimate aim. (Former second paragraph moved upfront)

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that personal data processing within the police should be based on predefined, clear and legitimate purposes set in the law; it should be necessary and proportionate to these legitimate purposes and should not be processed in a way incompatible with those purposes. Data processing should be carried out lawfully, fairly and in a transparent manner. Personal data within the police should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally they should be accurate and up-to-date to ensure the highest data quality possible.

1. Scope

The principles explained in the present guide apply to the processing of personal data for police purposes, for the purposes of the prevention, investigation and prosecution of criminal offences, the execution of criminal penalties [and for the maintenance of public order by the police] (hereafter referred to as "tasks of the police", ["police purposes"]). Where 'police' is used in the text, it can be taken to mean wider law enforcement authorities, and/or other public and/or private bodies authorised by law to process personal data for the same purposes.

2. Collection of data and use of data

Deleted: and, a

Deleted:

Deleted: ¶
¶

[41] See Report "Twenty–five years down the line" – by Joseph A. Cannataci

The police, as data controller, is responsible for all data processing it undertakes and is accountable for its data processing operations.

The collection of personal data for police purposes should be limited to what is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

It is understood from Point 2.1 of the Recommendation that in for the fulfilment of both of the main police tasks (prevention of a real danger and the suppression of a specific criminal offence), an evident and direct correlation should exist between the data processing carried out by the police and a situation where individuals have already committed or are likely to commit a crime.

The police should always choose the adequate legal basis to process personal data in a legitimate way. A careful assessment should be carried out by police to make sure that the processing is based on an appropriate legislation and the procedures for data processing foreseen by it are fully respected.

The police should apply at all stages of the processing the relevant data protection principles (most importantly the principles of necessity, proportionality and purpose-bound data processing) and should not continue to process data which are no longer needed for the purposes. In this context, personal data collected at an early phase of the investigation, which then proves to be no longer relevant after investigation should no longer be processed (e.g. innocence of a suspect is confirmed), and should therefore either be blocked or deleted. This does not apply where subsequent use of the data is allowed (point 3).

Prior to and during the collection of such data, the question of whether the personal data collected is necessary for the investigation or for a task of the police as described in Point 1 should always be considered. One should note that once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific task of the police) should exist. This link together with compliance to the data protection principles as described in the Guide must be demonstrable at all times. After the collection phase and at different stages of the investigation, a thorough analysis is needed to assess retention and deletion of the data.

Before collecting any personal data, investigators should ask themselves the question 'Why is it necessary to acquire the data?', 'What, exactly, do you seek to achieve?'.

Example – For personal data such as Telephone Billing: only the number(s) required for the time periods being investigated should be sought and for only those individuals suspected of having a link with the offence.

A list of phone numbers of the person(s) involved in the suspected offence can be collected if there are indications that such data serve the purpose of the investigation. It cannot be kept or processed in case the analysis shows that the data are not strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for police purposes should be used only for those purposes and should not be used in any other way that is incompatible with the original purpose stated at the time of collection and is necessary for and proportionate to the pursuing of police purposes unless this is provided for in law (see Article 9 of Convention 108). [In assessing the compatibility of the use of data for the same purpose, one should consider the following criteria: (i) relation between purposes; (ii) context of the collection and information given to data subjects; (iii) nature of personal data; (iv) consequences for data subjects of the intended subsequent use; (v) existence of appropriate safeguards.]

Subsequent use of data is considered for the purposes of this guide as a new data processing operation which has to fulfil all the criteria and conditions mentioned above. The subsequent use of data shall be lawful, undertaken for a legitimate aim and necessary and proportionate to this legitimate aim.

The police shall ensure at all stages of the data processing and for the subsequent use of data as stated in the General considerations that the personal data are accurate, up-to-date, adequate, relevant and not excessive in relation to the purposes for which they are processed.

Deleted: is

Deleted: ¶

Deleted: and should process personal data

Deleted: not

Deleted: with the process of the investigation

Deleted: ,

Deleted: 1,

Deleted: Guide,

Deleted: which

Deleted: are to be retained and which are to be deleted

Deleted: ¶

Deleted: only

Deleted: after

Deleted: only

Deleted: ,

Example: Police data collected for an investigation where the political affiliation is irrelevant, cannot be used subsequently to determine the political affiliation of the concerned person.

3. Subsequent use of data

Every subsequent processing of data for police purposes other than that the data were originally collected for, must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law and the processing should be undertaken for a legitimate aim and should be necessary and proportionate to the legitimate aim pursued.

Personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set out in Point 2. The general rule is that if data are likely to be used in a different case or in a different operation of the police, the assessment of compliance described in Point 2 shall be applied to this new processing as well. (This is not applicable if data are used for purely statistical or scientific purposes). Notwithstanding the computerised and/or automated data processing and the large volume of personal data stored very often in different processing environments, the personal data collected and retained for police purposes should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

Moreover, it should be noted that any subsequent use of personal data related to vulnerable individuals such as victims, minors or of those enjoying international protection, should be subject to additional care and legal analysis with a special attention to the application of the principles of necessity and proportionality.

In cases such as trafficking in human beings, drug trafficking or sexual exploitation, where victims' data may subsequently be used when they are considered as suspects, or where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to look at existing international good practice (in international or regional police bodies) and to enhance their exchange of information on the matter with other national police bodies. If all legal requirements as put forward in Point 2 are met, it should not represent any obstacle to the use of data of these persons for police purpose but during these exchanges, confidentiality rules have to be followed.

Example - Data collected for tax purposes from a data subject can only be processed for law enforcement use by police if the law allows it; if they are used for a legitimate aim and in a way that is necessary and proportionate to the aim pursued. In a concrete investigation of money laundering, the use of tax declarations' data of an individual can be envisaged to establish or deny a link between the individual and the money laundering operations.

4. Processing of special categories of data (sensitive data)[42]

Special categories of data such as genetic data, personal data related to offences, criminal proceedings and convictions and related security measures, biometric data uniquely identifying a person, personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if prescribed by law and appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical nature, for instance additional security measures, and of an organisational nature, for instance having such sensitive data processed separately from the processing environment of the "ordinary" categories of data. Safeguards should be adjusted to each data processing operation taking into account its specificity and it is highly recommended to use multiple levels of protection for those categories of data (e.g.: separate main-frames, shorter data retention periods, etc.). It is of paramount importance to prevent unauthorised or unwanted access to those categories of data even with additional security measures.

A careful balance of interests taking into account the purpose of the investigation, the context and the nature of the data is necessary to determine whether or not and to which extent the police could process sensitive

[42] Paragraph removed from previous Point 8

Deleted: then

Deleted: ,

Deleted: ,

Deleted: I

Deleted: ,

Deleted: moreover,

Deleted: ,

Deleted: ,

Deleted: also

Deleted: ,

Deleted: ,

Deleted: ()

Deleted: ,

Deleted: .

Formatted: Indent: Left: 1,27 cm, No bullets or numbering

Deleted: ,

Deleted: s

Deleted: their

Deleted: specificities

Deleted: ,

Deleted: extent, the

data. For instance, it would be advisable to differentiate when biometric data is processed by the police whether it is for identification purposes (where for instance 2 fingerprints could suffice) or it is for crime investigation purposes (where more fingerprints could be needed).

The use of Data Protection Impact Assessments (DPIA) which is generalised is to be carried out where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons. It can also be recommended in order to ensure that appropriate safeguards are put in place. The data controller should assess and demonstrate whether the purpose of the processing can be achieved in a manner that impacts less on the right to privacy and data protection and if the processing of special categories of data does not represent a risk of discrimination for the data subject.

Deleted: in
Deleted: is
Deleted: also
Deleted: help to
Deleted: processing can

Moreover, it should be recalled that the collection and processing of sensitive data in the context of profiling is prohibited (Principle 3.11 of Recommendation 2010 (13)[43] except if these data are necessary for and proportionate to the lawful and specific purposes of processing and as long as domestic law provides appropriate safeguards. In this context, besides measures detailed above, the use of PETs and more frequent checks on the lawfulness of the processing can be recommended. This could, for example, translate into measures put in place to counter the assumption that individuals belong to a criminal organisation because of where they live, where a criminal organisation is active or where the individuals have the same ethnic origin.

Deleted: , the

Example - Targeting groups or individuals based solely on religious beliefs would not be allowed. In an investigation into a group of individuals engaging in possible terrorist activities that were attached to a particular religious group, it could nevertheless be of importance to process data specific to the followers of this specific religious group (related to worshipping place, religious preachers, customs, teachings, members and structure of the religious community, etc. that was pertinent to the investigation).

5. Providing information to data subjects

One of the most important obligations of a data controller is to provide information on data processing to data subjects. This obligation is two-fold: it requires the data controller to provide *general information* to the public on the data processing that it carries out and to give *specific* information to data subjects if no restrictions or derogations apply to the data processing.

Deleted: ,

Information provided to the wider public should promote awareness, inform them of their rights and provide clear guidance on exercising their rights. The information provided should be effectively and broadly accessible. Moreover it should include details about the conditions under which exceptions apply to the data subject's rights and how they could submit an appeal to the DPA or to the judiciary.

Deleted: ¶
Deleted: , ,
Deleted: it should
Deleted: .

Websites and other easily accessible media perform a role in informing the public. It is recommended to have in place letter templates on these websites or other media to help the data subjects exercise their rights. It is the responsibility of the data controller to provide information which adequately highlights data protection and data subjects' rights.

In order to comply with the second obligation of giving data subjects specific information regarding data processed, the police shall inform data subjects on the data processing envisaged before the processing or, if it is not possible, for objective reasons, shortly after it. This communication shall comprise information on the data processing, on the collection of the individuals' data and comprehensive information on their rights.

The obligation to provide specific information implies that, in principle, the data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the

[43] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member stateson the protection of individuals with regard to automatic processing
of personal data in the context of profiling
(https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00)

set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.

The information should be provided unless a restriction or derogation applies as described in Point 7, taking into account the specific nature of sensitive files such as criminal intelligence files and files containing sensitive data in order to avoid serious prejudice to the performance of police functions or to the rights of individuals. Even if restrictions or derogations to the right to information were applied, information should be provided to the data subjects as soon as it no longer jeopardises the purpose for which the data were used.

Very often data subjects cannot receive complete information on the processing the police undertake with their data because of restrictions or derogations of their right to information; this should not affect their exercise of the right of access.

Example - For the purpose of covert monitoring of a high risk sex offender, data processing and long-term data retention may be justified without informing the individuals under surveillance if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved, the data subject should be informed about the fact that she or he was subject to such measure.

6. Data subject's rights[44]

Accessing their personal data is a fundamental right for data subjects as it allows them to be aware of the processing on data related to them. Moreover, it can also be a prerequisite to enable the exercise of further rights, such as the right to information, the right of rectification and the right of erasure.

In case an individual has her/his data collected during the course of an investigation or other tasks of the police as described in Point 1, as soon as circumstances safely permit, the police [in principle] should inform the individual of the data processing if there is such request. Specific information should be given in clear and plain language upon request. The communication has to contain the same information as described in point 5, unless data subjects wish otherwise.

The law can provide, under the strict conditions described in Point 7, that the right to be informed upon request may also be limited or excluded, should the provision of such information prejudice the investigation, or another important police task, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified.

The police should aim to answer even general questions arising from data subjects on the processing activities in relation to their personal data, but can use standardised forms to facilitate communication.

Example: If a data subject asks the police on data it processes about them, the police should provide a detailed answer with legal references, if no exception is applicable, but should do so in a plain language, avoiding uncommon or specialised expressions.

The right of access should, in principle, be free of charge.

It is possible to charge a reasonable administrative fee for the request if national law permits and the request is manifestly unfounded or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such refusal.

To ensure a fair exercise of the right of access, the communication "in an intelligible form" applies to the content as well as to the form of a standardised digital communication. It is, however, advisable to refer to national legislation to ensure consistency and to avoid suspects utilising this method to find out whether there is an on-going investigation into them.

[44] Paragraph removed from previous Point 17.

Deleted: ,
Deleted: ,
Deleted: .
Deleted: subjects, because of restrictions or derogations of their right to information, cannot
Deleted: ,
Deleted: the
Deleted: ,
Deleted: request .
Deleted: ,
Deleted:
Deleted: ,
Deleted: ¶
Deleted: on
Deleted: , if no exception is applicable,
Deleted: ,
Deleted: ,
Deleted: ,
Deleted: such refusal

In respect of direct access, the data subject can request access to the controller of the files. The data controller will assess the request and any possible restriction or derogation which can only be used if it is vital for the performance of a specific police task as described in Point 1 or it is necessary for the protection of the data subject or the rights and freedoms of others and reply directly to the data subject. In case of a restriction, partial information and in case of derogation, information on the use of derogation shall still be given with the motivation for using such measures in both cases, as well as information concerning redress.

Example: The access request can be refused if there is an on-going investigation on the person and providing the data subject access to the data could compromise such investigation.

If restriction or derogation were to be used, any answer should take into consideration, according to national law or practice and all circumstances to which the restriction or the derogation is applicable.

As a rule, domestic law should, ideally, provide for direct access. If the right of access provided for is indirect, the data subjects may direct their request to the supervisory authority, which after being properly mandated, will carry out the request on their behalf and conduct checks regarding the availability and lawfulness of the processing of the data subject's personal data. The supervisory authority will then reply to the data subject (providing what data is possible to release, subject to any legally allowed restrictions or derogation). In case of a restriction or derogation, the same communication should be made possible as in case of a direct access.

The data controller should assess the request and reply to the data subject within a reasonable time limit, as provided for by domestic law.

There should be arrangements in place to confirm the identity of the data subject before access to any data is granted as well as to obtain information on the processing activities to which the request refers. The same holds if the data subjects delegate the authority to someone else to exercise their rights.

It is an essential right of the data subjects to be able to amend any incorrect data held on them. If the data subject finds data that are incorrect or irrelevant, she/he should have the right to challenge it and ensure that they are amended or deleted.

In some cases, it may be appropriate to add additional or corrective information to the file. It is important to underline that this right can only be exercised with due respect to other individuals' rights, for instance to the rights related to a testimony in a criminal case (which does not preclude per se the exercise of the data subjects' rights related to soft police data).

Data subjects can ask for the deletion of their personal data where such processing is unlawful.

If the data to be corrected or erased has been communicated elsewhere, the relevant authorities should be informed of the changes to be made.

All proposed changes should be supported by evidence. If data subjects can prove by use of the official documentation that the data processed by police in respect to them are incorrect, the data controller shall not have the right of discretion whether to correct them.

It may be necessary for the police, as dealt with under Point 7, not to give information or grant the right of access, of deletion and of correction which might jeopardise an investigation and should therefore be excluded for its duration. Similar restrictions or derogation may be imposed by national law as described in Point 7.

Restrictions or derogations to the rights of data should only apply to the extent necessary and be interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis. Any decision to refuse a data subject's request should be provided in writing (including by electronic means). The response should provide clear justification of the decision making which can be verified by an independent authority or a court. It is possible that communicating the reasons for refusal could pose a risk to law enforcement or the

Deleted: ,
Deleted: ,
Deleted: ,
Deleted: derogation,
Deleted: be
Deleted: ,
Deleted: person, and
Deleted: ,
Deleted: it
Deleted: ¶
Deleted: ,
Deleted: ¶

data subject or to the rights and freedoms of others. If this is the case, it should be documented and provided to the independent authority or court to be verified, if required.

Example - If person A submitted a declaration against person B accusing her/him of committing a serious offence and later it emerges that the accusation was false, it might be relevant for the police to retain the false statement and the information surrounding it.

Although the statement was proven to be false, if the police needs to retain the data in the interest of the investigation, for instance, a clear corrective statement on the file, instead of removing the false statement, would be necessary.

The data subject should be informed of all available options following a refusal decision such as an appeal either to the supervisory authority, to court or to another independent administrative authority.
Depending upon national legislation, specifically whether there is a direct or an indirect right of access, the actual communication of the result of the review or appeal may differ. In the case of indirect access the data subject should at least be informed that a verification of the police file has taken place. Alternatively, the supervisory body may request the police to release the data contained in the file to the data subject. The court or tribunal may have powers to enforce the access, correction or deletion of data from the file even in access-request cases referred to them by police or the supervisory authority.

If police sends a refusal letter it should contain the name, address, web address, etc. of all possible redress.

The data subject should have access to a court or tribunal in order to submit an appeal and to have the reasons for refusal verified if they are not satisfied with the reply given by the supervisory authority or the independent authority. The supervisory authority should have sufficient powers to examine the police file concerned and have the assessment communicated.

7. Exceptions from the application of data protection principles

Exceptions can only be used for specific purposes foreseen by article 8 of European Convention on Human Rights and article 9 of Convention 108, if foreseen by law (the law should be public, open and transparent and also detailed enough) and if they constitute a necessary and proportionate measure in a democratic society.

The exceptions which have to be incorporated into national legislation should not be described in a general way, but should serve a well-defined purpose. Exceptions can be applicable to those principles described under Points 2, 3, 5 as well as to the data subjects' rights (Point 6) in case of some specific purposes in relation to which data processing activities are undertaken. They concern particularly activities undertaken for the purpose of the protection of national security, defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest (which includes purposes in connection with the fulfilment of a state's international legal commitments or obligations, most prominently deriving from the binding decisions of United Nations' bodies, and humanitarian purposes) or the protection of the rights and fundamental freedoms of others.

Example - If giving information to a data subject may endanger the safety of a witness or an informant, this right can be limited in light of such circumstances.

If the exception, as defined by national law providing specific safeguards is used by the police, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. The aim of using exceptions by the police should be limited to cases where the use of those rules and principles would endanger tasks of the police described under Point 1.

Example: If data collected for police purpose in an investigation are likely to serve national security purposes, they can also be used to these latter purposes to the extent set forth by national legislation. If specific

Deleted: for
Deleted: instance ,
Deleted: forafor
Deleted: ,
Deleted: , in addition,
Deleted: legislation
Deleted: ,
Deleted: ,3
Deleted: ,
Deleted: ,
Deleted: In particular they
Deleted:
Deleted: .
Deleted: ;
Deleted: by national
Deleted: .
Deleted: this latter purposes

intelligence proves that money laundering operations have been carried out to finance terrorist operations, data collected on individuals during the investigations on money laundering can be used for the purpose of eliminating the close and imminent terrorist risk.

8. Use of special investigative techniques

The police should always adopt the least intrusive means of data processing during its operations. If less intrusive methods can be used to achieve the desired ends, they should be preferred. The use of special investigative techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods.

With increasingly sophisticated technological developments, electronic surveillance has become easier; however, the use of these techniques interferes with the protection of fundamental rights and freedoms, in particular the right to privacy. When deciding upon the method of investigation, the high potential of severe interference with the right to privacy has to be balanced with the efficiency of investigations.

Example: In an investigation, the evidence for communication between two suspects can be gathered in various ways. If the same result can be achieved without jeopardising the effectiveness of the investigation by the use of interrogations, testimonies and the obtaining of call data, it is to be preferred to the use of more intrusive surveillance measures such as wiretapping.

9. Introduction of new data processing technologies

If the introduction of new technologies is likely to result in a high risk to the individual's rights, the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. The introduction of new data processing technologies is considered to be subject to a DPIA as probability of risks to the individual's rights is usually high. It is recommended that the assessment of risk is not static but takes into account the specific case: it is repeated at reasonable intervals and that it touches upon relevant phases of the data processing activity. The relevance of the DPIA shall be checked at reasonable intervals.

It is also of great importance to consider the highest standards when introducing new technologies in terms of data security and safety of communications.

Example - New data mining techniques may offer extended possibilities for identification of possible suspects and should be assessed carefully for their compliance with existing data protection law, together with assessment of the risks it may represent to individual's rights as well as suggestions for the adoption of safeguards to ensure the protection of data and data security.

The data protection authority has an important role in advising which risks are involved for data protection and which safeguards should be provided to ensure that any technical means comply with data protection law. However, the police do not have an obligation to turn in every case to the supervisory authority where it introduces new technologies. It may do so if the DPIA it previously conducted demonstrates a significantly persisting high risk to the individual's rights notwithstanding the adoption of specific safeguards.

The consultation between the supervisory authority and the data controller should provide the supervisory authority with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller whilst not jeopardising its core functions.

Appropriate details should be provided to the supervisory authority, in particular regarding the type of file, the data controller, the data processor, the legal basis and the purpose of the data processing, the type of data being processed and by whom the data is being accessed, as well as information on retention of data, log policy and access policy and other relevant technical aspects of implementation.

Example: Detailed information on national reference files such as purpose, data controller etc. containing

Deleted: ,

Deleted:

Deleted: ,

Deleted: ,

Deleted: the same result can be achieved without jeopardising the effectiveness of the investigation

Deleted: ,

Deleted: ¶

Deleted: ¶

Deleted: ,

Deleted: ,

Deleted: ,

Deleted: , that in

Deleted: , the highest standard is taken into account when introducing such technologies

Deleted: ,

Deleted: and

Deleted: , including with regard to

Deleted: .

Deleted: ,

Deleted: ,

fingerprint data could be reported to or made available for consultation to the data protection authority.

Following consultation, the data controller should consider carefully to implement any necessary measures and safeguards that have been recommended by the data protection authority.

Example - Introducing an automatic facial recognition system or other system based on the automated processing of biometric data would very likely require consultation in order to obtain a clear picture of the risks to individual's rights. Specific safeguards should be put in place (concerning the data retention time, the cross matching functionalities, the place of the storage of data and the access to data issues, etc.) to comply with data protection principles and provisions wherever needed and recommended after consultation with the data protection authority.

Deleted: be

Deleted: to need

Deleted: Where needed and recommended by the data protection authority after being consulted on the issue, specific

Use of the Internet of Things (IoT) technology in police work

Data sent to and from police during operational activity via the internet are good examples of the IoT already in use. Due to potential security vulnerabilities, IoT requires measures such as data authentication and access control to ensure data security and resilience to (cyber) attacks.

Deleted: ,

Example: In light of their potential security vulnerabilities, smart glass used by police should not be directly connected to a national criminal record database and data collected should be guaranteed a high level of security.

Deleted:

Big data analytics in the police

Technological advances in processing and analysing large and complex data sets leading to big data and big data analytics present opportunities and challenges to the police, who is turning to digital sources and profiling techniques to perform their tasks.

Big data technologies enable bulk collection and analysis of a vast quantity of data generated by electronic communications and devices aggregated with other bulk data. This could interfere with the right to privacy and data protection.

The Council of Europe's Recommendation CM/Rec (2010)13[45] on the protection of individuals with regard to automatic processing of personal data in the context of profiling and the Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data[46] can be of use in the context of Big Data analysis for police use too.

Deleted: Rec(

Deleted: ¶

Big data technologies and analysis techniques may help assist in detecting crime but there are, however, considerable risks to this type of data processing that should be taken into account:

Deleted: ,

- Databases originating from one domain can be used in another domain and for another purpose, which changes the context and may lead to inaccurate conclusions and lack of valid legal basis, therefore to unlawful data processing with possibly serious consequences for the individuals involved.
- Profiling may lead to drawing discriminatory conclusions, which can result in the reinforcement of stereotypes, stigmatisation and discrimination.
- The increasing amount of personal data held in databases may lead to severe vulnerabilities and subsequent risk of data breaches if information security is not guaranteed.

Deleted: ,

Wherever big data relies on personal data, data controllers should pay additional attention to the following requirements:

- Verification of data accuracy, context and relevance of the data.

[45] Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling

[46] Document T-PD(2017)1 - Big Data Guidelines

- Its use requires a high level of accountability.
- Its use shall be combined with methods of investigation which complement the conclusions drawn from the big data analysis. A decision affecting a person shall not be taken solely on automated processing of personal data.
- As for other types of data processing, it is of paramount importance that its use shall be ~~shall be be~~ necessary and proportionate for the fulfilment of police tasks described in Point 1, with special attention for the data processed to be adequate, relevant and non-excessive in relation to the purpose for which they are processed.
- Predictive analysis requires human intervention to assess the relevance of the analysis and conclusions.
- Ethical guidelines developed at national or at international level should be taken into consideration.
- As a principle and subject to restrictions and derogations mentioned in Point 7, transparency should be ensured by the data controller by explaining how the data are processed in accordance with privacy and data protection principles. If data collected for one purpose is used for another purpose, the data controller should, in principle, make the data subjects aware of this subsequent use.
- Even if complex methods are used, the lawfulness of the processing, including subsequent use of data, and compliance with the conditions set by Article 8 ECHR and Convention 108 should be demonstrated.
- An information security policy should be in place and implemented throughout the processing.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals and the administrative and judicial means exist for individuals to challenge those decisions. This implies data subjects' awareness of the reasoning of the algorithm used and the purposes for which it was used.

The above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones, are even more necessary when sensitive data are processed in Big Data analytics.

10. Storage of data

"As pointed out in Point 2", data shall be processed until they have served the purpose for which they were collected. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

There should be a clear distinction in how the police stores and processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses. This should also relate to the specific purpose for which the data was collected. Additional safeguards should be in place for persons who are not suspected of having committed or have not been convicted of a criminal offence. Clear rules have to be established in relation to the handling of different databases with special attention to the analysis of multiple results.

The principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve the purpose of the prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where personal data is processed for the purpose of the maintenance of public order.

The grounds for retention and processing should be reviewed periodically. The unlawful processing of personal data outside of the legal framework allowed for the retention constitutes a severe violation of the right to protection of personal data. If the law in relation with a specific crime provides for a data retention period of 4 years and if personal data are processed in relation with this crime by the police solely on this ground after 4 years have passed since the collection of the data in question and no other legal ground to process this data exists, the retention of this data could be considered as unlawful.

General data retention periods are usually regulated in national or international law. In order to comply with the legislation while ensuring the effectiveness and the success of an investigation, police bodies are strongly advised to develop internal rules and/or recommendations setting the data retention period for personal data or for a periodic review of the need for the storage of personal data.

Deleted: –
Deleted: -
Deleted: the reasoning
Deleted: algorythm
Deleted: ¶
Deleted: ,
Deleted: ,
Deleted:
Deleted: ¶

For example, in a case where the law prescribes a 4 year data retention period but the individual, subject to an investigation, is acquitted from all charges by the court after 2 years, her/his data shall be deleted (if the individual is not a recidivist or there is no information on her/him committing again the same category of crime) from the database, provided that all deadlines for the review of the case have expired. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judicial procedure terminates completely (which means all redress have been made or all deadline for redress have been passed).

The police should provide systems and mechanisms to ensure that the data that are stored are accurate and that their integrity is maintained.

International obligations, which include providing data to international bodies such as Europol, Eurojust and INTERPOL, bilateral agreements and mutual legal assistance between member states and third countries must be observed when shaping internal policies.

Data should be categorised according to the degree of accuracy and reliability in order to assist the police in their activities. It is recommended that handling codes are used to distinguish these categories. A classification system facilitates the assessment of the quality of the data and is the reliability. Classification of data is also important when it is to be communicated to other police bodies or states.

Example - Information collected directly from a person's statement will be assessed differently than information collected from a person's hearsay statement. Data based on facts, or 'hard' data, will be assessed differently than data based on opinions or personal assessments or 'soft' data.

Personal data collected by police for administrative purposes must be kept (as far as possible logically and physically) separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by law.

Examples of administrative data include lists of data on licence holders or data on human resources and firearms certificates.

11. Communication of data within the police sector

A distinction should be made between domestic communication of data and international transfer of data. Depending upon who is receiving the data, whether it is the police, another public body or private party, different requirements apply within these two distinct operations. The police can only communicate personal data within the police sector if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

There should be clear and transparent rules on how the police grant access to data held by it and on which grounds.

The police, domestically, should only share information (among police) when there is a legal basis for the request, e.g. an on-going criminal investigation or a shared law enforcement task and laws or agreements allowing the communication.

The police can share data with other police organisations if the personal data are relevant for the purpose of prevention, investigation and prosecution of criminal offences and execution of criminal penalties and where they are processed for the purpose of the maintenance of public order.

The communication of personal data in general should be in line with the general considerations described above.

Deleted: ,

Deleted: how reliable it is

Deleted: ,

Deleted: :

Deleted: ¶

Deleted: ¶

Deleted: Within these two distinct operations different requirements apply,

Deleted: depending

Deleted: a private party

Deleted: be in

Example: A police unit can share data on a suspect who presumably committed a tax fraud with another police unit investigating a murder case if there is indication that the suspect for this crime could be the same person or if doing so will materially assist the investigation.

Deleted: ¶

12. Communication of data by the police to other public bodies

The communication of data outside police is permissible if it is provided for by law and the data are required by the recipient to enable them to fulfil their lawful task. Mutual assistance agreements foreseen by the law between law enforcement and public bodies allows the public bodies to have access to law enforcement data which would be essential in the fulfilment of their duties and tasks (for example in their investigations or other legal duties in accordance with national law).

Deleted: ¶

Stricter principles than those set forth in Point 11 should be followed when data are to be transmitted domestically outside of the police sector as there is a risk that the processing of personal data, which are considered sensitive, could result in adverse effects for the individual.

Deleted: ,

Communication of data to any other public authority may also be allowed if it is foreseen by law, if it is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to other persons, to public order or to public security.

Deleted: ,

Deleted: or

The communicated data may only be used by the receiving body for the purposes for which the data were transferred.

Example - A claim for a residence permit is made by a migrant. Police data may be required to verify if the person was ever involved in criminal activity. It would be in the interest of the Immigration Office and the claimant for this communication of data to take place.

13. Communication of data by the police to private parties

There may be occasions when, under strict conditions, the police can communicate data to private bodies. This communication has to be based in law and can only be done by the authority which is processing the data. Such communication can only be done for the purpose of the investigation or other important police tasks as described in Point 1, in the interest of the data subject, for humanitarian reasons or if it is necessary to prevent serious and imminent risk to public order or public security. For example, there might also be instances where police data may be communicated to humanitarian organisations based on international law in the interest of the data subject or for humanitarian reasons.

Deleted: ¶

Deleted: ,

Where the police shares data with media in respect of making information related to an investigation public, special consideration should be given to the assessment to determine whether it is necessary and that such publicity is allowed in the public interest.

Deleted: that

Deleted: that such publicity is allowed.

Such communication should only be on a case by case basis and in each case there must be a clear legal basis providing the necessary procedure (e.g. need for specific authorisation) to be followed for any such communication to occur.

Example - When the police communicate with the financial sector in relation to known fraud or theft offenders, when it communicates with an airline about stolen or lost travel documents or when the police releases details of wanted persons believed to pose a risk to the general public.

14. International transfer

Any transfer of police data internationally should be limited to police bodies and should be fit for such purpose and is in accordance with the law. For this, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data handling, regional legal

Deleted: ¶

frameworks such as EU and EU institutions' legislation (on Europol, Eurojust, Frontex, etc.) and subsequent agreements (operational bilateral agreements), bilateral treaties and in general, international agreements on mutual assistance, other bilateral or multilateral agreements made regarding effective cooperation can be of use.

When considering sharing any data, consideration should be given as to whether the receiving authority is performing a function conferred to it in law related to the prevention, investigation, or prosecution of criminal offences, the execution of criminal penalties and the maintenance of public order, and whether the sharing of the data is necessary to perform its specific task.

The sending authority should ascertain that there is an appropriate level of data protection in the receiving state and that the receiving state complies with the relevant rules of international transfers of personal data. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. This means that transfer should be used as a last resort option. International transfers framework such as "INTERPOL's Rule on the Processing of Data" and its "Statute of the Commission for the Control of INTERPOL's files" Rules on the Control of Information and access to INTERPOL's Files", the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185) may be taken into account[47] so as to ensure that any transfer of data is legally justified and has appropriate safeguards in place. The request should clearly state all the necessary elements from the requesting party to enable the receiving party to make a sound decision on the request. These details would be expected to include the reason for the request as well as the purpose for the transfer of data.

An appropriate level of data protection should be guaranteed (e.g. through ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments) if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

If there are conditions applied by the sending authority in relation to the use of the data in the receiving state, these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout its lifecycle.

Example - Further transfer of data should only be allowed if this is necessary for the same police purpose as the original transfer and the second recipient is also a police body ensuring an appropriate level of data protection. The police body which originally sent the data must also consent to the onward transfer. If the police from country X sends personal data to the police of country Y, it is only permissible for the country Y to transfer this data if all the above requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) if country X consents to the transfer. If the data is sent to country Z, which is a non-member of the Convention 108, then country Y should ascertain that this country provides an appropriate level of protection of personal data and effective means of exercise of the related data subject rights.

The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases if it is required for the performance of the task of the transferring authority and if there is no effective means of transferring the data to a police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers.

Example: If tax authorities in country X requests the police in country Y about the whereabouts of a person involved in non-criminal tax evasion because they have evidence that the person is involved in criminal matters in country X, the police can transfer the personal data of the individual.

The international transfer of personal data between police and private bodies in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police as described in Point 1, provided by legal means and where the

[47] This is without prejudice to the right of the Committee of Convention 108 and other instances disposing such power to assess and to review if necessary the level of data protection guaranteed by those multilateral agreements

Deleted: , or

Deleted: ,

Deleted: of

Deleted: police purpose

Deleted: above

Deleted: of protection

Deleted: of personal

Deleted: and private

emergency, the gravity of the crime, its trans-border nature and the involvement of the police would not be possible for objective reasons. Other facts such as data security, the reassurance received as to the use of the data and the lawfulness of the data transfer in the receiving country have to be taken into account. In this context it is to be noted that, in such a case, the data controller has a double obligation with respect to the protection of personal data: one imposed by the legal framework of the country where it resides and the one which is related to the data transfer. The local police should be informed afterwards. The police are required, wherever possible, to make use of existing international legal instruments, in respect of this type of data transfer. International transfers may also exceptionally occur where the police communicate personal data for humanitarian purposes.

Example: In an investigation, carried out within the framework of an international multilateral agreement, into child sexual exploitation where the victim is in country Y and the police there have commenced an investigation and the material has been made available on the internet by the suspect residing in another (country X) and there is a high risk that the suspect seeks to avoid justice by fleeing country X, the police in country Y can request, on an exceptional basis, that a service provider in country X provide the whereabouts of its customer. However, the police of country Y should inform the police in country X of its operation as soon as is possible and then seek to resolve the matter in cooperation.

15. Conditions for communications

Since there is a general obligation for the data controller to ensure a high level of data quality, it is advisable to have in place an additional check before sharing the data with others. When communicating or transferring data, it is always advisable to double-check the quality of data, if it is correct, up-to-date and complete. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated. It is required to establish secure channels of communication which ensure data security at the highest level possible. The quality of data can be assessed up to the moment of communication.

Example: If personal data that contain incorrect data (personal or otherwise) are sent, they could adversely affect the investigation, cause harm to the individual concerned or others involved, or who may become involved as a result of the incorrect data being transferred. This can, as a result, leave the police in the transmitting and receiving states open to civil redress. In essence, if an individual is arrested based on a wrong communication of the suspect's name, it seriously harms several human rights of the individual concerned and can undermine any criminal investigation.

16. Safeguards for communication

It is of utmost importance that the necessity and purpose limitation principle should be applicable for any domestic communication or international transfer of personal data outside of police organisations.

Any data communicated should not be used for anything other than the purpose for which it was sent or received. The exceptions to this are when the sending authority, based on legal provisions, gives agreement to any further use, and if it is necessary and vital for the recipient to fulfil their task. Data can also be communicated if it is in the interest of the data subject, for humanitarian reasons, and is necessary to prevent serious and imminent risk to public order or public security or an appropriate level of data protection is guaranteed by the recipient by international, national legal instrument, ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments, as foreseen by Convention 108.

Example: Personal data sent by the police of country X to the police of country Y in a money laundering case cannot be used by the police as profiling on the given individual in respect of her/his religious beliefs or political activities (unless those are relevant to the crime committed and police in country X has given its consent for this use).

17. Interconnection of files and on-line access to files

Deleted: where
Deleted:
Deleted: communicates
Deleted: ,
Deleted: ,
Deleted: ,
Deleted: ¶
Deleted: ¶
Deleted: , and
Deleted: it is
Deleted: subject,for
Deleted: ,

In specific circumstances, the police may seek to collect data by coordinating its information with other data controllers and processors. Furthermore, it may combine personal data stored in different files or in different databases that are held for different purposes such as those held by other public bodies and/or private organisations. This may be in relation to an on-going criminal investigation or to identify thematic trends in relation to a certain type of crime.

In order for these actions to be legitimate they must be authorised or be underpinned by a legal obligation to comply with the purpose limitation principle.

If the relevant police body has direct access to files of other police or non-police bodies, it must only access and use the data if domestic law, which should reflect the key data protection principles, permits.

Clear legislation and guidance, which adheres to the data protection principles, should exist for cross-referencing of databases. Such cross referencing should be necessary, purpose bound and proportionate. With relation to personal data stored in other data controllers' or processors' database all conditions described in Point 2 have to be fulfilled and regularly checked.

Example - Data held for citizenship purposes can only be used in an investigation if the national legislation allows it and to the extent to which it is necessary for the purpose of the investigation to do so. For instance, the number of children a suspect has may not be relevant in an investigation and should therefore not be processed by police. Access in this case to a database can be perfectly lawful but it can only be legitimate if it respects the principles of data protection.

18. Data security

The police must take appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data. The controller must notify, without delay, at least, the competent supervisory authority of those data breaches which according to its assessment may seriously interfere with the rights and fundamental freedoms of data subjects. The information of data subjects of data breaches which may seriously interfere with their rights may also have to be ensured without undue delay, unless it jeopardises the task of the police.

Information security is essential to data protection. It is a set of procedures to ensure the integrity, availability and confidentiality of all forms of information within the police organisation with the aim of providing security of data and information and limiting the impact of security incidents and data breaches to a predetermined level.

The level of protection given to a database and/or an information system or network is determined by a risk assessment. The more sensitive the data, greater protection is required.

Authorisation and authentication mechanisms are essential to protect the data and sensitive information should always be encrypted. It is considered best practice to have in place an audit regime to regularly check that the level of security is appropriate.

Police authorities are advised, where necessary, to conduct DPIA (see Point 4) to assess the privacy risks to individuals in respect of the collection, use and any disclosure of information. This will help to identify risks and develop solutions to ensure that concerns are addressed appropriately. Any such impact assessment should cover relevant systems and processes of processing operations, but not individual cases.

A Data Protection Officer (DPO) within the police can play an essential role in carrying out internal audits and assessing the legitimacy of the processing, which contributes to a higher level of data protection and data security within the organisation. Moreover, the DPO can facilitate the dialogue between the organisation and the data subjects as well as the organisation and the supervisory authority which can add to the overall transparency of the police body.

Deleted: ,

Deleted: ir

Deleted: if domestic

Deleted: so

Deleted:

Deleted: ,

Deleted: ¶
¶

Deleted: jeopardisese

Deleted: ,

Deleted: ,

Deleted: are

Deleted: the

Deleted: ,

Deleted: ,

An Identity & Access Management System (IAM) may be recommended to manage employees and third party access to information. This will require authentication and authorisation to access the system and to set privilege rights to determine what can be viewed. IAM can be seen as a useful requirement to ensure safe and appropriate access to data.

The data controller, following an evaluation of the risks, should implement measures in respect of:

- equipment access control,
- data media control,
- storage control,
- user control,
- data access control,
- communication control,
- input control,
- transport control,
- recovery and system integrity,
- reliability and integrity.

Privacy-by-Design

The concept of privacy-by-design is an integral part of data security. Data protection and security may be embedded directly into information systems and processes, using technical and organisational measures, to ensure a high level of data protection and security and, in particular, to minimise the likelihood of data breaches. This approach is known as Privacy–by–Design, promoting privacy and data protection compliance from the start. It can be achieved through software and/or hardware. It requires a threat analysis, a full life cycle approach and rigorous testing.

Data controllers should ensure that privacy and data protection is a key consideration in the early stages of any project and then throughout its life cycle; specifically, when building new IT systems for storing or accessing personal data, developing legislation, policy or strategies that have privacy implications and embarking on an information sharing initiative using data for new purposes.

Privacy-by-Design requires the implementation of Privacy Enhancing Technologies (PETs) to enable a better protection of personal data. PETs prevent unnecessary processing of personal data without losing functionality in the information system itself.

Example: Body scanners used for police purposes have to be designed to respect the privacy of the individuals being inspected while fulfilling the purpose of their use. Therefore the body image in such tools has to be blurred by default.

19. External control

There has to be, at least, one supervisory authority responsible for ensuring compliance of data processing to the international and national legislation within the law enforcement sector.

Certain states may require more than one supervisory authority, for instance a national or federal authority and a number of decentralised or regional authorities, whilst others will prefer to have a single supervisory authority responsible for the entirety of the supervision of data processing operations.

The supervisory body should be completely independent, meaning that it belongs neither to the law enforcement organisation nor it is directed by another body within the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties and should not be instructed or forced to accept instructions from anybody. The personal independence of its chair/president including political, financial, functional and operational independence, are decisive factors when judging how independent the supervisory body is.

Deleted: at

Deleted: ¶

Deleted: .

Deleted: S

Deleted: ¶

Deleted: ,

Deleted: ,

Deleted: does not

Deleted: ,

Deleted: is

Deleted: h

National law should provide for advisory, investigative and enforcement powers to enable it to investigate complaints, to have regulatory measures or to be able to impose sanctions where needed. The legal and administrative tools at its disposal shall be efficient and enforceable.

Supervisory authorities should have the ability to cooperate in law enforcement matters bilaterally and also via the Committee of Convention 108.

Example: The supervisory authority must be independent and have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Deleted: has to

Glossary/Definitions

For the purposes of this Guide:

a. “personal data” means any information relating to an identified or identifiable individual (“data subject”);

b. “genetic data” are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

c. “biometric data” are data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual;

d. “soft data” (evidence based on testimony or other personal assessment) means data acquired through testimony of person involved in the investigation;

e. “hard data “(evidence based on documents or proven facts) means data acquired from official documents or other certified sources;

f. “data processing” means any operation or set of operations which is performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, data processing means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

g. “controller” means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has the decision-making power with respect to data processing;

h. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;

i. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.

j. Internet of Things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

k. “covert surveillance” means all measures aiming at monitoring discreetly the movements of persons, vehicles and containers, particularly those involved in organised or cross-border crime.

l. “special investigative techniques” techniques applied by the competent authorities in the context of criminal investigation for the purpose of detecting and investigating serious crimes and suspects, aiming at gathering information in such a way as not to alert the target person.

m. “privacy-enhancing technologies” (PETs) means a range of different technologies to protect personal data within information systems. The most important aspect for the use of PETs is to determine whether identifiable information is needed when a new information system is being developed, conceived, or an existing system upgraded.

Deleted: “ (

Deleted: ¶

Deleted: :

Deleted: if

MEMBER OF THE EUROPEAN COMMITTEE ON LEGAL COOPERATION/MEMBRE DU COMITE EUROPEEN DE COOPERATION JURIDIQUE

Following T-PD request may I be allowed to submit the following observations:

I am grateful for the opportunity to comment on the Draft practical guide on the use of personal data in the police sector.

It seems more appropriate to mention as the example under point 14 the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data instead of EU agencies regulations (Frontex, Europol, Eurojust). As regards EU, the main volume of international transfer of data is effected by EU Member States authorities and not by the EU agencies. Directive is more comprehensive than EU agencies rules. The future of personal data processing rules for EU institutions and bodies is now being amended (proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/ECThe relationship between point 11 and 12 is somehow unclear. The personal data processing both by the law enforcement authorities and other public authorities is subject to same principles (lawfulness, purposefulness, data quality, fairness and accountability). Therefore, the term “stricter rules” does not seem appropriate. I would recommend to consider “specific rules have to be in place when data are to be transmitted domestically outside of the police sector”.
In any case the first paragraph of point 11 seems to overlap with 12 and 14. As second paragraph also seems to refer to access by external (to police) bodies to data held by the police one may wonder whether first two paragraphs are necessary in point 11 and whether they do not create confusion. Probably point 11 would be more clear without first two paragraphs (limited to description of processing within law enforcement sector).

By the way, the accountability is mentioned only once in the guide when discussing big data processing. I would suggest to consider elaborating a little bit more on it, stressing for instance that controllers (within the police) are responsible for the compliance with data protection rules and they should be able to demonstrate it at any time. It is not only the supervisory authority that is responsible for ensuring compliance of data processing to the international and national legislation within the law enforcement sector (point 19), that compliance exists *per se*, by design (penultimate paragraph on page 10), that it is limited to the relevance of data (last paragraph on page 2 and second paragraph under point 3) or enforceable only with regard to big data processing. Accountability requires the active implementation of measures by controllers to promote and safeguard data protection in all their processing activities.

MONACO

Cette nouvelle version, qui laisse apparaître une vision beaucoup plus restrictive de l'utilisation des données personnelles par la police que la version précédente, n'appelle pas de demande de modification de la part des autorités monégasques, à l'exception du point suivant :

- dernier paragraphe de l'introduction : l'introduction fixe les grands principes à l'aune desquels les autres dispositions du guide doivent être interprétées.

Dans sa rédaction antérieure, ce paragraphe posait le principe d'un juste équilibre entre les objectifs poursuivis par les autorités publiques et la protection des droits des personnes, notamment leur vie privée.

La nouvelle version proposée abandonne le principe de ce juste équilibre au profit, selon la formule projetée, du "respect total du droit à la protection de la vie privée et à la protection des données".

Cette rédaction n'apparaissant pas de nature à garantir une conciliation équilibrée entre ces objectifs contradictoires, **MONACO propose de revenir à la rédaction antérieure. (Version rouge barrée).**

Cette notion de juste (soigné) équilibre, qui existe pour le traitement des données sensibles (art.4), est davantage conforme à l'esprit du Guide et transparaît également dans l'écriture du Guide dont de nombreuses dispositions font usage du conditionnel (exemples : la police devrait toujours choisir la base légale...les enquêteurs devraient....).

Telle est la proposition des autorités monégasques.
.

NETHERLANDS/PAYS-BAS

Herewith I would like to hand in two comments that the Netherlands would like to make with regard to this draft guideline:

- On page 3: two paragraphs cover the same topic (about the further processing of personal data). See paragraphs 6 and 9. The Netherlands proposes to integrate the topic into paragraph 3.

- On page 11, as regards the distinction between 'categories of personal data' (in the second paragraph) and 'reliability of personal data' (tenth paragraph): here, the guideline diverts from the EU-Directive on the use of personal data in the police and criminal justice sector. This EU-Directive links this distinction to the words 'where applicable and as far as possible', respectively 'as far as possible'. You may find this in articles 6 and 7 of the EU-Directive mentioned before. The Netherlands can only agree with the guideline whenever this wording is taken up in the said paragraphs of the draft guideline.

SWITZERLAND / LA SUISSE

Introduction

La Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police énonce un ensemble général de principes à appliquer dans ce secteur pour garantir le respect du droit à la vie privée et à la protection des données prévu par l'article 8 de la Convention européenne des droits de l'homme et par la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (« Convention 108 »).
Depuis son adoption, la Recommandation (87)15 a fait l'objet de plusieurs évaluations (en 1993, 1998 et 2002), sur le plan tant de son application que de sa pertinence. En 2010, le Comité consultatif de la Convention 108 a décidé de réaliser une étude[48] sur l'utilisation de données à caractère personnel dans le secteur de la police dans l'ensemble de l'Europe. Cette évaluation a montré que les principes de la Recommandation (87)15 constituaient toujours un point de départ approprié pour élaborer des réglementations s'appliquant à cette matière au niveau national et que l'élaboration d'un guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police, sur la base des principes énoncés par la Recommandation (87)15, fournirait des éléments d'orientation sur ce que ces principes impliquent au niveau opérationnel.
Le présent guide a donc été élaboré pour mettre en évidence les questions les plus importantes qui peuvent se poser dans le cadre de l'utilisation de données à caractère personnel par la police et pour signaler les principaux éléments à prendre en compte dans ce contexte.
Il ne reproduit ni les dispositions de la Convention 108 ni celles de la Recommandation (87)15 mais se concentre sur des éléments d'orientation pratiques.
Les principes généraux de la Recommandation (87)15 et leurs implications pratiques visent à ce que l'utilisation des données à caractère personnel dans le secteur de la police soit déterminée dans le respect total du droit à la protection de la vie privée et à la protection des données.
Pour faciliter la lecture du guide, un glossaire des termes utilisés est fourni à la fin du document.

Considérations générales

La collecte et l'utilisation de données à caractère personnel à des fins policières constitue une ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel prévus par l'article 8 de la Convention européenne des droits de l'homme et par la Convention 108 et doivent par conséquent être fondés sur des dispositions légales (claires et publiquement disponibles), poursuivre un but légitime et se limiter à ce qui est nécessaire pour atteindre le but poursuivi. (Déplacé du paragraphe 2)

Tout traitement de données doit être entièrement conforme aux principes de nécessité, de proportionnalité et de limitation de la finalité. Cela signifie que le traitement de données personnelles par la police devraient être effectué sur la base d'un but prédéfini, précis et légitime prévu par la loi. Il devrait être nécessaire et proportionné à ces fins légitimes et en aucun cas effectué d'une manière qui soit incompatible avec ces finalités. En outre, ce traitement devrait être assuré de façon licite, loyale et transparente, et être adéquat, pertinent et non excessif par rapport aux finalités. Enfin, les données devraient être exactes et actualisées pour que leur qualité soit optimale.

1. Champ d'application

Les principes énoncés dans le présent guide s'appliquent au traitement de données à caractère personnel à des fins policières, à des fins de prévention, d'investigation et de répression des infractions pénales, d'exécution des sanctions pénales et du maintien de l'ordre public par la police (désignée plus loin par : « les tâches de la police »). Le terme « police » utilisé dans le texte désigne plus généralement les services chargés de l'application de la loi et/ou d'autres organes publics et/ou entités privées autorisés par la loi à traiter des données à caractère personnel pour les mêmes fins.

[48] Voir le rapport « Twenty–five years down the line » de Joseph A. Cannataci.

Deleted: ,
Deleted: continuaient de constituer
Deleted: clairs et concrets
Deleted: à cette fin. Il vise à
Deleted: Ce guide
Deleted: lors de
Deleted: er
Comment [A66]: Cette formulation est trop péremptoire. Nous souhaitons que l'ancienne soit reprise, qui correspond mieux au préambule du la recommandation R (87) 15 elle-même (par 5)
Deleted: un juste équilibre soit trouvé entre les objectifs essentiels d'intérêt public général (prévention, investigation et répression des infractions pénales, exécution des sanctions pénales et maintien de l'ordre public) ainsi que le respect des droits des personnes
Deleted: s
Deleted: présent
Deleted: peut
Deleted: r
Deleted: du point 2
Deleted: Le
Deleted: devrait
Deleted:
Deleted: l
Deleted: s
Deleted: 'il ne devrait être effectué par dans la police devraient être traitées
Deleted: que dans
Deleted: ,
Deleted: qu'ils
Deleted: ,
Deleted: qu'il devrait toujours être
Deleted: la
Deleted: initialement poursuivie
Deleted: Il faudrait en o
Deleted: que
Deleted: soit
Deleted: qu'il soit
Deleted: les données traitées par la policeils
Deleted: ,
Deleted: principalement aux
Deleted: .
Deleted: par la suite
Field Code Changed

2. Collecte et utilisation des données

La police en tant que responsable du traitement de données, assume toutes les responsabilités concernant les traitements qu'elle effectue et sur lesquels elle doit rendre des comptes.

La collecte de données personnelles pour des objectifs de police devrait être limitée à ce qui est nécessaire à la prévention d'un danger réel ou la suppression d'une infraction précise. Toute exception à cette disposition devrait faire l'objet d'une législation nationale particulière.

Il est compris par le point 2.1 de la Recommandation que, dans l'accomplissement des deux tâches principales de la police (prévention d'un danger réel et suppression d'une infraction précise), une corrélation évidente et directe doit exister entre le traitement des données effectué par la police et une situation ou des individus ont commis ou sont susceptibles de commettre un crime.

La police devrait toujours choisir la base légale appropriée pour traiter des données personnelles et le faire de façon légitime. Elle devrait soigneusement évaluer si le traitement a bien une base légale et si les procédures prévues sont entièrement respectées. Les principes de la protection des données sont pertinents à tous les stades du traitement (surtout les principes de nécessité, proportionnalité et limitation de finalité) et on ne devrait pas traiter des données qui ne sont plus nécessaires au but poursuivi. Dans ce contexte, les données personnelles collectées à une phase précoce d'une enquête et qui au long de l'enquête ne se révèlent plus pertinentes ne devraient plus être traitées (par exemple, quand l'innocence d'un suspect est confirmée). Elles devraient donc être bloquées ou supprimées. Cela ne s'applique pas lorsqu'une utilisation ultérieure des données est autorisée.

Avant et pendant la collecte de données à caractère personnel, il faudrait toujours se demander si de telles données collectées sont nécessaires à l'enquête ou à d'autres taches de la police comme prévu au point 1. Il convient de noter que, une fois les données personnelles recueillies, il devrait exister un lien clair entre la personne dont les données sont traitées et le but du traitement (c'est-à-dire l'enquête ou la tâches spécifiques de la police). Ce lien, ainsi que la conformité aux principes de protection des données décrits dans le Guide, doivent être démontrés à tous moments. Après la collecte et aux différents stades de l'enquête, il faut impérativement procéder à une analyse approfondie pour évaluer quelles sont les données qui doivent être conservées et celles qui doivent être effacées.

Avant de procéder à toute collecte de données à caractère personnel, les enquêteurs devraient se poser les questions suivantes : «Pour quelle raison l'obtention de ces données est-elle nécessaire? », « Quel est exactement le but poursuivi ? ».

Exemple : S'agissant de données personnelles telles que des factures téléphoniques, seuls le(s) numéro(s) nécessaire(s) à la période sur laquelle porte l'enquête devraient être demandés et uniquement pour la ou les personnes susceptibles d'être en lien avec l'infraction.

Une liste des numéros de téléphone de la ou des personnes impliquée(s) dans l'infraction présumée peut être obtenue si des éléments existent indiquant que ces données peuvent servir l'enquête. Elles ne peuvent pas être conservées ou traitées une fois que l'analyse a montré qu'elles n'étaient pas strictement nécessaires à la finalité de l'enquête.

Conformément au principe de limitation de la finalité, les données à caractère personnel collectées à des fins policières doivent servir exclusivement à de telles fins et ne doivent pas être utilisées d'une manière qui soit incompatible avec cette finalité initiale énoncée au moment de la collecte, sauf disposition contraire de la loi (voir article 9 de la Convention 108). [Lors de l'évaluation de la compatibilité de l'utilisation des données pour une même finalité, les critères suivants devraient être pris en compte : (i) relation entre les objectifs ; (ii) contexte de la collecte et informations fournies aux personnes concernées ; (iii) nature des données personnelles ; (iv) conséquences pour les personnes concernées de l'utilisation ultérieure envisagée ; (v) existence de garanties appropriées.]
Dans le cadre de ce guide, une utilisation ultérieure des données est considérée comme une nouvelle opération de traitement de données qui doit remplir tous les critères et les conditions mentionnées plus haut.

Deleted: La collecte et l'utilisation de données à caractère personnel à des fins policières devrait se limiter à ce qui est nécessaire et proportionne à la prévention, l'investigation et la répression d'infractions pénales ainsi qu'à l'exécution de sanctions pénales (pour une des infractions pénales déterminées ou la suspicion de'une telles infractions par exemple) et au traitement de données à caractère personnel ayant pour finalité le maintien de l'ordre public. …a police comme…

Deleted: Interprétant le …oint 2.1 d…

Deleted: ¶
La collecte et l'utilisation de données à caractère personnel à des fins policières peut constituer une ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel prévus par l'article 8 de la Convention européenne des droits de l'homme et par la Convention 108 et doivent par conséquent être fondés sur des dispositions légales (claires et publiquement disponibles), poursuivre un but légitime et se limiter à ce qui est nécessaire pour atteindre le but poursuivi. ¶

Deleted: déquate…propriée pour …

Deleted: Interprétant le point 2.1 de la Recommandation il est compris que pendant l'accomplissement des tâches de la police (prévention d'un danger réel et la suppression des infractions pénales déterminées) une corrélation évidente et directe doit exister entre le traitement poursuivi par la police et une situation ou des individus ont commis ou potentiellement vont commettre un crime.¶
¶

Deleted: n… et pendant la collecte …

Deleted: La police devrait appliquer le principe de minimisation des données à toutes les étapes du traitement et ne devrait pas continuer à traiter des données qui ne sont pas nécessaires à la finalité poursuivie. Les données à caractère personnel qui sont collectées à un stade initial de l'enquête et pour lesquelles il est par la suite établi au cours de l'enquête qu'elles ne sont plus pertinentes ne devraient plus être traitées (par exemple, lorsque l'innocence d'un suspect est confirmée).

Deleted: la…collecte de données à …

Deleted: découlant telels que …

Deleted: 'il exis…te …es éléments …

Deleted: d… moment de la collecte …

Deleted: …ans le cadre de ce guid…

L'utilisation ultérieure des données doit être licite, servir une finalité légitime et y être nécessaire et proportionnée.
Comme cela est indiqué dans les Considérations générales, la police devrait s'assurer, à toutes les étapes du traitement des données et pour leur utilisation ultérieure, que les données personnelles sont exactes, à jour, adéquates, pertinentes et non excessives par rapport aux buts pour lesquels elles sont traitées.

Exemple : les données collectées par la police dans le cadre d'une enquête où l'affiliation politique de la personne concernée n'a pas d'importance ne peuvent pas être utilisées pour déterminer l'appartenance politique de la personne concernée, sauf si la loi l'autorise.

3. Utilisation ultérieure des données

Tout traitement ultérieur de données pour des finalités policières autres que celles pour lesquelle elles ont été recueillies en premier lieu, doit respecter les obligations légales applicables au traitement de données à caractère personnel : être prévu par la loi, poursuivre une finalité légitime et être nécessaire et proportionné au but légitime poursuivi.
Les données à caractère personnel traitées ultérieurement devraient avoir un lien avec une finalité policière et doivent satisfaire aux critères et conditions du point 2. La règle générale est que si les données sont susceptibles d'être utilisées dans un autre dossier ou dans une autre opération de police, l'analyse de conformité décrite au point 2 devrait être appliquée également pour le nouveau traitement. (Cela n'est pas applicable si les données sont utilisées dans un but purement statistique ou scientifique). Nonobstant le traitement numérique et / ou automatisé des données et du volume important de données personnelles stockées très souvent dans des environnements de traitement différents, les données personnelles recueillies et conservées à des fins de police ne doivent pas être conservées et traitées à des fins non spécifiques ou générales ou d'une manière incompatible au principe de limitation de finalité.
Il convient par ailleurs de noter que toute utilisation ultérieure de données à caractère personnel liées à des personnes vulnérables, telles que victimes, mineurs, personnes bénéficiant d'une protection internationale, devrait faire l'objet d'une attention particulière être soumise à une analyse juridique qui veillerait particulièrement à l'application des principes de nécessité et de proportionnalité.
Dans des affaires concernant la traite d'êtres humains, le trafic de drogue, l'exploitation sexuelle, etc., dans lesquelles les données des victimes peuvent être utilisées ultérieurement lorsqu'elles sont aussi considérées comme des suspects, ou dans lesquelles la protection des victimes d'un crime plus grave peut l'emporter sur l'intérêt de poursuivre des crimes moins graves, il est conseillé aux services de police de se référer aux bonnes pratiques internationales existantes (au sein des instances policières internationales ou régionales) et d'améliorer la façon dont ils échangent des informations sur la question avec d'autres services de police nationaux. Si toutes les exigences légales telles qu'énoncées au point 2 sont remplies, cela ne devrait pas représenter aucun obstacle à l'utilisation des données de ces personnes à des fins de police, mais les règles de confidentialité doivent être respectées pendant ces échanges.

Exemple - Les données rassemblées à des fins fiscales auprès d'une personne concernée ne peuvent être traitées pour des fins de police que si la loi l'autorise, si elles sont utilisées dans un but légitime et d'une manière nécessaire et proportionnée au but recherché. Dans le cadre concrèt d'une enquête sur le blanchiment d'argent, l'utilisation des données de déclarations fiscales d'un particulier peut être envisagée pour établir ou nier un lien entre l'individu et les opérations de blanchiment d'argent.

4. Traitement portant sur des catégories particulières de données (données sensibles)[49]

Les catégories spéciales de données telles que les données génétiques, les données à caractère personnel concernant des infractions, des procédures et des condamnations pénales et des mesures de sûreté connexes, les données biométriques identifiant de façon unique une personne, une donnée personnelle indiquant l'origine raciale et ethnique, les opinions politiques, l'appartenance à un syndicat, les croyances religieuses ou autres convictions ou donnant des indications sur la santé ou la vie sexuelle ne peuvent être traitées que si la loi l'autorise et que des garanties appropriées ont été mises en place pour aborder des risques potentiels de discrimination ou d'impact juridique défavorable affectant de manière significative les personnes concernées. Les garanties peuvent être de nature technique, par exemple des mesures de sécurité supplémentaires, et de nature organisationnelle, par exemple, des données sensibles traitées séparément de l'environnement de traitement des catégories de données "ordinaires". Les sauvegardes devraient être ajustées à chaque opération de traitement de données en tenant compte de leurs spécificités

[49] Déplacé du point 8 précèdent

Deleted: entreprise pour…une finali…

Comment [A67]: L'obligation est au conditionnel dans le considérations générales.
Prévoir un impératif irait au-delà de la recommandation elle-même (art. 7, ch. 7.2)

Deleted: L… police doit

Deleted: l'…tilisation ultérieure des

Deleted: u…l'affiliation politique de

Deleted: par la police (indépendamment de la finalité initialeu fait que le traitement initial a été mené à des fins policières ou à d'autres fin…

Deleted: Au regard de la nature du traitement, les données à caractère personnel collectées dans le cadre d'une finalité précise peuvent être utilisées dans le cadre d'une autre finalité, les données recueillies à des fins policières ne devraient pas être conservées et traitées d'une façon non structurée, sauf s'il existe un intérêt légitime, une base légale et une justification opérationnelle à cela, dans le cadre des pouvoirs légaux conférés à la police. Cela implique que l…es

Deleted: toutefois …ar ailleurs de

Deleted: devrait être fondée sur des bases légales solides et faire l'objet d'un examen approfondi.¶

Deleted: prises…assemblées à de…

Deleted:

Comment [A68]: Quelle est la signification de cette mesure organisationnelle ? Que veut dire "des données sensibles traitées séparément de l'environnement de traitement des catégories de données "ordinaires""?

et il est fortement recommandé d'utiliser plusieurs niveaux de protection pour ces catégories de données (par exemple : trames principales séparées, périodes de conservation de données plus courtes, etc.). Il est primordial d'empêcher l'accès non autorisé ou indésirable à ces catégories de données, même avec des mesures de sécurité additionnelles.

Un équilibre soigneux des intérêts prenant en compte le but de l'enquête, le contexte et la nature des données est nécessaire pour déterminer si oui ou non et dans quelle mesure la police pourrait traiter des données sensibles. Par exemple, il serait conseillé de différencier lorsque les données biométriques sont traitées par la police, que ce soit à des fins d'identification (quand par exemple, deux empreintes digitales pourraient suffire) ou à des fins d'enquête criminelle (où d'avantages d'empreintes digitales pourraient être nécessaires).

La mise en oeuvre d'évaluations d'impact de la protection des données (DPIA) est recommandée afin de s'assurer que les garanties appropriées sont mises en place. Le responsable du traitement devrait évaluer et démontrer si le but du traitement peut être réalisé d'une manière qui ait le moins d'impact sur le droit à la vie privée et la protection des données et si le traitement de catégories spéciales de données ne représente pas un risque de discrimination pour la personne.

De plus, il convient de rappeler que la collecte et le traitement de données sensibles dans le contexte du profilage sont interdits (Principe 3.11 de la Recommandation 2010(13) sauf si ces données sont nécessaires pour les finalités légitimes et spécifiques du traitement et pour autant que le droit interne prévoit des garanties appropriées. Dans ce contexte, en plus des mesures détaillées ci-dessus, on peut recommander l'utilisation de Privacy-Enhancing Technologies (PET) et de contrôles plus fréquents sur la légalité du traitement. Cela pourrait, par exemple, se traduire par des mesures mises en place pour contrer l'hypothèse que les individus appartiennent à une organisation criminelle en raison de leur lieu de résidence et qu'une organisation criminelle y est active ou où les personnes sont de même origine ethnique.

Exemple : Cibler des groupes ou des individus seulement sur la base de motifs religieux ne devrait pas être autorisé. Cependant, lors d'une enquête sur un groupe de personnes participant éventuellement à des activités terroristes associées à un groupe religieux particulier, il pourrait être important de traiter des données visant spécifiquement les adeptes de ce groupe (liées au lieu de culte, aux prédicateurs religieux, aux coutumes, à l'enseignement, aux membres et à la structure de la communauté religieuse, etc.). Il est néanmoins strictement interdit de cibler tous les adeptes d'une religion, seulement sur la base de leur croyance.

5. Information des personnes concernées

L'une des obligations les plus importantes du responsable du traitement des données est de fournir des informations sur le traitement de leurs données aux personnes concernées. Il s'agit d'une double obligation : 1) le responsable du traitement doit communiquer au public des *informations générales* sur le traitement des données qu'il effectue et 2) il doit donne aux intéressés des informations *spécifiques* sur le traitement de leurs données à caractère personnel si aucunes des restrictions ou dérogations ne s'appliquent à cet égard.

Les informations données au public dans son ensemble devraient permettre de promouvoir sa sensibilisation, de l'informer de ses droits et d'offrir des orientations claires concernant les modalités de leur exercice. Les informations fournies devraient être largement et effectivement accessibles. Par ailleurs, elles devraient également préciser dans quelles conditions les droits des intéressés peuvent faire l'objet d'exceptions et comment ils pourraient former un recours devant l'autorité de contrôle ou un tribunal.

Les sites internet et autres média facilement accessibles jouent un rôle dans l'information du public. Il est recommandé, de mettre des lettres-types à la disposition des personnes concernées qui souhaitent exercer leurs droits. Il est de la responsabilité du responsable du traitement de fournir une information qui met en lumière la protection des données et les droits des personnes concernées.

Deleted: équilibré
Deleted: où,
Deleted: 2
Deleted: d'autres
Deleted: 'utilisation
Deleted: es
Deleted: impacte
Deleted: En ce qui concerne ces données, le risque potentiel de discrimination négative ou d'impact juridique défavorable affectant de manière significative la personne concernée devrait être évité, car tous les profilages basés sur des données sensibles entraînant une discrimination négative sont interdits.
Comment [A69]: Mettre le terme entier avant l'abréviation.
Deleted: s
Deleted: ou
Deleted: que si cela est prescrit par la loi et que des garanties appropriées ont été prévues.. Ces protections peuvent être de nature technique, comme par exemple des mesures de sécurité supplémentaires ou organisationnelle ...
Deleted: religieux
Deleted: sera
Deleted: appartenance
Deleted: religieuse
Deleted: qui en font la demande
Deleted: pas
Deleted: .
Deleted: ¶ ...
Deleted: de façon générale
Deleted: leur
Deleted: es i
Deleted: l
Deleted: eurs
Deleted: d'assurer
Deleted: de manière efficace et large
Deleted: ils
Deleted: Les informations fournies
Deleted: ces personnes
Deleted: peuvent
Deleted: le
Deleted: contre une décision prise, ...
Deleted: tout
Deleted:
Deleted: en guise de bonne pratique,

Afin de respecter la deuxième obligation de fournir aux personnes concernées des informations spécifiques concernant les données traitées, la police doit les informer sur le traitement des données envisagé avant le traitement ou, si cela n'est pas possible, pour des raisons objectives, peu de temps après. Cette communication comprendra des informations sur le traitement des données, la collecte des données des personnes et des informations complètes sur leurs droits.

L'obligation de fournir des informations spécifiques implique que, en principe, les personnes concernées reçoivent des détails tels que le nom et les coordonnées du responsable du traitement de données, le sous-traitant des données, les destinataires , l'ensemble de données à traiter, le but de leur traitement , la base juridique pour le faire et des informations sur leurs droits.

Les informations doivent être fournies à moins qu'une restriction ou une dérogation ne s'applique comme décrit au point 7, en tenant compte de la nature spécifique des fichiers sensibles, tels que les fichiers de renseignements criminels, les fichiers contenant des données sensibles afin d'éviter un préjudice grave à l'exercice des fonctions de la police ou aux droits des individus. Même si des restrictions ou des dérogations au droit à l'information étaient appliquées, des informations devraient être fournies aux personnes concernées dès que cela ne créé plus d'obstacle au but pour lequel leurs données ont été utilisées.

Très souvent, les personnes concernées, en raison de restrictions ou de dérogations à leur droit à l'information, ne peuvent pas recevoir des informations complètes sur le traitement que la police entreprend sur leurs données ; cela ne devrait pas affecter leur exercice du droit d'accès.

Exemple : pour procéder à la surveillance discrète d'un délinquant sexuel à haut risque, il peut être parfaitement justifié de ne pas communiquer à l'intéressé sous surveillance des informations sur le traitement de ses données et leur conservation prolongée si l'on considère que ces informations peuvent nuire à l'enquête en cours ou planifiée. Cependant, une fois que le but de la surveillance secrète est atteint, la personne concernée doit être informée qu'elle ou il a été sujet(te) à une telle mesure.

6. Droits de la personne concernée

L'accès aux données est un droit fondamental reconnu à tout individu car cela lui permet d'être au courant des traitements qui sont effectués sur des données qui le concernent. De plus, cela peut consister en un pré-requis pour l'exercice d'autres droits comme le droit à la rectification et le droit à la suppression.

La police [en principe] doit informer les personnes sur les traitements des données qui les concernent. Cela signifie que, dans le cas où la police collecte des données d'un individu au cours d'une enquête ou pour d'autres tâches policières décrites au point 1, dès que les circonstances l'autorisent en toute sécurité, la police devrait en principe l'informer du traitement des données s'il le demande. L'information devrait être fournie sur demande dès que les données sont traitées, par exemple au moment de la collecte et ce dans des termes clairs et simples. La communication doit contenir les mêmes informations que celles décrites au point 5, à moins que les personnes concernées ne le souhaitent autrement.

La loi peut prévoir, dans les conditions strictes décrites au point 7, que le droit d'être informé sur demande puisse également être limité ou exclu, si cela porte préjudice à l'enquête ou à d'autres tâches importantes de la police, aux intérêts de l'État (comme la sécurité publique, la sécurité nationale) ou la protection des droits et libertés d'autrui. Cependant, le fait de ne pas donner d'informations sur le traitement des données par la police devrait être une exception et pouvoir être clairement justifié.

La police devrait chercher à répondre même aux questions d'ordre général posées par les intéressés sur les activités de traitement de leurs données à caractère personnel, mais elle peut utiliser des formulaires pour faciliter la communication.

Exemple : si une personne concernée demande à la police des informations sur le traitement de ses données à caractères personnel, la police, s'il n'y a pas d'exception applicable, devrait répondre en indiquant les

Deleted: les personnes concernées
Deleted: ,
Deleted: individus
Deleted: ,
Deleted: contrôleur
Deleted: processeur
Deleted: des données
Deleted: u
Deleted: des données
Deleted: de
Deleted: 'elles
Deleted: met
Deleted: tent
Deleted: en péril le
Deleted: avec
Deleted: ses
Deleted: Conformément à la seconde obligation consistant à donner des informations spécifiques relatives à ses données à la personne concernée, sur demande, il appartient au responsab...
Deleted: a
Deleted: de celles-ci,
Deleted: individu s'agissant de ses...
Deleted: Le droit à l'information sur...
Deleted: de
Deleted: d'effacement sont des droi...
Deleted: de la
Deleted: e, comme il est
Deleted: si elle ou il le demande ain...
Deleted: l'individu
Deleted: elles doivent être fournies
Deleted: en langage
Deleted: peut
Deleted: tte dernière
Deleted: É
Deleted: N
Deleted: ,
Deleted: cependant,
Deleted: utilisé comme
Deleted: où il peut
Deleted: Le droit à l'information vis...
Deleted: fournir une réponse,
Deleted: police,
Deleted: citant
Deleted: d

références juridiques pertinentes de façon claire, détaillée, sans utiliser d'expressions peu courantes ou spécialisées.

En principe, le droit d'accès devrait être gratuit.

Il est possible de facturer des frais administratifs raisonnables pour la demande si la législation nationale le prévoit et si la demande est manifestement infondée ou excessive. La police peut également refuser de répondre à de telles demandes manifestement infondées ou excessives, en particulier lorsque leur caractère répétitif le justifie.

Pour que l'exercice du droit d'accès soit équitable, la communication « sous une forme intelligible » s'applique aussi bien au contenu qu'à la forme d'une communication numérique standardisée.

S'il s'agit d'un accès direct, la personne concernée peut demander un accès au responsable du traitement. Après avoir évalué la demande et l'application de toute restriction ou dérogation éventuelle qui ne pourraient être appliquée que dans la mesure où elle serait indispensable pour l'accomplissement d'une tâche légale de la police comme prévu au point 1 ou serait nécessaire pour la protection de la personne concernée ou des droits et libertés d'autrui, le responsable du traitement répond directement à la personne concernée. Dans le cas d'une restriction ou d'une information partielle et dans le cas d'une dérogation la personne concernée doit tout de même recevoir une information sur l'application de la dérogation assortie des motifs de telles mesures, et ce dans les deux cas, ainsi qu'une informa tion sur ses voies de recours.

Exemple : la demande d'accès peut être refusée si une enquête est en cours sur la personne concernée et si lui permettre d'accéder aux données risque de compromettre l'enquête.

Si une restriction ou une dérogation devait être utilisée, toute réponse devrait tenir compte, conformément à la législation ou à la pratique nationales, de toutes les circonstances pour lesquelles la restriction ou la dérogation est applicable.

En règle générale, le droit interne devrait idéalement prévoir un accès direct. Si le droit d'accès prévu est indirect, la personne concernée peut adresser sa demande à l'autorité de contrôle, qui, après avoir été dûment mandatée, traitera la demande en son nom et procédera à des vérifications sur la disponibilité et la licéité du traitement de ses données à caractère personnel. L'autorité de contrôle répondra ensuite à la personne concernée (à condition que les données puissent être diffusées, sous réserve des restrictions ou dérogations autorisées légalement). Dans le cas d'une restriction ou d'une dérogation, la même communication que celle applicable à l'accès direct devrait être rendue possible.

Le responsable du traitement des données devrait évaluer la demande et répondre à la personne concernée dans le délai raisonnable prévu par le droit interne.

Les dispositions en vigueur devraient prévoir le moyen de confirmer l'identité de la personne concernée et d'obtenir des informations sur les activités de traitement auxquelles la demande se réfère avant toute autorisation d'accès aux données. Il doit en être de même si la personne concernée délègue à un tiers la faculté d'exercer ses droits.

Le droit d'une personne concernée de pouvoir modifier toute donnée inexacte détenue à son sujet est un droit essentiel. Une personne concernée qui découvre des données inexactes ou non pertinentes devrait avoir le droit de les contester et de veiller à ce qu'elles soient rectifiées.

Dans certains cas, il peut être utile d'ajouter au fichier des informations supplémentaires ou rectificatives. Il est important de souligner que ce droit peut seulement être exercé dans le respect des droits des autres personnes, par exemple, des droits relatifs des témoins dans un procès pénal (ce qui n'empêche pas en soi l'exercice des droits des personnes concernées par rapport à des données de police subjectives).
Si les données à corriger ou à effacer ont été communiquées à des tiers, il appartient aux autorités compétentes d'informer ces derniers des modifications à apporter.

Deleted: ant…d'es …xpressions ...

Deleted: L'accès aux données est un droit fondamental reconnu à tout individu s'agissant de ses données à caractère personnel. Dans l'idéal, le droit interne devrait prévoir, en règle générale, un droit d'accès direct. ¶

Deleted: L… droit d'accès (comme ...

Deleted: que…la demande est ...

Deleted: Il est toutefois conseillé de se référer à la législation nationale pour assurer la cohérence et pour éviter que les suspects utilisent cette méthode pour savoir s'il existe une enquête en cours sur eux.¶

Deleted: l'…ccès au responsable du ...

Deleted: avoir une réponse sur le recours à la dérogation ainsi que sur le motif d'une telle mesure tout en l'informant sur des voies de recours. , quoique la réponse doive prendre en considération selon le droit national ou la pratique établie toutes les circonstances selon lesquelles la dérogation est appliquée.¶

Deleted: que …i lui permettre ...

Deleted: avait été …pplicablequé. ...

Deleted: ¶ ...

Deleted: Il faudrait que l…es ...

Deleted: La …ne personne concern ...

Deleted: . ¶

Toutes les modifications proposées devraient être étayées par des éléments de preuve. Si les personnes concernées peuvent prouver au moyen de documents officiels que les données traitées par la police à leur égard sont incorrectes, le responsable du traitement n'aura pas la liberté de décider s'il faut les rectifier ou les supprimer.

Conformément à ce qui est prévu au point 7, la police peut avoir besoin de ne pas donner d'informations ou de droit d'accès, de suppression ou de correction qui pourrait compromettre une enquête. La divulgation de ces données devrait donc être exclue pendant toute la durée de l'enquête. Des restrictions ou de dérogations similaires peuvent être prescrites par la loi nationale comme décrit au point 7.

Les restrictions ou dérogations imposées aux droits de la personne concernée ne devraient s'appliquer que dans la mesure où elles sont nécessaires et faire l'objet d'une interprétation restreinte. Chaque demande de la part des personnes concernées devrait être évaluée soigneusement, au cas par cas. Tout refus de donner suite à la demande d'une personne concernée devrait être communiqué par écrit (y compris par des moyens électroniques). La réponse devrait indiquer clairement les motifs de la décision qui pourront être vérifiés par une autorité indépendante ou un juge. Il peut arriver que le fait de communiquer les motifs d'un refus présente un risque pour la police, pour la personne concernée ou pour les droits et libertés d'autrui. En pareil cas, il importe que le refus soit transmis, documents à l'appui, à l'autorité indépendante ou au juge qui vérifiera si nécessaire son bien-fondé.

Exemple : si une personne A a fait une déclaration au sujet d'une personne B l'accusant d'avoir commis une grave infraction et qu'il s'avère par la suite que cette accusation était fausse, les services de police peuvent juger utile de conserver cette fausse déclaration et les informations qu'elle comprenait.

Bien que la déclaration se soit avérée fausse, si la police exige la conservation des données, une déclaration corrective claire serait nécessaire dans le dossier faute de supprimer la fausse déclaration.

Il convient d'informer la personne concernée de toutes les possibilités dont elle dispose en cas de refus, comme le dépôt d'un recours auprès de l'autorité de contrôle, d'un tribunal ou d'une autre autorité administrative indépendante La communication effective de l'issue de cet examen ou du recours peut varier en fonction de la législation nationale et de l'existence d'un droit d'accès direct ou indirect. Il peut arriver que l'autorité de contrôle ne puisse pas communiquer les données à la personne concernée, même si rien ne justifie qu'elle ne puisse y accéder. Dans ce cas, la personne concernée devrait être informée du fait que le fichier de police a fait l'objet d'une vérification. À défaut, l'autorité de contrôle peut décider de demander à la police de communiquer les données du fichier à la personne concernée. En outre, une cour ou un tribunal peut avoir le pouvoir d'ordonner l'accès aux données du fichier, leur rectification ou leur suppression, même dans le cas où une demande d'accès lui à été transmise par la police ou l'autorité de contrôle.

Exemple : une lettre de refus envoyée par la police doit contenir le nom, l'adresse, l'adresse internet, etc. de toutes les formes de recours possibles.

Si elle n'est pas satisfaite d'une réponse donnée par l'autorité de contrôle ou par l'autorité indépendante, la personne concernée devrait avoir la possibilité de saisir une cour ou un tribunal afin de contester la décision et de faire examiner les motifs du refus. L'autorité de contrôle devrait disposer de pouvoirs suffisants pour examiner le fichier de police concerné et pour recevoir l'appréciation de la demande d'accès.

7. Exceptions à l'application des principes de protection des données

Conformément à la Convention européenne des droits de l'homme et à la Convention 108, les exceptions ne peuvent être utilisées que si elles sont prévues par la loi (celle-ci doit être publique, ouverte, transparente ainsi que suffisamment détaillée) et constituent une mesure nécessaire et proportionnée dans une société démocratique.
Les exceptions qui doivent être intégrées au droit national devraient répondre à un objectif clairement déini. Des exceptions peuvent être applicables aux principes décrits aux points 2, 3 et 5 ainsi qu'aux droits des

Deleted: du même pays
Deleted: L
Deleted: , conformément à ce qui est prévu au point 57,
Deleted: ne pas accorder un
Deleted: ,
Deleted: R
Deleted: une
Deleted: La personne concernée peut être amenée, selon la législation nationale, à obtenir une copie de son dossier. Or la fourniture d'une copie ou d'une communication écrite n'est peut-être pas dans son intérêt ou faisable par la police; dans ce cas, le droit interne peut autoriser la communication orale du contenu demandé.¶
Deleted: ¶
Deleted: ait été prouvée
Deleted: sur le dossier,
Deleted: au lieu d'enlever la fausse déclaration,
Deleted: ¶
Au lieu de supprimer la déclaration dont la fausseté a été démontrée, ils peuvent ajouter au fichier concerné une déclaration rectificative claire.
Deleted: soit
Deleted: toujours obligée de
Deleted: s'oppose
Deleted: à ce
Deleted: la juridiction compétente
Deleted: . ¶
Deleted: instances
Deleted: À chaque fois
Deleted: qu'
Deleted: L'issue de cet examen ou du recours peut varier en fonction de la législation nationale et de l'existence d'un droit d'accès direct ou indirect. Il peut arriver que l'autorité de contrôle ne soit pas toujours obligée de communiquer les données à la personne concernée, même si rien ne s'oppose à ce qu'elle puisse y accéder. Dans ce cas, la personne concernée devrait être informée du fait que le ...
Deleted: ¶
Deleted: elle
Deleted: et
Deleted: de manière compatible ave ...
Deleted: L
Deleted: ,
Deleted: 4, 7

personnes concernées (point 6) dans le cas de certains objectifs spécifiques en relation desquels des activités de traitement de données sont entreprises. Il s'agit en particulier d'activités menées dans le but d'assurer la sécurité nationale, la défense, la sûreté publique, la protection d'intérêts économiques et financiers importants, l'impartialité et l'indépendance de la justice, la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales ou d'autres objectifs essentiels d'intérêt général (qui inclut des objectifs liés au respect d'engagements ou d'obligation internationaux de l'État, principalement découlant de décisions contraignantes d'organes des Nations Unies ou des objectifs humanitaires) ou la protection des droits et libertés fondamentales d'autrui.

Exemple : si le fait de donner des informations à une personne concernée peut mettre en danger la sécurité d'un témoin ou d'un informateur, ce droit peut être limité dans de telles circonstances.

Si une exception telle qu'elle est définie par le droit national qui prévoit des garanties spécifiques est utilisée par la police, elle doit l'être pour des finalités légitimes et seulement dans la mesure où elle est nécessaire et proportionnée pour atteindre la finalité pour laquelle elle a été utilisée. Le but dans lesquel la police utilise ces exceptions devraient être limitées aux cas où ces règles et principes risqueraient de mettre en danger les tâches de police décrites au Point 1.

Exemple : si des données collectées dans des buts policiers dans le cadre d'une enquête sont susceptibles de servir des objectifs de sécurité nationale, elles peuvent également être utilisées pour ce dernier objectif dans la mesure prévue par la législation nationale. Si des renseignements particuliers prouvent que des opérations de blanchiment d'argent ont été menées pour financer des activités terroristes, les données collectées sur des individus au cours des enquêtes sur le blanchiment d'argent peuvent être utilisées pour éliminer le risque probable et imminent d'acte terroriste.

8. Utilisation de techniques d'enquête spéciales

La police devrait toujours choisir les moyens les moins intrusifs de traitement de données durant ses opérations. Si des mesures moins intrusives pour aboutir au but recherché existent, elles doivent être privilégiées. L'emploi de techniques spéciales d'enquête ne peut être envisagé que si le même résultat ne peut être obtenu par des méthodes moins intrusives. Quelles que soient les méthodes d'enquête ou d'autres opérations menées par la police, celle-ci a l'obligation de se conformer aux principes généraux relatifs à la protection des données à caractère personnel décrits dans les Considérations générales, sauf dans les cas où la législation l'en dispense explicitement.

Les progrès techniques ont rendu la surveillance électronique plus facile, mais il ne faut pas oublier que leur utilisation peut constituer une ingérence dans les droits et libertés fondamentales, en particulier dans le droit au respect de la vie privée. Le choix de la méthode d'enquête doit donc s'accompagner d'une mise en balance du potentiel de risque élevé d'ingérence grave dans le droit à la protection de la vie privé avec l'efficacité de l'enquête.

Exemple : dans une enquête, les preuves de la communication entre deux suspects peuvent être recueillies de diverses façons. Si des interrogatoires, des témoignages, l'obtention des données d'appels téléphoniques ou une surveillance discrète permettent d'obtenir le même résultat sans nuire à l'efficacité de l'enquête, ces moyens doivent être préférés à l'utilisation de mesures de surveillance plus intrusives telles que les écoutes.

9. Introduction de nouvelles technologies de traitement des données

Si l'introduction de nouvelles technologies risque fortement susceptible de porter atteinte aux droits de l'intéressé(e), il appartient au responsable du traitement des données de procéder à une évaluation de l'impact sur la protection des données (EIPD), afin d'apprécier l'ensemble des risques que ce traitement présente au regard des actions envisagées. Il est recommandé que l'évaluation des risques ne soit pas statique mais qu'elle prenne en compte le cas spécifique, qu'elle soit répétée à des intervalles raisonnables, et qu'elle concerne les étapes pertinentes de l'activité de traitement des données. La pertinence de l'EIPD doit être contrôlée à intervalles raisonnables.

En terme de sécurité des données et des communications, il est aussi très important que les normes les plus élevées soient prises en compte au moment d'introduire les nouvelles technologies.

Deleted: 17
Deleted: e
Deleted: activités
Deleted:
Deleted: .
Deleted: principalement
Deleted: es
Deleted: L'article 3 de la Convention 108 prévoit que d'autres exceptions puissent être applicables.
Deleted: ¶
Deleted: , fondée sur
Deleted: ,
Deleted: s finalités
Deleted: les
Deleted: c
Deleted: sont utilisées
Deleted: la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales ou d'autres fins policières.
Deleted: Exemple : si le fait de donner des informations à une personne concernée peut mettre en danger la sécurité d'un témoin ou d'un informateur, ce droit peut être limité dans de telles circonstances.¶
Deleted: policières peuvent être échangées avec des services de sécurité nationale par exemple pour déjouer un attentat terroriste. Afin d'identifier rapidement l'auteur de l'attentat, la police doit coopérer ...
Deleted: Dans le cas où
Deleted:
Deleted: elle peut employer des ...
Deleted: les
Deleted: er
Deleted:
Deleted: réflexion sur
Deleted: des éléments tels que le ...
Deleted: secrète, telles que l
Deleted: l'information
Deleted: Lorsque de nouveaux ...
Deleted: le traitement est
Comment [A70]: Le caractère ...
Deleted: ,
Deleted: continue (c'est-à-dire ...
Deleted:),
Deleted: vise chacune d

Exemple : les nouvelles techniques de *data mining* peuvent offrir des possibilités étendues pour l'identification d'éventuels suspects et il convient d'évaluer soigneusement leur conformité avec la législation en vigueur en matière de protection des données, y compris en ce qui concerne la sécurité des données.

L'autorité de protection des données a un rôle important à jouer ; elle doit signaler les risques que ce traitement automatisé présente pour la protection des données et présenter les garanties à mettre en place pour que tous les moyens techniques soient conformes à la législation sur la protection des données. Cependant, la police n'est pas tenue de s'adresser à l'autorité de contrôle à chaque fois qu'elle met en place de nouvelles technologies. Elle peut le faire si l'EIPD a démontré l'existence d'un risque élevé d'atteinte aux droits de l'intéressé.

Les consultations entre l'autorité de contrôle et le responsable du traitement des données devraient avoir lieu dans un cadre qui permet suffisamment à cette autorité de donner un avis motivé et une évaluation des activités du responsable du traitement des données sans compromettre ses fonctions essentielles.

Des renseignements appropriés devraient être fournis à l'autorité de protection des données, notamment en ce qui concerne le type de fichier, le responsable du traitement des données, le sous-traitant, la base légale et la finalité du traitement des données, le type de données traitées et qui y a accès. Il faut également fournir des informations sur la conservation des données et la politique applicable en matière d'enregistrement et d'accès ainsi que sur tous les aspects techniques de mise en oeuvre.

Exemple : les informations détaillées sur les fichiers nationaux de référence telles que la finalité ou le responsable du traitement des données, etc qui contiennent des données sur les empreintes digitales devraient être indiquées ou mise à disposition de l'autorité de protection des données pour consultation.

À l'issue de ces consultations, le responsable du traitement devrait soigneusement les examiner afin de mettre en œuvre les mesures et les garanties nécessaires recommandées par l'autorité de protection des données.

Exemple : la mise en place d'un système de reconnaissance faciale automatique ou tout autre système basé sur le traitement automatisé de données biométriques devrait très probablement nécessiter une consultation pour que les risques encourus par les droits de l'intéressé soient clairement définis. S'il le faut et si cela est recommandé par l'autorité de protection des données consultée sur la question, des garanties spécifiques devraient être mises en place (concernant la durée de conservation des données, les fonctionnalités de correspondance croisée, le lieu de stockage des données et les problèmes d'accès aux données, etc.) pour se conformer aux principes et dispositions de la protection des données.

Utilisation de l'internet des objets dans le travail de police

Les données transmises à la police et à ses agents ou par ceux-ci dans le cadre de leurs activités opérationnelles par internet montrent que la technologie de l'internet des objets est déjà opérationnelle. En raison des vulnérabilités qu'elle peut présenter en matière de sécurité, cette technologie exige des mesures telles que l'authentification des données, le contrôle de l'accès pour assurer la sécurité des données et la protection des données pour résister aux cyber-attaques.

Exemple : compte tenu de possibles problèmes de sécurité, les « lunettes intelligentes » utilisées par la police ne doivent pas être directement connectées à une base de données nationale des casiers judiciaires. Il convient de garantir aux données collectées le plus haut niveau de sécurité.

Analyse des big data dans les services de police

Les avancées technologiques dans le domaine du traitement et de l'analyse d'ensembles de données importants et complexes qui donnent lieu à la création de mégadonnées (*big data*), ainsi que l'analyse de ces mégadonnées présentent aussi bien des occasions à saisir que des défis à relever pour les services de

Deleted: .

Deleted: Au cours de la procédure d'échange avec l'autorité de contrôle, l'accent devrait être mis sur l'atténuation des effets négatifs spécifiques que le traitement des données pourrait produire sur le droit à protection de la vie privée et le droit à la protection des données.¶
¶
Les consultations entre l'autorité de contrôle et le responsable du traitement des données devraient avoir lieu dans un cadre qui permet suffisamment à cette autorité de donner un avis motivé et une évaluation des activités du responsable du traitement des données sans compromettre ses fonctions essentielles. ¶
¶
Il convient, pendant le processus de consultation, de communiquer d

Deleted: qui figurent dans le fichier

Deleted: les destinataires des données.

Deleted: toutes

Deleted: telles que la finalité ou le responsable du traitement des données, etc.

Deleted: Il est préférable de consulter l'autorité de protection des données durant la procédure législative.

Deleted: devrait faire l'objet de

Deleted: s

Deleted: indiqués

Deleted: de prendre

Deleted: , directement reliées aux bases de données pertinentes,

Deleted: liées

Deleted: ; elles devraient recueillir des informations qui seront ensuite téléchargées dans un environnement informatique sécurisé pour analyses ultérieures.

Deleted: ¶
¶
¶
¶

Deleted: *B*

Deleted: *et profilage*

police qui décident d'utiliser des sources d'information numériques et des techniques de profilage pour accomplir leur tâches.

Les technologies du big data permettent la collecte et l'analyse d'une quantité massive de données générées par les communications et les dispositifs électroniques qui s'ajoutent à d'autres données de masse. Ce mode de traitement des données pourrait interférer avec le droit au respect de la vie privée et à la protection des données.
La Recommandation CM/Rec(2010)13 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage[51] et les Lignes directrices du Conseil de l'Europe sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées[52] peuvent être également utiles dans le contexte de l'analyse de ces masses de données par la police.
Les technologies du big data et les techniques d'analyse de ces données peuvent contribuer à la détection d'une infraction, mais il est toutefois important de tenir compte des risques considérables que présente cette forme de traitement de données :

- l'interprétation d'informations provenant de bases de données utilisées dans des domaines et contextes différents peut aboutir à des conclusions erronées et à des manques de base légales valides et de ce fait conduire à des traitement de données illégales qui peuvent avoir de graves conséquences pour les intéressés ;
- le profilage peut déboucher sur des conclusions discriminatoires susceptibles de renforcer les préjugés, la stigmatisation et la discrimination ;
- la quantité croissante de données détenues dans des bases de données peut entrainer une grave vulnérabilité et par conséquent des risques de violation des données si la sécurité de ces informations n'est pas garantie.

Lorsque le traitement de big data s'appuie sur des données à caractère personnel, le responsable du traitement des données devrait porter une attention particulière aux exigences suivantes :

- la vérification de l'exactitude, du contexte et de la pertinence des données ;
- leur utilisation exige une forte obligation de rendre des comptes ;
- leur utilisation doit être combinée avec des méthodes d'enquête qui complètent des conclusions tirées de l'analyse des mégadonnées. Une décision qui affecte une personne ne doit pas être prise sur la seule base d'un traitement automatisé de données personnelles mais doit impliquer une intervention humaine ;
- en ce qui concerne d'autres types de traitement des données, il est fondamentalement important que leur utilisation soit nécessaire et proportionnée à l'accomplissement des tâches policières décrites au Point 1, avec une attention particulière à ce que les données ainsi traitées soient correctes, pertinentes et ne soient pas excessives par rapport au but poursuivi ;
- toute analyse prédictive nécessite notamment une intervention humaine pour évaluer sa pertinence et les conclusions tirées ;
- les lignes directrices en matière d'éthique élaborées au niveau national ou international devraient être prises en considération ;
- comme principe et sous réserve des restrictions et dérogations mentionnées au Point 7, le responsable du traitement doit faire preuve de transparence et expliquer comment les données sont traitées dans le respect des principes applicables à la protection des données. Lorsque les données collectées dans un but précis sont utilisées dans un autre but, il devrait normalement en informer les personnes concernées ;
- même dans le cas d'une utilisation de méthodes complexes, la légalité du traitement des données – y compris une utilisation secondaire - et sa conformité avec les conditions fixées par l'article 8 de la Convention européenne des droits de l'homme devraient être démontrées ;
- il importe de mettre en place et d'appliquer une politique de sécurité des informations tout au long du traitement ;
- les responsables du traitement devraient veiller à la loyauté du traitement des données à caractère personnel lorsque des big data servent de base à la prise de décisions qui ont des conséquences pour des individus et s'assurer que les voies administratives et judiciaires permettant de contester ces

[51] Recommandation CM/Rec(2010)13 du Conseil de l'Europe sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage
[52] Document T-PD(2017)1 – Lignes directrices

Deleted: mission judiciaire
Deleted: potentiellement ou involontairement
Deleted: Les lignes directrices
Deleted: sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des mégadonnées[50]
Deleted:
Deleted: ,
Deleted: sévère
Deleted: ¶
Deleted: tenir dûment compte des
Deleted: considérations
Deleted: s'impose
Deleted: l
Deleted: traditionnelles
Deleted: ..;
Comment [A71]: Cela concorde plus avec la directive 680/2016 (art. 11)
Deleted: ;
Deleted: <#>¶
Deleted: est
Deleted: aux fins
Deleted: l'
Deleted: l
Deleted: de l'analyse
Deleted: d
Deleted: si possible, faire
Deleted: compatible
Deleted: i
Deleted: e
Deleted: mporte que l'organe responsable du traitement i
Deleted: de cette utilisation secondaire
Deleted: oit
Deleted: 'il
Deleted: l
Deleted: intéressés
Deleted: doit
Deleted: l

décisions existent. Cela implique que les personnes intéressées soient informées du mode opératoire des algorithmes utilisés ainsi que du but de leur utilisation de manière compréhensible.

Les exigences mentionnées ci-dessus sont plus que jamais nécessaires quand des données sensibles sont traitées dans le cadre d'analyses de mégadonnées, en particulier eu égard à l'intervention humaine et la combinaison de méthodes d'analyses nouvelles et traditionnelles.

10. Conservation des données

Comme énoncé au point 2, les données sont traitées tant qu'elles servent les fins pour lesquelles elles ont été collectées. Les données conservées devraient être adéquates, actualisées, nécessaires, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées.

Le classement et le traitement des données à caractère personnel par la police devrait suivre une distinction claire entre les différentes catégories de personnes, par exemple les suspects, les personnes condamnées pour une infraction pénale, les victimes et les tiers tel que les témoins. Cette distinction devrait également tenir compte de la finalité précise des données collectées. Des garanties supplémentaires devraient être prévues pour les personnes qui ne sont pas soupçonnées d'infraction pénale ou qui n'ont pas été condamnées pour une infraction pénale. Des règles claires doivent être mises en place en ce qui concerne le traitement des différentes bases de données, avec une attention particuière portée à l'analyse des résultats multiples.

Le principe de nécessité doit être appliqué tout au long du cycle de vie du traitement. Le stockage peut être autorisé si l'analyse montre que les données à caractère personnel sont nécessaires pour atteindre l'objectif de prévention, d'enquête et de répression des infractions pénales et de l'exécution des sanctions pénales et lorsque les données à caractère personnel sont traitées dans le but du maintien de l'ordre public.

Les motifs de conservation et de traitement des données devraient être réexaminés périodiquement. Il est à noter que le traitement ilicité des données à caractère personnel en dehors du délai légal prévu pour la conservation constitue une violation grave du droit à la protection de ces données. Si la loi relative à un crime spécifique prévoit une période de 4 ans de rétention des données, et si un individu est détenu par la police seulement sur la base de ces données, 4 ans plus tard la preuve - fondée uniquement sur ces données - peut potentiellement être considérée comme illégale par la Cour.

Les périodes de conservation des données sont généralement réglementées dans le droit interne ou international. Pour être en conformité avec la législation tout en veillant à l'efficacité et à l'aboutissement d'une enquête, il est fortement recommandé aux services de police d'élaborer des procédures internes et/ou des recommandations sur la fixation de la durée de conservation et sur le réexamen régulier de la nécessité de conservation des données à caractère personnel.

Par exemple, si la loi prescrit une durée de conservation des données de 4 ans mais que la personne ayant fait l'objet d'une enquête est acquittée au bout de 2 ans de toutes charges, ses données devront être effacées de la base de données (si elle n'est pas récidiviste ou si aucune autre information n'indique qu'elle a de nouveau commis un crime de la même catégorie), pourvu aussi que tous les délais de révision de l'affaire aient également expiré. De même, si l'enquête est toujours en cours après 4 ans et que les données concernant cette personne restent pertinentes, la police devrait être en mesure de les conserver.

Dans ce dernier cas, il semble important d'élaborer la stratégie de conservation de telle sorte que les données utilisées dans les poursuites pénales restent à la disposition du responsable de traitement jusqu'à la

Deleted: .

Deleted: <#>Traitement portant sur des catégories particulières de données (données sensibles) ¶
¶
Les catégories spéciales de données telles que les données génétiques, les données à caractère personnel concernant des infractions, des procédures et des condamnations pénales et des mesures de sûreté connexes, les données biométriques identifiant une personne, une donnée personnelle indiquant l'origine raciale et ethnique, les opinions politiques, l'appartenance à un syndicat, les croyances religieuses ou autres convictions ou donnant des indications sur la santé ou la vie sexuelle ne peuvent être traitées que si cela est prescrit par la loi et que des garanties appropriées ont été prévues.. Ces protections peuvent être de nature technique, comme par exemple des mesures de sécurité supplémentaires ou organisationnelle, tel que la mise en place d'un traitement de ces données à part et non dans l'environnement de traitement prévu pour les catégories de données « normales ».Les données sensibles peuvent néanmoins être traitées afin de protéger la vie de la personne concernée ou celle d'une autre personne.¶
¶ ...

Deleted: Les données qui ne sont plus pertinentes de ce point de vue doive ...

Deleted: Il convient de mettre en place d

Deleted: ¶

Deleted: peut

Deleted: r

Deleted: et que les éléments de preuve recueillis ainsi peuvent être ...

Deleted: comme période de

Deleted: l

Deleted: '

Deleted: retenu

Deleted: le fondement

Deleted: les

Deleted: qui pèsent contre elle

Deleted:

Deleted: sont

Deleted: 'il

Deleted: s'avère qu'

Deleted: au terme des

Deleted: l'enquête est toujours en cours

fin de la procédure judiciaire (c'est-à-dire que toutes les voies de recours ont été épuisées ou tous les délais de recours sont expirés).

La police devrait prévoir des systèmes et des mécanismes pour veiller à ce que les données enregistrées soient exactes et que leur intégrité soit préservée.

Les obligations internationales qui imposent la transmission de données à des organes internationaux comme Europol, Eurojust et INTERPOL, ainsi que les accords bilatéraux et l'entraide judiciaire entre États membres et pays tiers, doivent être respectées au stade de l'élaboration des politiques internes.

Les données devraient être classées par catégorie en fonction de leur degré d'exactitude et de fiabilité afin d'aider la police dans ses activités. Il est recommandé d'utiliser des codes de traitement pour différencier ces catégories. L'utilisation d'un système de classification permet de faciliter l'appréciation de la qualité et de la fiabilité des données. La classification des données est également importante lorsqu'elles doivent être communiquées à d'autres services de police ou à d'autres États.

Exemple : les informations directement tirées des déclarations d'une personne seront évaluées différemment des informations collectées par ouï-dire ; les données factuelles, ou données objectives, seront appréciées différemment des données qui se fondent sur des appréciations ou des avis personnels, ou données subjectives.

Les données à caractère personnel collectées par la police à des fins administratives doivent être séparées (autant que possible logiquement et physiquement) des données collectées à des fins policières. La police peut y accéder lorsque c'est nécessaire et autorisé par la loi.

Parmi les données administratives figurent, par exemple, les listes de données relatives aux titulaires de licences ou les données relatives aux ressources humaines et aux permis de port d'arme.

11. Communication de données au sein de la police

Il convient de faire la distinction entre la communication de données sur le plan national et le transfert international de données. Il s'agit en effet d'opérations distinctes soumises à des obligations différentes en fonction du destinataire des données : la police, un autre organe public ou un tiers privé. La communication de données entre services de police ne peut être permise que s'il existe un intérêt légitime pour cette communication dans le cadre des attributions légales de ces services.
Des règles claires et transparentes devraient définir le motif et la façon dont la police accède aux données qu'elle détient.
Les autorités policières nationales ne devraient échanger leurs informations que dans le cadre d'une demande prévue par la loi, par exemple en cas d'enquête judiciaire en cours ou de mission de police conjointe et dans le cadre d'une loi ou d'accords l'autorisant.
La police peut communiquer des données à d'autres services de police si les données à caractère personnel sont nécessaires aux fins de prévention, d'enquête et de répression des infractions pénales et d'exécution des sanctions pénales et lorsque les données à caractère personnel sont traitées dans le but du maintien de l'ordre public.
En général, la communication de données à caractère personnel doit être conforme aux considérations générales décrites ci-dessus.

Exemple : un service de police peut communiquer des données sur une personne soupçonnée de fraude fiscale à un autre service de police qui enquête sur une affaire de meurtre si des éléments indiquent que le suspect de ce crime pourrait être la même personne ou si cette communication pourrait matériellement aider l'enquête.

12. Communication de données par des services de police à d'autres organismes publics

La communication de données en dehors de la police est autorisée si cela est prévu par la loi et si ces données sont indispensables au destinataire pour accomplir la tâche licite qui lui incombe. Des accords d'entraide mutuelle prévus par la loi entre les services chargés de l'application de la loi et des organes publics permettent à ces derniers d'avoir accès à des données policières essentielles à leurs fonctions et tâches (par exemple dans leurs enquêtes ou d'autres attributions légales conformes au droit interne).

Deleted: ce que
Deleted: s'achève
Deleted: Lors de l'élaboration de politiques internes, l
Deleted: É
Comment [A72]: Qu'est-ce que cela signifie ? S'agit-il d'une émanation du principe de privacy by design? C'est peu clair.
Deleted: .
Deleted: Il convient de classer l
Deleted:
Deleted: si faisable ;
Deleted: ¶ ¶
Deleted: En général,
Deleted: l
Deleted: devrait
Deleted: communiquer
Deleted: lorsque la
Deleted: qui leur en est faite est
Deleted: qui
Deleted: e
Deleted: la communication
Deleted: soumise au principe de nécessité et de proportionnalité et servir aux fins sus
Deleted: mentionnées
Deleted: aux autorités publiques

Des principes plus stricts que ceux prévus au point 11 devraient être respectés lorsque des données doivent être transmises à d'autres organismes nationaux que des services de police, car il y a un risque que le traitement de données à caractère personnel considérées sensibles puisse avoir des conséquences dommageables à la personne concernée.

La communication de données à une autre autorité publique peut également être autorisée si elle est prévue par la loi, dans l'intérêt incontestable de la personne concernée, ou si elle est nécessaire pour éviter un risque grave et imminent pour d'autres personnes, pour l'ordre public ou la sécurité publique.

Les données communiquées ne peuvent être utilisées par l'organe destinataire qu'aux fins pour lesquelles elles ont été transmises.

Exemple : demande de permis de séjour faite par un migrant. Des données policières peuvent être nécessaires pour vérifier si la personne a été impliquée dans des activités criminelles. Il serait dans l'intérêt de l'office de l'immigration et du demandeur que cette communication de données ait lieu.

13. Communication de données par la police à des organismes privés

Il peut arriver que, dans des conditions strictes, la police puisse communiquer des données à des organismes privés. Cette communication doit être prévue par la loi et être effectuée uniquement par l'autorité qui traite les données. Cela ne devrait être effectuée qu'aux fins d'une enquête ou d'autres missions importantes de la police telles que décrites au point 1, dans l'intérêt de la personne concernée, pour des raisons humanitaires ou s'il est nécessaire d'éviter un risque grave et imminent, pour l'ordre ou la sécurité publics. Par exemple il devrait aussi y avoir des cas dans lesquels la police serait autorisée à communiquer des données à des organisations humanitaires sur le fondement du droit international, dans l'intérêt de la personne concernée ou pour des raisons humanitaires.

Lorsque la police communique des données aux médias afin de rendre publique des informations liées à une enquête, il importerait d'évaluer si cela est nécessaire et dans l'intérêt public qu'une telle publicité soit permise.

Cette communication ne devrait avoir lieu qu'au cas par cas, être chaque fois clairement prévue par la loi stipulant la procédure nécessaire à suivre pour une telle communication (notamment la nécessité d'une autorisation spécifique).

Exemple : lorsque la police communique avec le secteur financier à propos de délinquants coupables de fraude ou de vol, lorsqu'elle communique avec une compagnie aérienne au sujet de documents de voyage volés ou perdus ou quand elle divulgue des informations sur une personne recherchée qui est supposée constituer un risque pour la population.

14. Transfert international

Tout transfert international de données de police devrait être limité à d'autres services de police, être adapté au but poursuivi et prévu par la loi. A cet effet, un certain nombre d'instruments juridiques internationaux multilatéraux peuvent être utiles, tels que la Convention 108 et la Constitution d'Interpol et ses documents annexes concernant le traitement des données, des cadres juridiques régionaux tels que la législation de l'UE et des institutions de l'UE (sur Europol, Eurojust, Frontex, etc.) et des accords ultérieurs (accords bilatéraux opérationnels), des traités bilatéraux et en général des accords internationaux sur l'entraide, voire d'autres accords bilatéraux ou multilatéraux concernant la coopération effective.

Lorsqu'il est envisagé de partager des données, il conviendrait de vérifier si l'autorité destinataire a légalement une fonction qui vise la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales et le maintien de l'ordre public et si la communication de données lui est nécessaire pour exercer ses fonctions.

Deleted: 0
Deleted: sont
Deleted: a communication
Deleted: ces données pourrait servir à d'autres fins qu'a des fins policières
Deleted: A titre d'exception, l
Deleted: si elle effectuée
Deleted: ou
Deleted: O
Deleted: ait besoin de
Deleted: ,
Deleted:
Deleted: type de communication
Deleted: e l'
Deleted: ,
Deleted: des données aux médias qui diffusent des informations liées à une enquête publique,
Deleted: qui devrait établir
Deleted: (notamment la nécessité d'une autorisation spécifique)
Deleted: qu'
Deleted: puisse se produire
Deleted: Dans ce cadre
Deleted: concernant
Deleted: communiquer
Deleted: ,

L'autorité expéditrice doit veiller à ce que l'État destinataire dispose d'un niveau suffisant de protection des données et se conforme aux dispositions pertinentes en matière de communication internationale des données à caractère personnel. Elle doit notamment prévoir des garanties appropriées en matière de protection des données au cas où il n'y aurait aucune disposition légale nationale pertinente ni aucun accord international dans ce domaine. Ce mode de transfert ne devrait être utilisé qu'en dernier ressort. Des cadres de transferts internationaux tels que le « Règlement gouvernant le traitement des données » et les « Règles sur le contrôle de l'information et l'accès aux fichiers Interpol (RCI)» , ainsi que des dispositions de la Convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 et de la Convention sur la cybercriminalité (STE n° 185) peuvent être prises en compte[53] pour veiller à ce que tout transfert de données soit légalement justifié et soit encadré par des garanties suffisantes. Le demandeur doit clairement communiquer tous les éléments nécessaires pour que la partie destinataire puisse prendre une décision fondée concernant la demande, notamment son motif ainsi que la finalité du transfert de données.

Un niveau de protection approprié des données devrait être garanti lorsque des données doivent être transférées vers des pays qui ne sont pas parties à la Convention 108 (par exemple, par des moyens de sauvegarde standardisés ad hoc ou approuvés prévus par des instruments juridiquement contraignants et applicables.

Si l'autorité expéditrice soumet l'utilisation des données dans l'État destinataire à un certain nombre de conditions, celles-ci devraient être respectées. Le pays expéditeur et le pays destinataire devraient être d'accord sur l'utilisation des données tout au long de leur cycle de vie.

Exemple : la retransmission à un autre destinataire des données communiquées ne devrait être autorisée que si elle est nécessaire à des fins identiques à celles de la communication initiale et si ce deuxième destinataire est également un service de police garantissant un niveau approprié de protection des données. Le service de police qui a envoyé initialement les données doit également donner son accord pour une éventuelle retransmission. Si un service de police du pays X envoie des données à caractère personnel à un service du pays Y, celui-ci ne peut les transférer que dans le cadre des dispositions légales susmentionnées (autrement dit si la loi encadre le transfert et si celui-ci correspond à l'objectif d'origine) et si le pays X l'accepte. Si les données sont communiquées à un pays Z qui n'est pas membre de la Convention 108, le pays Y doit veiller à ce que ce pays offre un niveau de protection approprié des données à caractère personnel et des moyens effectifs pour l'exercice des droits correspondants des personnes concernées.

Le transfert international de données à caractère personnel à un service public qui ne dépend pas de la police n'est autorisé qu'à titre exceptionnel et dans des cas particuliers, s'il est nécessaire pour l'exécution de la tâche de l'autorité émettrice et s'il n'existe aucun autre moyen efficace de transférer les données à un service de police. Les principes de protection des données énoncés dans la Convention 108 doivent être respectés pour tous les types de transferts.

Exemple : si les autorités fiscales d'un pays X demandent à la police d'un pays Y de lui indiquer l'adresse d'une personne impliquée dans une évasion fiscale non criminelle parce qu'elle a la preuve que la personne participe à des affaires criminelles dans le pays X, la police peut transférer les données à caractère personnel de la personne concernée pour autant que sa loi nationale l'y autorise. .

En règle générale, le transfert international de données à caractère personnel entre la police et des organismes privés résidant dans une juridiction différente devrait être évité. Cela ne peut avoir lieu que dans des cas très exceptionnels dans lesquels cela est absolument nécessaire pour l'accomplissement des fonctions de police telles que décrites au point 1, prévu par des voies légales et quand l'urgence, la gravité du crime, son caractère transfrontalier et quand l'implication éventuelle de la police locale pourraient nuire à l'objet de l'enquête pour des raisons objectives. D'autres faits tels que la sécurité des données, l'assurance reçue relative à l'utilisation des données et la licéité du transfert des données dans le pays destinataire

[53] Cela est sans préjudice du droit du Comité de la Convention 108, et d'autres instances disposant de ce pouvoir, d'évaluer et de réexaminer si nécessaire le niveau de protection des données garanti par ces accords multilatéraux.

Deleted: adéquates

Deleted: appliqués

Deleted: le

Deleted: de celle-ci

Deleted: sont

Deleted: .

Deleted: ¶
¶

Comment [A73]: Le texte du principe 5 de la recommandation ne le dit pas. Déduit-on cette condition du principe 4 ? Ne faudrait-il pas plutôt dire "que si elle vise des finalités compatibles avec les finalités initiales? "

Deleted: précises

Deleted: le transfert

Deleted: dispose d'une

Deleted: juridique adéquate

Deleted: en matière de traitement

Deleted: garantisse un niveau approprié de protection des données à caractère personnel.

Deleted: de transfert

Deleted:

Comment [A74]: Compléter avec "pour autant que sa loi nationale l'y autorise"

Deleted: L

Deleted: policières

Deleted: à

Deleted: en règle générale

Deleted: type de transfert

Deleted: la participation

Deleted: en raison de la durée de la procédure.

doivent être pris en compte. Dans ce contexte, il convient de noter que, dans un tel cas, le responsable du traitement des données a une double obligation en ce qui concerne la protection des données à caractère personnel : celle imposée par le cadre juridique de son pays de résidence et celle liée au transfer de données. La police locale devrait être informée ultérieurement. La police est invitée, dans la mesure du possible, à utiliser les instruments juridiques internationaux existants en ce qui concerne ce type de transfert de données. Des transferts internationaux sont aussi exceptionnellement possibles quand la police doit communiquer des données à caractère personnel à des fins humanitaires.

Exemple : dans une enquête menée dans le cadre d'un accord international multilatéral sur du matériel pédopornographique diffusé sur internet, la victime est dans le pays Y et la police y a commencé l'enquête mais le suspect ayant mis en ligne ce matériel réside dans un autre pays (pays X), le risque est élevé que la personne cherche à fuir le pays X. Dès lors, la police du pays Y peut demander à un fournisseur de services internet du pays X de lui fournir, à titre exceptionnel, des informations sur le lieu de résidence de son client. Cependant, la police du pays Y devrait informer la police du pays X de son opération le plus tôt possible et chercher à résoudre l'affaire en coopération.

15. Conditions de la communication

Dans la mesure où le responsable du traitement a l'obligation générale de veiller à une haute qualité des données, il est souhaitable de procéder à une vérification supplémentaire avant de communiquer des données à d'autres organismes. Toute communication ou transfert de données doit s'accompagner d'un contrôle rigoureux de leur qualité : leur exactitude, leur actualité et leur exhaustivité. Autant que possible, les décisions judiciaires ainsi que les décisions de ne pas poursuivre devraient être indiquées lors de toute communication de données. Des canaux de communication sûrs doivent être mis en place afin d'assurer une sécurité des données au plus haut niveau possible. La qualité des données peut être évalué jusqu'au moment de la communication.

Exemple : si des données à caractère personnel qui contiennent des données erronées (données à caractère personnel ou non) sont envoyées, elles peuvent négativement affecter l'enquête, causer préjudice à la personne concernée ou à d'autres personnes impliquées ou qui pourraient l'être du fait d'un transfert de données incorrectes. Cela peut entraîner la responsabilité de l'État expéditeur comme de l'État receveur vis-à-vis des personnes concernées. L'arrestation d'une personne du fait de la mauvaise communication du nom d'un suspect porte gravement atteinte à plusieurs droits de l'homme de la personne concernée et peut affecter l'enquête pénale.

16. Garanties concernant la communication

Il est de la plus haute importance que les principes de nécessité et de limitation de la finalité soient applicables à toute communication nationale ou transfert international de données à caractère personnel en dehors des services de police.

Toute donnée communiquée ne devrait pas être utilisée à d'autres fins que celles pour lesquelles elle a été communiquée ou reçue. Les seules exceptions à cela s'appliquent lorsque l'autorité expéditrice donne, sur une base légale, son accord pour une autre utilisation et si cela est nécessaire et indispensable pour que le destinataire accomplisse sa tâche. Les données peuvent également être communiquées dans l'intérêt de la personne concernée ou pour des raisons humanitaires, ou encore si cela est nécessaire pour prévenir un risque grave et imminent à l'ordre public ou à la sécurité publique ou qu'un niveau approprié de protection des données est garanti par le destinataire au moyen d'un instrument juridique international ou national, ou par des moyens de sauvegarde standardisés ad hoc ou approuvés prévus par des instruments juridiquement contraignants et applicables, comme le prévoit la Convention 108.

Exemple : des données à caractère personnel envoyées par la police du pays X à la police du pays Y dans un cas de blanchiment d'argent ne peuvent pas être utilisées par des policiers pour mettre en place un profilage sur les croyances religieuses ou les activités politiques de la personne concernée (sauf si elles ont un lien manifeste avec le crime commis et si la police du pays X a également donné son accord pour cette utilisation).

17. Interconnexion des fichiers et accès direct (accès en ligne)

Deleted: en
Deleted:
Deleted: ,
Deleted: l
Deleted: pédopornographique
Deleted: il existe alors un
Deleted: quitte
Deleted: L
Deleted: et devrait donc
Deleted: :
Deleted: ,
Deleted: de
Deleted: de
Deleted: de
Deleted: Cela
Deleted: l
Deleted: sont envoyées
Deleted:
Deleted: , cela
Deleted: impliquées
Deleted: é
Deleted: é
Deleted: e à une
Deleted: a
Deleted:
Deleted: le traitement est prévu par la loi,
Deleted: ,
Deleted: est
Deleted: et
Deleted: données tel que prévu par la Convention 108est
Deleted: .
Deleted: l

Dans des situations particulières, la police peut chercher à collecter des données en coordonnant ses informations avec celles d'autres responsables de traitement et sous-traitants. Elle peut également combiner des données à caractère personnel dans divers fichiers ou bases de données détenus à des fins différentes, par exemple des fichiers conservés par d'autres organismes publics ou privés. Ces recoupements peuvent être en relation avec une enquête pénale en cours ou servir à repérer des tendances thématiques en relation avec un certain type de crime.

Pour être légitimes, ces démarches doivent être autorisées ou s'appuyer sur une obligation légale de se conformer au principe de limitation de la finalité.

Le service de police qui a directement accès aux fichiers d'autres services répressifs ou non répressifs ne doit y accéder et utiliser les données consultées que si la législation nationale qui doit prendre en compte les principes fondamentaux de la protection des données le permet.

Une législation et des indications claires, conformes aux principes de protection des données, doivent être en place pour encadrer ces croisements de bases de données. Ces croisements de base de données devraient être nécessaires, servir une finalité précise et être proportionnés. En ce qui concerne les données personnelles conservées dans les bases de données d'autres responsables de traitement ou de sous-traitants, toutes les conditions décrites au point 2 doivent être remplies et régulièrement vérifiées.

Exemple : des données conservées aux fins de la citoyenneté ne peuvent être utilisées dans une enquête que si la législation nationale le permet et dans la mesure où elles sont nécessaires aux fins de l'enquête. Par exemple, le nombre d'enfants d'un suspect est une information qui n'est probablement pas utile à une enquête et ne devrait donc pas être traitée par la police. Si l'accès à une base de données peut être parfaitement légale, elle peut n'être légitime que dans le respect des principes de la protection des données personnelles.

18. Sécurité des données

La police doit prendre des mesures adéquates de sécurité contre des risques tels que l'accès accidentel ou non autorisé à des données à caractère personnel ou la destruction, la perte, l'utilisation, la modification ou la divulgation de ces données. Le responsable du traitement doit, au minimum, informer sans délai l'autorité de contrôle compétente de ces violations de données qui, selon son jugement, peuvent gravement porter atteinte aux droits et libertés fondamentales des personnes concernées. Les personnes concernées par des violations de leurs données qui peuvent gravement porter atteinte à leurs droits doivent être informées sans délais superflu, sauf si cela présente un risque pour les activités de la police.

La sécurité des informations est essentielle à la protection des données. Il s'agit d'un ensemble de procédures destinées à garantir l'intégrité, la disponibilité et la confidentialité de toutes les formes d'information et qui doit être mis en place au sein de la police en vue d'assurer la sécurité des données et des informations et de limiter l'impact des incidents de sécurité et violations des données à un niveau prédéterminé.

Le niveau de protection conférée à une base de données et/ou à un système ou un réseau informatique est déterminé au moyen d'une évaluation des risques. Plus les données sont sensibles, plus la protection devra être importante. Les mécanismes d'autorisation et d'authentification sont essentiels à la protection des données et il conviendrait de procéder au chiffrement systématique des informations sensibles. La mise en place d'un dispositif régulier de vérification de l'adéquation du niveau de sécurité est considérée comme une bonne pratique.

Il est conseillé aux services de police de procéder le cas échéant à une évaluation de l'impact sur la protection des données personnelles (EIPD) (voir point 4) afin d'évaluer les risques pour les droits de la

Deleted: dans le cadre de

Deleted: Il conviendrait d'élaborer u

Deleted: <#>Droits de la personne concernée¶
¶
Le droit à l'information, le droit d'accès, le droit de rectification et le droit d'effacement sont des droits interdépendants. Le droit à l'information visé au point 4 est une condition préalable au droit d'accès ; la personne concernée a le droit d'obtenir des informations sur le traitement de ses données et d'exercer d'autres droits sur la base de ces informations. Le responsable du traitement des données doit veiller à ce que tout type de traitement des données soit notifié au public, accompagné de toute autre information pertinente relative au traitement tel que prévu au point 4. L'autorité de contrôle peut contribuer à la diffusion publique des informations nécessaires.¶
¶
La police devrait fournir une réponse, même aux questions d'ordre général posées par les intéressés sur les activités de traitement de leurs données à caractère personnel, mais elle peut utiliser des formulaires pour faciliter la communication.¶
¶
Exemple : si une personne concernée demande à la police des informations sur le traitement de ses données à caractères personnel, la police, s'il n'y a pas d'exception applicable, devrait répondre de façon claire, détaillée et citer des références juridiques pertinentes.¶
¶
L'accès aux données est un droit fondamental reconnu à tout individu s'agissant de ses données à caractère personnel. Dans l'idéal, le droit interne devrait prévoir, en règle générale, un droit d'accès direct. ¶
¶
Le droit d'accès (comme le droit à l'information) devrait, en principe, être gratuit. ¶
¶
Il est possible de facturer des frais administratifs raisonnables pour la demande si la législation nationale le prévoit et que la demande est manifestement infondée ou excessive. La police peut également refuser de répondre à ces demandes manifestement infondées ou excessives, en particulier lorsque le caractère répétitif de celles-ci justifie un tel refus.¶
¶
Pour que l'exercice du droit d'accès soit équitable, la communication « sous une forme intelligible » s'applique aussi b ...

Deleted: pour lutter

Deleted: de

personne concernée découlant de la collecte, de l'utilisation et de la divulgation des informations. Elle permettra de recenser les risques et d'élaborer des solutions pour remédier efficacement aux défaillances constatées. Une telle évaluation doit porter sur les systèmes et procédures pertinents des opérations de traitements, et non sur des cas individuels.
Un délégué à la protection des données (DPD) au sein de la police peut jouer un rôle essentiel dans la réalisation de vérifications internes et l'évaluation de la légitimité du traitement. Cette fonction contribue au renforcement de la protection des données et de la sécurité des données. En outre, ce délégué peut faciliter le dialogue entre l'administration et les personnes concernées et entre l'administration et l'autorité de contrôle, ce qui peut également renforcer la transparence globale du service de police.

Il est recommandé d'utiliser un système de gestion de l'identité et des accès pour gérer l'accès des employés et des tiers aux informations. L'accès au système sera soumis à une authentification et à une autorisation ; un système de droits réservés permettra de déterminer les données consultables. Un tel système peut être considéré comme une condition utile pour garantir un accès sécurisé et adéquat aux données.

Le responsable du traitement des données devrait mettre en œuvre, après une évaluation des risques, les mesures destinées à garantir :

- le contrôle de l'accès à l'équipement,
- le contrôle des supports des données,
- le contrôle de l'enregistrement des données,
- le contrôle des utilisateurs,
- le contrôle de l'accès aux données,
- le contrôle de la communication des données,
- le contrôle de la saisie des données,
- le contrôle du transfert des données,
- la récupération des données et l'intégrité du système,
- la fiabilité et l'intégrité des données.

Le respect de la vie privée dès la conception (« privacy by design »)

Le concept du respect de la vie privée dès la conception fait partie intégrante de la sécurité des données. La protection et la sécurité des données peuvent être directement intégrées dans les systèmes et processus d'information, au moyen de mesures techniques et organisationnelles, afin d'assurer un niveau élevé de protection et de sécurité des données et, en particulier, de réduire au minimum le risque de violation. Cette approche, appelée « respect de la vie privée dès la conception », favorise dès le début la prise en compte de la protection de la vie privée et des données. Elle peut être mise en place au moyen d'un logiciel et/ou d'un matériel informatique. Elle suppose une analyse des risques, une approche fondée sur un cycle de vie complet et une vérification rigoureuse.

Il importe que les responsables du traitement veillent à ce que la protection de la vie privée et des données soit rigoureusement prise en compte aux premiers stades d'un projet, puis tout au long de son cycle de vie. C'est tout particulièrement le cas lorsqu'on conçoit un nouveau système informatique d'enregistrement de données à caractère personnel ou d'accès à celles-ci, lorsqu'on élabore une législation, une politique ou une stratégie ayant des répercussions sur la vie privée et lorsqu'on met en place un partage des informations qui utilise des données à de nouvelles finalités.

Le « respect de la vie privée dès la conception » (PETs) suppose la mise en œuvre de technologies de renforcement de la protection de la vie privée afin de permettre une meilleure protection des données à caractère personnel. Ces technologies empêchent le traitement excessif des données à caractère personnel sans réduire les capacités fonctionnelles du système informatique.

Exemple : les scanners corporels utilisés à des fins policières doivent être conçus pour respecter la vie privée des individus à inspecter tout en répondant à l'objectif de leur utilisation. C'est pourquoi l'image du corps qui apparaît dans ces outils doit être brouillée par défaut.

Deleted: ¶
¶
¶
¶

Deleted: droit au respect

Deleted: *Les technologies de renforcement de la protection de la vie privée* (« PET »)¶
¶
Ce terme désigne un éventail de technologies différentes qui visent à protéger les données à caractère personnel sensibles dans les systèmes informatiques.

Deleted: qui permettent aux utilisateurs de mieux protéger leurs

Deleted: Elles sont principalement utilisées pour déterminer si des informations identifiables sont nécessaires lorsqu'il est question de l'élaboration, de la conception d'un nouveau système informatique, ou de l'amélioration d'un système existant.¶

Deleted: ,

19. Contrôle externe

Au minimum, une autorité de contrôle doit être chargée de veiller à la conformité du traitement des données avec la législation nationale et internationale dans le secteur de la police.

Certains États peuvent exiger l'existence de plusieurs autorités de contrôle, par exemple une autorité nationale ou fédérale et plusieurs d'autorités décentralisées ou régionales, tandis que d'autres préféreront une seule autorité de contrôle, responsable de l'intégralité de la supervision des opérations de traitement des données à caractère personnel.

L'organe de contrôle devrait être totalement indépendant et donc ne pas appartenir à un service de répression ni être dirigé par un autre organe dépendant de la partie exécutive d'une administration nationale. Il devrait disposer des ressources suffisantes pour exécuter ses tâches et fonctions et ne pas être obligé de recevoir des instructions d'où qu'elles viennent. L'indépendance personnelle de son président, aussi bien politique, financière, fonctionnelle et opérationnelle, est un critère essentiel lorsqu'il s'agira d'en évaluer l'indépendance.

La législation nationale devrait conférer à cet organe des pouvoirs de conseils, d'enquête et des pouvoirs répressifs lui permettant d'enquêter à la suite de plaintes, d'appliquer des mesures réglementaires ou d'infliger des sanctions le cas échéant. Les outils juridiques et administratifs à sa disposition doivent être efficaces et pouvoir être mis en œuvre.

Les autorités de contrôle devraient avoir la capacité de coopérer bilatéralement dans le domaine répressif et par l'intermédiaire du Comité de la Convention 108.

Exemple : l'autorité de contrôle doit être indépendante et doit disposer de tous les pouvoirs nécessaires pour accomplir sa tâche. Une autorité mise en place au sein d'un ministère ou de la police elle-même ne remplit pas cette obligation.

Deleted: É
Deleted: membres
Deleted: ou à l'exécutif
Deleted: .
Deleted: oit
Deleted: mener une enquête
Deleted: 'une

Glossaire/définitions

Aux fins du présent guide :

a) « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (« la personne concernée ») ;

b) « données génétiques » : toutes les données concernant les caractéristiques génétiques d'une personne qui ont été héritées ou acquises durant la phase de développement prénatal, tels qu'elles résultent d'une analyse d'un échantillon biologique de la personne concernée: analyse chromosomique, analyse d'ADN ou d'ARN ou analyse de tout autre élément permettant d'obtenir des informations équivalentes ;

c) « données biométriques » : données résultant d'un traitement technique spécifique des données concernant les caractéristiques physiques, biologiques ou physiologiques d'une personne et qui permettent son identification unique ou son authentification ;

d) « donnés subjectives » (preuve fondée sur un témoignage ou une déclaration personnelle) : données acquises par le biais de témoignages de personnes impliquées dans l'enquête ;

e) « données objectives » (preuve fondée sur des documents ou des faits avérés) : données acquises provenant de documents officiels ou d'autres sources certifiées ;

f) « traitement de données » : toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données. Lorsqu'un traitement automatisé n'est pas utilisé, le traitement de données désigne une opération ou un ensemble d'opérations effectuées sur des données à caractère personnel présentes dans un ensemble structuré de ces données qui sont accessibles ou récupérables selon des critères spécifiques ;

g) «responsable du traitement » : la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision à l'égard du traitement de données;

h) « destinataire » : la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui reçoit communication de données ou à qui des données sont rendues accessibles;

i) «sous-traitant»: la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. ;

j) « Internet des objets » (IdO): interconnexion d'appareils physiques, de véhicules (également appelés « appareils connectés » et « appareils intelligents »), de bâtiments et d'autres dispositifs intégrant de l'électronique, des logiciels, des capteurs, des actionneurs, et connectivité réseau qui permettent à ces objets de collecter et d'échanger des données ;

k) « surveillance secrète » : toutes les mesures visant à surveiller discrètement les mouvements de personnes, de véhicules et de conteneurs, en particulier ceux qui sont employés par la criminalité organisée ou transfrontière ;

l) « techniques d'enquêtes spéciales » : techniques appliquées par des autorités compétentes dans le contexte d'enquêtes criminelles en vue de détecter des crimes graves et d'identifier des suspects et d'enquêter sur eux dans le but de rassembler des informations de telle manière à ne pas attirer l'attention de la personne visée ;

m) « technologies d'enforcement de la protection de la vie privée » (PETs) : diverses technologies utilisées pour protéger les données personnelles au sein de systèmes d'information. L'aspect le plus important dans l'utilisation des PETs est de déterminer au moment du développement ou de la conception d'un

Deleted:

Deleted:

Deleted: un

Deleted: <#>« autorité compétente » : organisme public ou privé habilité par la loi et disposant d'une compétence dans la prévention, les enquêtes, les poursuites des infractions pénales et l'exécution des sanctions pénales ;¶

Deleted:

Deleted: ;

Deleted: .

Deleted: e

Deleted:

nouveau système d'information ou de la mise à jour d'un système existant si une information identifiable est nécessaire .

Deleted: .

UNITED KINGDOM/ROYAUME UNI

A guide such as this must provide a pragmatic overview of the broad guidelines to be followed, as set out in the Council of Europe Recommendation (87) 15 but also take account of other relevant international public law. Whilst the EU Data Protection Directive 2016/680/EU (hereafter EU DPD) is separate, if this draft guidance is to achieve its purpose, we consider that it should take account of the EU DPD's requirements.

We have found that this draft practical guide is in part in keeping with the EU DPD but at times does not take into account those requirements, resulting in a skewed view of what is expected of police when handling data.

Our starting point is that data protection in the law enforcement area must provide a balance between the need for public protection and the protection of the data subject's personal data. Some initial suggestions are outlined below. These written comments are without prejudice to any further comments that we may make.

Paragraph 2 - General Considerations

The phrase refers to data being processed in a "transparent manner". We would like to highlight that **transparency is no longer a requirement** under the EU DPD, Article 4(1) (first data protection principle). Member States must only provide for personal data to be processed lawfully and fairly in respect of processing data for law enforcement purposes.

We therefore propose to **remove the reference** and use "Data processing should be carried out lawfully and fairly."

***Paragraph 2* - Collection of data and use of data**

(paragraph 2.1)

The phrase from Recommendation (87) 15 - that the collection of personal data for "police purposes" should be "limited to that which is necessary for the purpose of prevention, investigation and prosecution of criminal offences and the execution of criminal penalties (i.e. to a specific criminal offence)' is not sufficiently broad as to capture the broader range of tasks which the police perform, particularly in the safeguarding arena.

The drafting in the EU DPD better reflects that role and it would be **clearer to state** that the collection of personal data for law enforcement purposes is permitted for "the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to

public security" (Article 1(1), EU DPD) which aligns with the scope and definition explanation of "police purposes" in Recommendation (87) 15.

We would furthermore suggest **rewording** of the expression 'real danger' as it leaves too much space for speculation

(paragraph 2.3)

The explanation that "prior to and during the collection of such data the question of whether the personal data collected is necessary for the investigation should always be asked" is misleading as data collection does not necessarily imply an investigation.

We consider that it would be more accurate to **remove "for the investigation" or replace it** with "collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes" (Article 4(1)(b), EU DPD).

(paragraph 2.10)

The paragraph states that "According to the purpose limitation principle, personal data collected for police purposes should be used for those purposes only and should not be used in any other way that is incompatible with the original purpose stated at the time of collection and is necessary for and proportionate to the pursuing of police purposes, unless this is provided for in law (see Article 9 of Convention 108)".

We suggest **replacing** the wording "unless provided for in law" with "as set out in the Data Protection legislation" to correct this sentence.

***Paragraph 3* – Subsequent use of data**

(paragraph 3.2)

The explanation refers to "criteria and conditions set in point 2". However, neither the conditions nor "point 2" are being evidently outlined in the draft. It would be helpful to **provide clarification**.

(paragraph 3.4)

In the first sentence, we suggest to **include the wording "or"** so the sentence would read as: "In cases such as trafficking in human beings, drug trafficking or sexual exploitation, **or** where victims' data may subsequently be used also when they are considered as suspects, where the protection of victims of a more severe crime can override the interest of prosecuting less severe crimes, [...]."

This is to clarify that victims are not considered suspects, which is how the sentence would otherwise read.

***Paragraph 4* – Processing of special categories of data (sensitive data)**

(paragraph 4.1)

The first paragraph suggests that data revealing a subject's racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life "can only be processed if prescribed by law and appropriate safeguards have been put in place." This is **not correct** as Article 10 of the EU DPD clearly sets out that this can be done where authorised by a Member State law OR to protect the vital interets of the data subject. We therefore **suggest removing or rephrasing** this reference.

We furthermore suggest **adding that another possibility to process sensitive data** is when it has been made public by the data subject.

(paragraph 4.3)

Profiling as a general rule is not prohibited under the EU DPD, which is why the reference to "profiling should be avoided as a general rule" is **misleading**.

We suggest **making it clearer** that the issue lies in collecting data *solely* on the basis of profiling. We suggest therefore that the explanation should be expanded to state that a decision based solely on profiling which has the impact of producing an "adverse legal effect concerning the data subject or significantly affects him or her" should be prohibited. This is to take account of the EU DPD (Article 11).

***Paragraph 5* - Providing information to data subjects**

(paragraph 7 and 8)

We would encourage that the practical guide **clearly illustrates that it may be necessary to withhold this information for other purposes** such as for the avoidance of obstructing official or legal inquiries, investigations or procedures, to protect public security, to protect national security, or to protect the rights and freedoms of others. These criteria can be found in Article 13(3) of the EU DPD.

***Paragraph 6* – Data subjects' rights**

(paragraph 6.3)

The paragraph reads "Withholding information about the data processing by police, however, should be used only sparingly and where it can be clearly justified." We strongly recommend removing the words "only sparingly" as this is not correct. If an exception applies, then withholding notification would be justified based on the applicable law. The reference to frequency is misleading.

We would encourage that the practical **guide clearly illustrates that it may be necessary to withhold this information for other purposes** such as for the avoidance of obstructing official or legal inquiries, investigations or procedures, to protect public security, to protect national security, or to protect the rights and freedoms of others. These criteria can be found in Article 13(3) of the EU DPD.

(paragraph 6.10)

The last sentence in the paragraph states that "In case of a restriction, partial information, and in case of derogation, information on the use of derogation shall be still given, with the motivation for using such measures in both cases, as well as information concerning redress."

We would like to highlight that the EU DPD permits restrictions – so domestic law which implements it will permit a controller, for instance, to restrict a data subject's right of access, where this is considered necessary and proportionate measure. The controller will not have to provide the data subject with the reason for the restriction where this would undermine the purpose of the restriction.

We therefore suggest **rephrasing** the sentence to "Measures concerning restrictions and partial derogations shall be based on provisions set out in the EU Data Protection Directive".

(paragraph 6.18)

The paragraph states that "Data subjects can ask for the deletion of their personal data where such processing is unlawful." This sentence is quite vague and does not reflect the data subject's rights appropriately.

Therefore, we suggest **rephrasing** the sentence to: "Data subjects can ask for the deletion of their personal data where it would infringe relevant data protection legislation. This should include a requirement to process data which is accurate, a duty to take all reasonable steps to ensure that personal data that is inaccurate is erased or rectified without delay. This should also apply to situations where the controller has a legal obligation to erase the data."

***Paragraph 7* – Exceptions from the application of data protection principles**

(paragraph 7.1)

The explanation should take note of Article 55 of the EU DPD which makes clear that any action of this kind must be clearly mandated. In addition, **the ability to "Neither Confirm Nor Deny" (which is provided for in the EU DPD in Article 13(3)) must still be upheld with both direct and indirect access,** and so the explanation that "the DPA will then reply to the data subject" should be amended to ensure that this reply upholds this essential NCND requirement where necessary.

(paragraph 7.3)

Again, regarding the "possible exemptions" from direct access, and in the event of a refusal of that right, the explanation should clearly outline the possibility to provide a "Neither Confirm Nor Deny" (NCND) in response to such requests. This is consistent with Article 13 (3) of the EU DPD and essential in some cases, particularly concerning national security.

We therefore feel that the reference to being able to provide a "**Neither Confirm Nor Deny" response should be incorporated** in the draft.

***Paragraph 9* – Introduction of new data processing technologies**
(paragraph 9.2)

The paragraph states that "The introduction of new data processing technologies is considered to be subject to a DPIA as probability of risks to the individual's rights is usually high." We find it incorrect to generalise and describe all new technologies as risky without providing any specification.

We therefore suggest to **rephrase** the sentence to "In deciding whether a new type of data processing is likely to result in a high risk to the rights of the individual, the controller must take into account the nature, scope, context and purposes of the processing."

***Paragraph 11* – Communication of data within the police sector**

We presume that "Communication of data" refers to data *sharing*, but this is not clear from the headline, which is why we suggest **replacing** "communication of data" with "data sharing".
(paragraph 11.1)

The paragraph reads as follows: "The police can only communicate personal data within the police sector if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies."

This sentence should be **deleted**, because domestic data sharing between police units is a matter for domestic regulations.

Instead, the paragraph should make clear that whilst sharing data between different police organisations, the fundamental rights and freedoms of natural persons need to be protected, in particular their right to privacy with respect to the processing of personal data (Article 1(1) EU DPD).

***Paragraph 12* – Communication of data within the police sector**
As per Paragraph 11, we suggest **replacing** "communication of data" with "data sharing".

(paragraph 12.1)

Article 8 EU DPD refers to "performance" (not fulfillment) of a task carried out by a competent authority which seems to cover either the tasks of the recipient Competent Authority or transferring Competent Authority. We therefore recommend replacing the phrase "in the fulfilment of their duties and tasks" with "in the performance of their duties and tasks".

(paragraph 12.2)

As a matter of law the phrase "stricter principles" is quite vague. We therefore suggest **replacing** it with the following wording: "careful consideration should be given".

***Paragraph 13* - Communication of data by the police to private parties**
As per Paragraph 11 and 12, we suggest **replacing** "communication of data" with "data sharing".

The document refers to "private bodies" and occasionally to "private parties" referring to the same thing. For the purpose of consistency, we suggest replacing any reference of "parties" with "bodies".

(paragraph 13.1)

The paragraph states that "[...] under strict conditions, the police can communicate data to private bodies [...]". We ask for **clarification** as to what 'strict conditions' mean in this context.
It is clear that private bodies can be viewed as carrying out a public role, on behalf of public bodies, and in order to reflect that context the EU DPD included in its definition of a competent authority, in addition to a public body, any other body or entity entrusted by law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" (Article 3 (7) (b), EU DPD).

***Paragraph 14* – International transfers**
(paragraphs 14.1)

Our previous comment doesn't seem to have been considered, but as we feel strongly about it, we would like to stress once again that:

For international transfers, the EU DPD provides for a range of routes; by virtue of an adequacy decision, appropriate safeguards as well as a section on derogations. These all provide means of transferring internationally with a broader range of possible criteria.

In addition, the EU DPD clearly allows for the transfer of data to a private entity internationally which is not consistent with the explanation in the draft guidance which states that "any communication of data internationally should be strictly limited to another police organisation."

Furthermore, Paragraph 14.3 is inconsistent with Part D of the EU DPD which allows transfer to third states, international organisations and directly recipients in a range of circumstances.

(paragraphs 14.3)

Paragraph 3 states that international transfers should be used as a last resort option. This statement is inconsistent with Part D of the EU DPD which allows transfer to third states, international organisations and directly recipients in a range of circumstances. We therefore suggest **removing** this reference.

(paragraphs 14.6 - Example)

The first sentence reads “Further transfer of data should only be allowed if this is necessary for the same police purpose as the original transfer and the second recipient is also a police body ensuring an appropriate level of data protection.” This is **inaccurate** as the only requirement for onward transfers is consent of the original transferring Member State (Art 35(1)(e) DPD).

We suggest **removing** this reference.

(paragraph 14.7)

We consider that the explanation **must make even clearer** that it is not just occasionally when it is necessary to transfer data to private entities in order to protect the public, and that it might be helpful to draw upon the criteria in Article 39 (1) (a) to (e) of the EU DPD.

We would also like to point out that Article 39 does not limit transfers to exceptional cases as the phrase “The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases...” might suggest. We stress that this paragraph **needs to be re-worded**.

It would be better if this **could read more permissively** and we suggest **the following wording**: ‘The transfer of personal data to a non-police body is permissible when necessary to comply with a duty required of the transferring authority and it is not possible to transfer to a policing body’.

Furthermore, the wording referring to “the gravity of the crime” in this paragraph will **lead to debate as to how to define ‘gravity’**, which we suggest **rephrasing**.

We would also need to **ensure proper measures were in place** to protect the security of the information and have reassurances as to the use to be made of it.

Additionally, there would need to be **certainty** that this did not contravene local law.

(paragraph 14.9)

The paragraph states that “It can only be done in very exceptional cases, where it is strictly necessary for the fulfilment of the tasks of police as described in Point 1, provided by legal means and where the emergency, the gravity of the crime, its trans-border nature and where the involvement of the police would not be possible for objective reasons”.

We suggest **replacing** the phrase “strictly necessary” with just “necessary” as we are of the opinion that the addition “strictly” may lead to a debate regarding its definition; in addition, the word “strictly” does not add any value to the sentence.

We suggest **replacing** the word “fulfilment” with “performance” to be accurate.

The wording referring to “the gravity of the crime” in this paragraph will also lead to debate as to how to define ‘gravity’, which we suggest **rewording**.