COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 8 September 2017 T-PD (2016)02rev9

Deleted: 26

Deleted: June

Deleted: 02rev8

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

Draft practical guide on the use of personal data in the police sector

Revised version prepared by the Secretariat based on comments received

Directorate General of Human Rights and Rule of Law

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied for ensuring 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.

Deleted: clear

The present Guide was therefore prepared, aiming to highlight the most important issues that may arise in the use of personal data in the police sector and pointing 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 in the police use of personal data are determined in full respect of the the rights of the individual to privacy and data protection.

Deleted: 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

To facilitate the reading of the Guide, a glossary of the terms used is provided at the end of the document.

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

General considerations

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 that they should be necessary and proportionate to these legitimate purposes and should always be in compliance with the original purpose. The data processing should be carried out lawfully, fairly and in a transparent manner. The 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.

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, foreseeable and accessible), pursue a legitimate purpose and be limited to what is necessary and proportionate to achieve that legitimate purpose and it *must* be carried out in a legitimate way.

1. Scope

The principles explained in the present guide apply to the processing of personal data for police purposes, primarily for the specific purposes of the prevention, investigation and prosecution of criminal offences, the execution of criminal penalties and for the maintenance of public order (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

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 and the execution of criminal penalties (i.e. to a specific criminal offence(s) or the suspicion thereof) and where personal data is processed for the purpose of the maintenance of public order. The police as data controller is responsible for all data processing it undertakes therefore it can be held accountable for its data processing operations.

It has to be reiterated that according to Point 2.1 of the Recommendation during the fulfilment of both of the main police tasks (prevention of a real danger and the suppression of 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.

Police should always choose the adequate legal base to process personal data and should process personal data in a legitimate way. A careful assessment on the legal basis (law, consent, contract, vital interest of the individual, etc.) the personal data is processed on needs to be done taking into account the different operations during which the police is processing data (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 respond to certain criteria explained below.

Police should apply at all stages of the processing the relevant data-protection principles, most importantly the principle of necessity, proportionality and purpose-bound data processing principle and should not continue to process data which are not needed for the purpose of the processing. In this context, personal data collected at an early phase of the investigation, which then proves with the

Deleted: processing

Deleted: based

Deleted: that

Deleted: it

Deleted: It

Deleted: data which are processed within the police

Moved (insertion) [1]

Deleted: clear

Deleted: publicly available

Deleted: aim

Deleted: aim

Deleted: offences and the

Deleted: that which

Moved up [1]: 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.

process of the investigation to be no longer relevant should no longer be processed (e.g. innocence of a suspect is confirmed), therefore they should be either blocked or deleted permanently.

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 specific task of the police as described in Point 1 should always be asked. 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 and is to be demonstrated at all times as well as the compliance of the data and of the processing to the data protection principles as described in this Guide. After the collection phase and at different stages of the investigation a thorough analysis is needed in order 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 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 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), provided that this is based on an adequate legal measure (foreseeable and accessible) which is necessary and proportionate in a democratic society. In assessing the compatibility of the use of data one should assess 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 before, especially those related to the principles of necessity and proportionality, the lawful and legitimate data processing.

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 and up-to-date and are 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 fact that the original processing has been carried out for police purpose or for other purposes) 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 legitimate, necessary and proportionate to the legitimate aim pursued by the police.

Personal data subsequently used should be linked to a specific, well-defined police purpose and must fulfil the criteria and conditions set in Point 2. The general rule is that if a data is likely to be used for in a different case or in a different operation of the police the compliance tests 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 automatized data processing and 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 too general purposes

Deleted: During collection, provided that all legal requirements are met, a larger scale of personal data can be processed.

Deleted: Police should apply the data-minimisation principle at all stages of the processing and should not continue to process data which are not needed for the purpose of the processing. 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). ¶

Deleted: the relevant people.

Deleted: in law

Deleted:).

Deleted: use

Deleted: applicable to the collection and the use of data.

Deleted: ¶
¶

Deleted: ~~same~~

Moved down [2]: 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.

Deleted: This means that p

Deleted: point

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

Moved (insertion) [2]

Deleted: the

Deleted: nature of data processing, it is possible to use personal data collected for one purpose for another

or in a way which would not comply with the principle of purpose limitation, unless in specific cases where there is a legal basis (as discussed in Point 7), a legitimate interest and operational reason within the legal powers of the police for this (e.g. in the case of multiple recidivist or terrorist groups).

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 principles of necessity and proportionality which shall include possibilities for the exercise of the right to deletion.

In cases such as trafficking in human beings, drug trafficking, 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. This however, if all legal requirements as put forward in Point 2 are met 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 commonly followed.

Example - Biometric data taken for immigration purposes can be processed for law enforcement use (such as checks against persons wanted for serious/organised crime/terrorism) if the law allows and appropriate information were given on the subsequent use of her/his data. Any such use should be lawful and proportionate and subject to specific rules on access to data by police collected for other than police purposes.

4. Processing of special categories of data (sensitive data)

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 negative discrimination or of adverse legal effect significantly affecting the data subjects. Safeguards can be of a technical, 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. The purpose of appropriate safeguards is to prevent any negative or unwanted discrimination based on these special categories of data. Safeguards should be adjusted to each of data processing operations taking into account its specificities and it is highly recommended to use multiple level of protection for those categories of data (e.g.: separate main-frames, anonimisation, shorter data retention periods, etc.). It is of paramount importance to prevent unauthorised or unwanted access those categories of data even with additional security measures.

A careful balance of interests is necessary to determine whether or not and to which extent the police would process sensitive data on the top of personal criminal data. For instance it would be advisable to differentiate when biometric data is processed by the police whether it is for identification purposes (where 2 fingerprints would suffice) or it is for crime investigation purpose (where 8 to 10 fingerprints would be needed). A greater use of Data Protection Impact Assessment (DPIA) is recommended in order to ensure that the appropriate safeguards are put in place adequately. The data controller should assess and demonstrate whether the purpose of the processing (i.e. tasks of the police) can be achieved in a manner that impacts less on the right to privacy and data protection of the data subject 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 as all profiling based on sensitive data which result in a negative discrimination are prohibited. In this context, besides measures detailed above, pseudo-anonymisation, the use of PETs and a more frequent checks on the legitimate processing (of these data can be recommended. This can, 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 are from the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

Deleted: in

Deleted: an unstructured manner

Deleted: , a legal basis

Deleted: data, in particular in respect of

Deleted: based on solid legal grounds and thorough analysis

Deleted: other

Deleted: does

Deleted: if all legal requirements as put forward in point 2 are met

Deleted: .

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 to target all followers of a religion, purely because they were members of that religion, would be 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. It should be noted that this obligation is three-fold: it requires the data controller to provide *general information* on the data processing that it carries out; to give specific information to data subjects *ex officio*, if no restrictions or derogations apply prior to the data processing and *upon request* on the processing of their personal data.

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 should be provided unless a restriction or derogation applies as described in Point 7 taking into account of the specific nature of sensitive files, such as criminal intelligence files, files containing sensitive data, etc in order to avoid serious prejudice to police in performing their functions or to other individuals' rights. Even if restrictions or derogation to the right to information were applied information should be provided to the data subjects as soon as it is not jeopardising any more the purpose for which the data were used.

The information provided to the wider public, in respect of broader information, should promote awareness, inform them in general 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 can submit an appeal to the DPA or to the judiciary against a decision of the data controller in reply to their request for information.

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

According to the second obligation of giving data subject specific information regarding their data processed by police *ex officio* respond to the general principle that an individual should always be in control of her/his data. In order to comply with this obligation police shall inform data subject on the data processing it envisages undertaking or if it is not possible for objective reasons, shortly after it undertook in relation to her/his data. This communication shall comprise information on data processing, most typically on the collection of the individuals' data and comprehensive information on their rights. 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 subject to exercise if they wish effectively their rights as prescribed in Point 6. Police can however apply restrictions or derogations to this obligation if it is foreseen by national legislation for reasons described in Point 7.

As to the third, *upon request* obligation to provide information to data subjects, the police in principle has to inform the individuals on the data processing activities that it has pursued with their data only if it receives a founded request. This means that also 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 in case of an *ex officio* communication, unless data subject wish otherwise.

Deleted:
Deleted: wo
Deleted: and
Deleted: ,
Deleted: should strike the balance between all interests concerned and also, most importantly,
Deleted: e
Deleted: ad hoc or temporary files and other particularly
Deleted:
Deleted: Information provided
Deleted: In respect of making information available which highlight data protection and data subjects' rights, this
Deleted: for access
Deleted: data controller
Deleted: if
Deleted: its
Deleted: advise

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

Deleted: mission

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 a measure.

6. Data subject's rights

The right to information, the right of access, the right of rectification and the right of erasure are interdependent rights. The right to information 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 their 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 obligation to inform data subjects in specific cases *ex officio* or *upon request*. 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.

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 the 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 in a plain language avoiding using uncommon special expressions.

Accessing data is a fundamental right for the data subjects in relation to their personal data. As a rule domestic law should, ideally, provide for direct access.

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 or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a 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 of approach 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 task of the police 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 the investigation.

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

If the right of access provided for is indirect, the data subject 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 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 subject delegates 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, excessive 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).

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 the data subjects can prove by use of the official documentation that the data processed by the police in respect of them are incorrect the data controller shall not have the right of discretion whether to correct them, or delete 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 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.

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.

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 police to retain the false statement and the information surrounding it.

Although the statement was proven to be false, if the police require retaining the data, 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 forum 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 (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 should serve a well-defined purpose and have to be incorporated into national legislation in a manner compatible with the ECtHR jurisprudence.

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 it affects 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 biding decisions of United Nations' bodies and from international humanitarian obligations etc.) 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: 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 investigate in a case of a recent terrorist attack.In order to rapidly identify the perpetrator of a terrorist act, police can envisage an urgent and extraordinary cooperation with national security agencies. During this cooperation a special procedure for the purpose of the national security is applied which takes into account the imminent risk of other individual's life and physical safety and security during which, for a limited time, exceptions to data protection provisions can be applied. In this case, access by police to both metadata and communication data in relation to person close to the scene of an attack can be granted by a less stringent fast-track procedure if such is foreseen by national law. However if there is no risk of terrorist attack, police should share its data with national security agencies according to general, well-established procedure in which stronger safeguards are put in place) with a view of ensuring the right to privacy and data protection.

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

8. Use of special investigative techniques

Deleted: ¶

Deleted: exceptions

Deleted: 4

Deleted: 7

Deleted: 17

Deleted: those

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

Moved (insertion) [3]

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

Moved up [3]: 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:

Deleted: prevent

Deleted: .

Deleted: shall

Deleted: 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

Deleted: ~~to a greater extent~~

Deleted:

Deleted: ~~imminent~~

Deleted: (such as judicial authorisation, stricter rules on purpose limitation

Deleted: an enhanced protection to the individual's

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, it is to remember that 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, it must be remembered that 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 ~~Use~~ of new data processing technologies

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.

If the processing 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, that it is repeated at reasonable intervals, and that it should touch upon relevant phases of the data processing activity. The relevance of the DPIA shall be checked at reasonable intervals.

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.

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 as those data processing methods shall be regulated by law. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights or the national legislation does not provide sufficient clarity on the implementation of these methods.

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 process 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. 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 important 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.

Deleted: those considerations

Deleted: have

Deleted: cost-effectiveness, use of resources and

Deleted: covert

Deleted: continuous (i.e.

Deleted:)

Deleted: every

Deleted: by

Moved (insertion) [4]

Deleted: with the supervisory authority

Deleted: 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

Moved up [4]: The consultation 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: are to

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

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

Deleted: which is directly linked to relevant databases

Big data analytics in the police

Deleted: *and profiling*

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

Deleted: way of processing data

Deleted: potentially and inadvertently

The Council of Europe's Recommendation CM/Rec(2010)13[2] 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[3] can be of use in the context of Big Data analysis for police use too.

Deleted: ¶

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 an additional attention to the following requirements:

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 less intrusive methods of investigation to complement the conclusions drawn. A decision affecting a person shall not be taken solely on such automatized processing of personal data.

Deleted: traditional

[2]

[3] Document T-PD(2017)1

- As for other type of data processing it is paramount that its use~~shall 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 they are processed.
- Predictive analysis requires notably 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 provided 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 secondary use.
- Even if complex methods are used and/or lengthy processing are undertaken 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.
- A clear and detailed policy regarding the classification of documents and the handling of classified information should be in place and be 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 would imply to ensure transparency of the algorhytm used and the purposes it was used for to avoid any negative discriminatory action.

It is to be stressed the above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones seems to be even more necessary to consider 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. As per the principle of legitimate processing of personal data, 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 police store and process personal data that relates 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 queries in different data base 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 processing of personal data outside of the legal framework allowed for the retention can constitute a severe violation of the right to protection of personal data and evidence gathered in this way can be seen as unlawful. If the law in relation with a specific crime provides for a data retention period of 4 years and if an individual is retained by the police solely on this ground after 4 years have passed since the collection of the data in question the retention of this data and the measures undertaken by the police based solely on this data could possibly be considered as unlawful by the court.

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: I

Deleted:

Deleted:

Deleted: purpose

Deleted: Where possible

Deleted: compatible

Deleted: L

Deleted: n

Deleted: information security

Deleted: <#>Processing of special categories of data (sensitive data)¶
¶
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. Safeguards can be of a technical for instance additional security measures and organisational nature for instance having such sensitive data processed separately from the processing environment of the "normal" categories of data. Sensitive data can, however, be processed to protect the vital interest of the data subject or of another person.¶
¶
A careful balance of interest is necessary to determine whether or not and to which extent the police would 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 2 fingerprints would suffice) or it is for crime investigation purpose (where 8 to 10 fingerprints would be needed). A greater use of Data Protection Impact Assessment (DPIA) is recommended in order ...

Deleted: If data are no longer relevant for the purpose collected, they should be deleted, unless subsequent processing is possibl...

Deleted: S

Deleted: S

Deleted: , 4 years later the evidence based solely on

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 also 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 the integrity of the data 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 the 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, dependent upon who is receiving the data, whether it is the police, another public body or a private party. 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 law or agreements that allow the communication

The police can share data with other police organisations if the personal data is relevant for the purpose of 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 communication of personal data in general should be in line with the General considerations describe above.

Deleted:

Deleted: revision

Deleted: When shaping internal policies i

Deleted: This uses a

Deleted: to

Deleted: if feasible

Deleted: As a general rule p

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

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 is 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 criminal data, which are considered sensitive data could result in negative discrimination against 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 was 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 share 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 which should provide 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 they communicate with an airline about stolen or lost travel documents or when the police release details of persons wanted who are 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

Deleted: m

Deleted: 0

Deleted: the communicated data

Deleted: be used for non-law enforcement purposes

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

Deleted: missions

Deleted: organisations

handling contained within its legal framework, 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 in respect 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 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) maybe taken into account[4] so as to ensure that any transfer of data is legally justified and has in place appropriate safeguards. The request should clearly state all necessary elements from the requesting party to enable to 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.

Deleted: ,

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

Deleted: can be applicable

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

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

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 it has 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 to and from a private body from and to police 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

Deleted: police

Deleted: residing

Deleted: the

Deleted: the fact that

[4] 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

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 data controller has a double obligations 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: because of the length of the procedure

Example: In an investigation carried out in 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

As 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 data or transferring it is always advisable to double-check the quality of data, if it is correct, up-to-date, complete. As far as possible, in all communications of data, judicial decisions, as well as decisions not to prosecute, should be indicated and data based on opinions or personal assessments cheked at source before being communicated and their degree of accuracy or reliability indicated. It seems to be preferable to establish secure channels of transfers 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 contains incorrect data (personal or otherwise) are sent it can 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.

Deleted: is sent

16. Safeguards for communication

It is of the 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 safely communicated if it is in the interest of the data subject or for humanitarian reasons or is necessary to prevent serious and imminent risk to public order and 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: only

Deleted: is

Deleted: and if the processing is based on law,

Deleted:

Deleted: ,

Deleted: or public security

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 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 crime type.

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 have direct access to files of other police or non-police bodies they must only access and use the data if domestic permits which should reflect the key data protection principles.

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 of 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 therefore should not be processed by police. Access in this case to 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 subject of any data breach which may affect them shall also be ensured without undue delay.

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 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: in

Deleted: accordance with

Deleted: legislation

Deleted: <#>Data subject's rights¶
¶
The right to information, the right of access, the right of rectification and the right of erasure are interdependent rights. The right to information covered under point 4 is a prerequisite to right of access; the data subject has the right to know about the data processing which is made on their data and on the basis of this information, exercise other rights. The data controller should ensure that all types of data processing are notified to the public along with any relevant details on data processing as prescribed under point 4. The supervisory authority can assist in ensuring that the necessary information is made public.¶
¶
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 the communication.¶
¶
Example: If a data subject asks the police on data it processes on them, the police, if no exception is applicable, should give a detailed answer with legal references but in a plain language.¶
¶
Accessing data is a fundamental right for the data subjects in relation to their personal data. As a rule domestic law should, ideally, provide for direct access. ¶
¶
The right of access (as the right to information) 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 or excessive. The police can also refuse to respond to such manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a 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 ...

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

Privacy-by-design concept can be 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 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 users to better protect their 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 which includes political, financial functional and operational independence are decisive factors as wel when judging how independent the supervisory body is.

Deleted: is

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: 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:

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;

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 sensitive 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;¶