



Strasbourg, 8 September / septembre 2017

T-PD(2017)16

**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

AUSTRIA / AUTRICHE	2
BELGIUM / BELGIQUE.....	17
CZECH REPUBLIC / REPUBLIQUE TCHEQUE	20
FRANCE	36
GERMANY / ALLEMAGNE	53
IRELAND / IRLANDE	69
ITALY / ITALIE	75
EUROPEAN COMMISSION / COMMISSION EUROPEENNE	91
PORTUGAL.....	107
EUROPEAN DATA PROTECTION SUPERVISOR / LE CONTRÔLEUR EUROPEEN DE LA PROTECTION DES DONNEES (EDPS).....	110
INTERNATIONAL COMMITTEE OF THE RED CROSS / COMITÉ INTERNATIONAL DE LA CROIX-ROUGE (ICRC / CICR).....	126
INTERPOL.....	142
NATIONAL INSTITUTE FOR TRANSPARENCY, ACESS TO INFORMATION AND PERSONAL DATA PROTECTION / INSTITUT NATIONAL DE TRANSPARENCE, ACCES A L'INFORMATION ET PROTECTION DES DONNEES DU MEXIQUE (INAI).....	143

AUSTRIA / AUTRICHE

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 survey¹ 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 clear guidance on what the principles imply at an operational level.

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 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 the rights of the individual to privacy and data protection.

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

Deleted: use of personal data

Deleted: the

General considerations

All processing of personal data has to comply with the necessity, proportionality and purpose limitation principle. Accordingly, personal data processing by the police should be based on predefined, clear and legitimate purposes. Moreover, data processing should be necessary and proportionate and should always be in compliance with the original purpose. The data processing should be carried out lawfully, fairly and in a transparent manner. Furthermore, it should be adequate, relevant and non-excessive in relation to the purposes. Finally the processed data should be accurate and up-to-date in order to ensure the highest data quality possible.

Deleted: data

Deleted: s

Deleted: This implies

Deleted: that

Deleted: within

Deleted: that it

Deleted: to these legitimate purposes

Deleted: I

Deleted: furthermore

Deleted: which are processed within the police

Deleted: and

Deleted: Where

Deleted: is used in the text, it can be taken to mean wider

Deleted: same

Deleted: should

Deleted: limited to that which is

Deleted: and

Deleted: and

Deleted: and

Deleted: where personal data is processed

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. The used term ‘police’ also applies to law enforcement authorities, and/or other public and/or private bodies which are authorised by national law to process personal data for the mentioned purposes.

2. Collection of data and use of data

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

¹ See Report “[Twenty-five years down the line](#)” – by Joseph A. Cannataci.

The collection and use of personal data for law enforcement purposes can cause an interference with the right to private life and data protection enshrined in Article 8 of the European Convention on Human rights and by Convention 108. Therefore, the collection and use of personal data must be based on law, pursue a legitimate objective and be limited to what is necessary to achieve this legitimate objective.

Deleted: constitute ...ause an ...

Before and during the collection of personal data the question whether the relevant personal data are necessary for the investigation should always be asked. During the collection, provided that all legal requirements are met, larger scale of personal data can be processed. Nevertheless, after the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be deleted.

Deleted: Prior to...efore and during ...

Police should apply the data-minimisation principle at all stages of their work and should not continue to process personal data which are no longer needed. Accordingly, personal data collected at an early stage of the investigation, which then prove to be irrelevant, should no longer be processed (e.g. the innocence of a suspect is confirmed).

Deleted: processing ...nd should no ...

Before collecting any personal data, investigators should ask themselves the question 'Why is it necessary to acquire these particular data?' and 'What, exactly, do I want to achieve with these data'?'

Deleted:'What, exactly, do you ...

Example -Telephone Billing: ▾

In the beginning of an investigation it may be necessary to collect all phone numbers listed on a telephone bill in order to get an overview of the suspect's social environment. However, after it becomes clear that some phone numbers are not necessary for the purpose of the investigation they should no longer be kept or processed.

Deleted: For personal data such as ...

Deleted: A list ...ll of ...hone number ...

According to the purpose limitation principle, personal data collected for police purposes should be used for these purposes only and should not be used in any other way that is incompatible with the original purpose at the time of collection, unless this is provided by law (see Article 9 of Convention 108). The term "subsequent use of data" means a new data processing operation which has to fulfil all the criteria and conditions applicable to the collection and the use of data.

Deleted: those ...hese purposes on ...

Example: Personal data collected by the police in connection with a car theft cannot be used to determine the political affiliation of the concerned persons.

Deleted: olice...data collected by ...

3. Subsequent use of data

Every subsequent processing of data by police must comply with the applicable legal requirements for the processing of personal data.

Deleted: (irrespective of the fact that the original processing has been carried out for police purpose or for other purposes)...must meet ...ompl ...

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. Personal data that are subsequently used must be linked to a police purpose and must fulfil the criteria and conditions set out in point 2. The general rule is that all personal data processed by police should have a link to a case or a specific task and should be processed in relation to this.

Comment [001]: The meaning of this sentence is not clear.

Deleted: This means that p...ersona ...

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 international good practice and to enhance their exchange of information on the matter with other police bodies. This does not represent any obstacle to the use of data of these persons for police purpose if all legal requirements as put forward in point 2 are met.

Deleted: It should be noted however, that any subsequent use of personal data, in particular in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.¶

Comment [002]: The meaning of this sentence is not clear.

Example - Biometric data taken for immigration purposes can be processed by the police in connection with a robbery if the relevant law allows such processing.

Deleted: for law enforcement use (such as checks against persons wanted for serious ...)

4. Providing information to data subjects

One of the most important obligations of a data controller is to provide data subjects with information. This obligation is two-fold: Firstly, the data controller has to inform the public on its data processing. Secondly, the data controller - upon request of the data subject - has to provide specific information in regard to the processed personal data.

Deleted: a ... data controller is to ...

In general the data subject should be informed about details such as the name and contact details of the data controller and/or data processor, the recipients of the data, the categories of personal data processed, the purpose and the legal basis of the data processing and his/her rights.

Deleted: The general obligation implies that, in principle, ...n general ...

The information provided to the public, should promote awareness, inform the public in general of their rights and provide clear guidance on exercising their rights. Furthermore, the information, should include details about the conditions under which exceptions apply to the data subject's rights and how data subjects can submit an appeal against such a decision.

Deleted: the wider...he public, in ...

Websites and other easily accessible media can play an important role to inform the public. It is recommended to provide letter templates in order to help data subjects to exercise their rights.

Deleted: perform ...an play an ...

In regard to a request for access, the data controller has to inform the data subject as to whether or not personal data concerning him/her are being processed. The information should be provided in clear and plain language.

Deleted: ¶ According to the second obligation of giving data subject specific information regarding their data upon ...n regard ...

The national law can provide that the right to be informed may be limited, in cases where, providing such information would jeopardize the investigation, an important police task, a state interest (such as public security, or national security) or the protection of the rights and freedoms of others. However, withholding information of data processing should be used only sparingly and where it can be clearly justified.

Deleted: should...providing such ...

Example - For the purpose of covert monitoring data processing and long-term data retention may be justified without informing the individuals 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.

Deleted: of a high risk sex offender, ...

5. 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, and they constitute a necessary and proportionate measure in a democratic society. The exceptions have to be incorporated into national legislation in a manner compatible with the ECtHR jurisprudence.

Comment [003]: This seems to far. Exceptions should only refer to the data subject's rights but not to the data protection principles in general.

Deleted: (should be public, open and transparent and in addition detailed enough)

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 17) in case of some specific data processing activities. In particular it affects those 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 or the protection of the rights and fundamental freedoms of others. Other applicable exceptions are foreseen in Article 3 Convention 108.

If the police decides to refer to such an exception, it should be done for a legitimate objective and only when necessary and proportionate. Moreover, it should be limited to cases where data subject's rights would endanger the prevention, investigation or prosecution of criminal offences or the execution of criminal penalties or other tasks of the police.

Deleted: , based on national law is used by the police ...it should be use ...

Example - The data subject's right to information can be limited if this information will endanger the safety of a witness or an informant.

Deleted: I...f this giving

Example: Police data can be shared with national security agencies to prevent a terrorist attack. In order to identify the perpetrator quickly, police shall cooperate actively with national security agencies following a special procedure which takes into account the imminent risk of other individual's life and physical safety, as well as the security of personal data stored on identified suspects. However, if there is no risk of a 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 (such as judicial authorisation, stricter rules on purpose limitation) in order to ensure an enhanced protection to the individual's right to privacy and data protection.

Deleted: in respect of national security, for example ...to prevent a

Comment [004]: What is the connection here? Or does this refer to data protection?

Deleted: with national security agencies... However, if there is no

6. Use of special investigative techniques

The police should always use the least intrusive data processing methods. If less intrusive methods are available, these 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.

Deleted: ¶

Deleted: adopt ...se the least intrus

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, those considerations have to be balanced with cost-effectiveness and efficiency.

Deleted: ...however...however, it m

Example: The evidence for communication between two suspects can be gathered in various ways. If the same result can be achieved by interrogating the suspects this method should be preferred to the use of more intrusive covert surveillance measures, such as wiretapping.

Deleted: In an investigation, t...he

7. Introduction of new data processing technologies

When new technical methods for data processing are introduced, a Regulatory Impact Analysis should be carried out which should take into account the compliance with existing privacy and data protection standards.

Deleted: It is advisable w...hen new

If the processing is likely to result in a high risk for data subjects the data controller should perform a Data Protection Impact Assessment (DPIA) to assess all risks for the envisaged actions. The DPIA should not be static, but should take into account a specific case and should relate to every stage of the data processing activity. The relevance of the conducted DPIA shall be checked periodically.

Deleted: to the individual's rights...c

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 plays an important role when advising which safeguards should be introduced to ensure that any technical means comply with data protection law. Even though there is no obligation to consult the supervisory authority when introducing new technology, the data controller should consult the supervisory authority if the DPIA demonstrates a significantly high risk to the individual's rights.

Deleted: has ...lays an important ro

The focus of the data controller should be on mitigating the specific negative impacts that the data processing would represent to the right to privacy and to data protection.

Deleted: During the process with the supervisory authority the

The consultation between the supervisory authority and the data controller should be defined in a way that the supervisory authority is provided with sufficient opportunity to give its reasoned opinion and assessment of the data processing activities of the data controller.

Deleted: provides ...he supervisory

During the consultation process police should provide appropriate details to the supervisory authority, in particular regarding the categories of personal data, the data controller, data processor, the legal basis and the purpose of the data processing, and by whom the data are being accessed as well as information on retention of data, log policy and access policy.

Example: Detailed information regarding the set-up of a national reference file, containing fingerprint data such as purpose, data controller etc. should be reported to or made available to the data protection authority. The Data protection authority is preferably to be consulted during the legislative procedure.

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

Example - Introducing an automatic facial recognition system would need consultation in order to obtain a clear picture of the risks to data subjects. 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 glasses which are directly linked to relevant databases should not be directly connected to a national criminal record data base; the glasses should only collect information which should then be downloaded to a secure IT environment for further analysis.

Big data and profiling in the police

Technological advances in processing and analysing large and complex data sets as well as big data analytics present opportunities and challenges for the police.

Big data technologies enable bulk collection and analysis of a vast quantity of data with other bulk data. This could potentially and inadvertently interfere with the right to privacy and data protection.

The Council of Europe's Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data² can also be of use for the police.

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 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 take due account of 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 traditional methods of investigation.

- Deleted:** should be provided
- Deleted:** type
- Deleted:**
- Deleted:** file
- Deleted:** , the type of data contained
- Deleted:** is
- Deleted:** on
- Deleted:** s
- Deleted:** containing fingerprint data are to
- Deleted:** any
- Deleted:** by the data protection authority
- Deleted:** individual's rights
- Deleted:** Where needed, s

- Deleted:** used by police
- Deleted:** is
- Deleted:** they
- Deleted:** gather
- Deleted:** is
- Deleted:** to
- Deleted:** leading to big data
- Deleted:** and
- Deleted:** to
- Deleted:** who are turning to digital sources and profiling techniques to perform their legal tasks
- Deleted:** generated by electronic communications and devices aggregated
- Deleted:** in the context of Big Data analysis
- Deleted:** use too

² Document T-PD(2017)1

- Its use is necessary and proportionate for police purpose.
- 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.
- Where possible, 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 compatible purpose the data controller should make the data subjects aware of this secondary use.
- Lawfulness of the processing and compliance with the conditions set by Article 8 ECHR should be demonstrated.
- An information security policy should be in place.
- 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.

8. 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 nature, 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. However, sensitive data can be processed in order to protect the vital interest of the data subject or of another person.

- Deleted: S
- Deleted: however,
- Deleted: would

A careful balance of interests is necessary to determine whether or not and to which extent the police can 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 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. criminal investigation) can be achieved in a less intrusive manner and/or if the processing of special categories of data represents a risk of discrimination.

- Deleted: that impacts less on the right to privacy and data protection of the data subject
- Deleted: does not
- Deleted: for the data subject
- Deleted: these

Regarding special categories of data, profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subject. 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 habitants are from the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

Example - Targeting groups or individuals based solely on religious beliefs would not be allowed. However, where a group of individuals engaging in possible terrorist activities that were attached to a particular religious group is investigated, it could be of importance to process data specific to the followers of this 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 they are members of this religion, would be strictly prohibited.

- Deleted: in an investigation into
- Deleted:
- Deleted: to
- Deleted: were
- Deleted: that
- Formatted: English (U.S.)

9. Storage of data

As pointed out in Point 2 data shall only be processed until they have served the purpose for which they were collected. If data are no longer relevant for this purpose, they should be deleted, unless subsequent processing is possible on the grounds put forward in Point 3. Stored data should be accurate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

- Deleted: the
- Deleted: collected
- Deleted: adequate

There should be a clear distinction in how police store 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 were collected. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

Deleted: was

Deleted: ,

Deleted: ,

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 necessary for the purpose of prevention, investigation or prosecution of criminal offences and execution of criminal penalties or where personal data are processed for the purpose of the maintenance of public order.

Deleted: to achieve

Deleted: the

Deleted: and

Deleted: and

Deleted: is

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, 4 years later the evidence based solely on this data could possibly be considered as unlawful by the court.

General data retention periods are usually laid down 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 foresees a 4 year data retention period but the person 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 revision of the case have also expired. Likewise, if, after 4 years, the investigation is still on-going and his/her data is still relevant to it, the police should be able to retain it.

Deleted: regulated

Deleted: prescribes

Deleted: individual

Deleted: their

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 stored data are accurate and that the integrity of the data is maintained.

Deleted: that are stored

When issuing internal policies, international obligations, bilateral agreements and mutual legal assistance between member states and third countries should be taken into account.

Deleted: shaping

Deleted: which include providing data to international bodies such as Europol, Eurojust and INTERPOL

Deleted: must

Deleted: observed

Deleted: uses a classification system to

Deleted: and how

Deleted: reliable

Deleted: it is

Deleted: C

Deleted: it is to be communicated

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. This will facilitate the assessment of the quality of the data which helps assessing their reliability. The classification of data is also important when communicating them 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 (if feasible: 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.

10. 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. As a general rule police can 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: ,

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

The police should only share information domestically 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.

Deleted: , domestically,

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

Deleted: and

Deleted: and

Deleted: and

Deleted: is

Deleted: T

Deleted: in general

In general, the communication of personal data should be subject to the principle of necessity and proportionality and has to serve the above mentioned purposes.

Deleted: d

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 it materially assist the investigation.

Deleted: doing so will

11. 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).

Deleted: mutual

Stricter principles than those set out in Point 10 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the communicated data could be used for non-law enforcement purposes.

Deleted: forth

As an exception, communication 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.

12. 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, in order to protect the vital interests of the data subject or another person, or if it is necessary to prevent serious and imminent risk to public order or public security. There might also be instances where police data

Deleted: ,

Deleted: missions

Deleted: ,

Deleted: the interest of the data subject, for humanitarian reasons

Deleted: For example, t

may be communicated to humanitarian organisations based on international law, in order to protect the vital interests of the data subject or another person,

Where the police shares data with the media, special consideration should be given if this is necessary and in the public interest,

Such communication should only be done 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.

13. International transfer

Any international transfer of police data, should be limited to police organisations, should be necessary and in accordance with the law. In this respect, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data 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.

Before sharing any data, consideration should be given as to whether the receiving authority is performing a function conferred to it by law in regard to the prevention, investigation, or prosecution of criminal offences, the execution of criminal penalties or the maintenance of public order or whether the sharing of the data are 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 basic rules in regard to international transfers. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. Such transfer should be a last resort option. International transfers framework such as Interpol's "Rules Governing the Processing of Data and its 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) can be consulted³ to ensure that any transfer of data is legally justified and has in place appropriate safeguards. A request should clearly state all necessary elements to enable the receiving party to make a sound decision. These elements should include the reason for the request as well as the purpose of the transfer,

An appropriate level of data protection has to be guaranteed if data are to be transferred to countries not participating in Convention 108.

If the sending authority stipulates conditions on the use of the personal data transferred this should be communicated to the receiving state. The sending and the receiving states should be in agreement on the use of the data throughout its lifecycle.

Example - Further onward transfer of personal data should only be allowed if this is necessary for the same specific 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 with 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 requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) are met and if country X consents to the transfer. If the data is sent to country Z which is a non-member of the Convention 108, country Y should ascertain that this country

³ This is without prejudice to the power of the Committee of Convention 108 and of other bodies, to assess and to review, if necessary, the level of data protection guaranteed by multilateral agreements.

- Deleted: ,
- Deleted: the interest of the data subject or for humanitarian reasons
- Deleted: in respect of making ...
- Deleted: to the assessment to ...
- Deleted: it
- Deleted: that such publicity is allowed
- Deleted: internationally
- Deleted: and
- Deleted: fit for purpose
- Deleted: For this
- Deleted: ,
- Deleted: ,
- Deleted: When considering
- Deleted: in
- Deleted: related
- Deleted: ,
- Deleted: and
- Deleted: and
- Deleted: is
- Deleted: ,
- Deleted: the relevant
- Deleted: respect of
- Deleted: This means of
- Deleted: used
- Deleted: s
- Deleted: applicable
- Deleted: as
- Deleted: The
- Deleted: from the requesting party
- Deleted: to
- Deleted: on the request
- Deleted: details would be expected to
- Deleted: for
- Deleted: of data
- Deleted: should
- Deleted: there are conditions applie ...
- Deleted: in relation to the use of the ...
- Deleted: adhered to
- Deleted: above
- Deleted: then
- Deleted: right
- Deleted: instances
- Deleted: having such power
- Deleted: those

has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

Deleted: ...in place, ...

The international transfer of personal data to a non-police body is only exceptionally permissible in individual cases if this 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.

Deleted: permissible exceptionally a ...

Comment [005]: The meaning of this sentence is not clear.

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 police data to a private body should in general be avoided. It should only be done in exceptional cases when laid down by law and where the gravity of the crime, its trans-border nature and the fact that the involvement of the local police would compromise the purpose of the investigation. Other factors, such as data security, the reassurance to transfer the data, and the lawfulness of the data transfer in the receiving country have to be taken into consideration. The local police should be informed afterwards. In regard to this type of transfer, the police should make use of existing international legal instruments.

Deleted: residing in a different jurisdiction ...ould in general be ...

Comment [006]: The meaning of this sentence is not clear.

Example: In an investigation carried out in the framework of an international multilateral agreement, in regard to child sexual exploitation the victim lives 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.

Deleted: into ...n regard to child ...

Comment [007]: This example seems in respect to data protection rather irrelevant.

14. 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, and complete.

Deleted: , ...and complete. The qua ...

Example: The transfer of personal data which contain incorrect data can adversely affect the investigation and moreover, the relevant person. This may lead to a claim for 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: If personal data is sent th ...

15. Safeguards for communication

It is of the utmost importance that any communication meets the necessity and purpose limitation principle.

Deleted: the ...ny communication ...

Any personal data communicated should not be used for anything other than the purpose for which it was sent or received. The only exception to this is when the sending authority, based on legal provisions, agrees to any further use and if this further processing is based on law and is necessary and vital for the recipient to fulfil their task, to protect the vital interests of the data subject or another person, or is necessary to prevent serious and imminent risk to public order or public security and an appropriate level of data protection is guaranteed by the recipient as foreseen by Convention 108.

Deleted: gives agreement ...grees t ...

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 in the country Y to investigate the religious beliefs or political activities of the suspect (unless it would be relevant to the crime, and the police in country X has given its consent for this use as well).

Deleted: as profiling on the ...

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

In specific circumstances the police may seek to cross-reference its information with other data controllers and processors, or to combine personal data stored in different files or in different databases that are held by other public bodies and/or private organisations.

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 they must only access and use the data in accordance with domestic legislation 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 proportionate.

Example - Data held for citizenship purposes can only be used in a police 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 which is why such information should not be processed by police.

17. 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 which was explained under point 4 is a prerequisite to the right of access; the data subject should know which personal data concerning him or her are being processed, for which purpose, and how he or she can exercise his/her rights. The data controller should ensure that all types of data processing are communicated 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 right of access is fundamental, hence domestic law should, ideally, provide that the right of access is exercised directly.

The police should aim to give its answer in plain language.

Example: If a data subject asks the police which personal are processed concerning him, the police, if no exception is applicable, should give a detailed answer with legal references but in a plain language.

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

In respect of direct access, the data subject can request access to his/her data. The data controller will assess the request and any possible restriction and reply directly to the data subject. In case of a restriction, the data subject still has to have an answer.

If the right of access is indirect, the data subject may direct their request to the supervisory authority, which will carry out the request on behalf of the data subject. In the same vain, the supervisory authority may conduct checks regarding the lawfulness of the processing. The supervisory authority will then reply to the data subject. In case of a restriction, the same communication should be made possible as in case of a direct access.

Deleted: collect data by coordinating

Deleted: .

Deleted: Furthermore it may

Deleted:

Deleted: 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.

Deleted: have

Deleted: n

Deleted: of

Deleted: therefore

Formatted: English (U.S.)

Deleted: covered

Deleted: has the right to

Deleted: about

Deleted: the data processing which is made on their data and on the basis of this information,

Deleted: other

Deleted: notified

Comment [008]: The text does not say what kind of information the answer has to contain.

Deleted: answer

Deleted: even general questions arising from data subjects on the ...

Deleted: on

Deleted: data it processes on them

Deleted: Accessing data is a ...

Deleted: (as the right to information)

Deleted: ¶ ...

Deleted: I

Deleted: the controller of the files

Deleted: which can only be used if ...

Deleted: f

Deleted: restrict

Deleted: ion was to be used

Deleted: , albeit any answer should ...

Deleted: provided for

Deleted: after being properly ...

Deleted: their

Deleted: and

Deleted: availability and

Deleted: data subject's personal data

Deleted: (providing what data it is ...)

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

Deleted: domestic

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

Deleted: to any data ...s granted as

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

Deleted: the data subject ...ccess

It is, however, advisable to refer to national legislation to ensure consistency in regard to this approach and to avoid suspects utilising this method to find out whether there is an on-going investigation into them.

Deleted: of

Comment [009]: The meaning of this sentence is not clear.

The data subjects should also have the right to rectify or delete any incorrect, excessive or irrelevant data relating to him or her.

Deleted: It is an essential right of t...

Comment [0010]: Maybe there should be subsection 17.2. The right to rectification and erasure.

However, in some cases, it may be appropriate to add additional or corrective information to the file.

Formatted: English (U.S.)

If personal data which are subject to correction or erasure were communicated elsewhere, the relevant authorities should be informed of the changes to be made.

Deleted: In...some cases,...it may k

All proposed changes should be supported by evidence. This means that if a data subject can prove that his/her data are incorrect the data controller shall not have a right of discretion whether to correct or delete them.

Deleted: the ...ersonal data which a

Deleted: I... a the ...ata subjects...

Comment [0011]: There is no connection between the two sentences.

It may be necessary for the police, as dealt with under point 5, not to give information to a data subject or grant the right of access, or the right of correction or deletion, in case where this would jeopardise an investigation.

Deleted: , ...or the right of correctio

However, the rights of data subjects should only be restricted, when absolutely necessary, whereas the relevant provisions should be interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis. Any refusal should be provided in writing. The response should contain a clear justification of the decision, whereas the data subject should also have the possibility to review the decision by an independent authority or a court.

Deleted: Restrictions to ...he rights

National law may provide that a data subject may obtain a copy of its police file. However, national law may provide in such case the oral communication of the contents.

Deleted: A... data subject may be

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

Deleted: it emerges ...hat the

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.

Example: If police sends a refusal letter it should contain the name, address, web address, etc. of the competent authority which has to deal with the complaint.

Deleted: all ...he competent

The data subject should have access to a court or tribunal in order to submit an appeal and have the reasons for refusal verified. The supervisory authority should have sufficient powers to examine the police file concerned and to communicate its findings of the assessment to the data subject.

Deleted: if they are not satisfied with the reply given by the supervisory authority or the independent 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 is not obliged to 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 decide 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.

18. Data security

The police must take appropriate security measures against risks such as accidental or unauthorised access to personal data as well as destruction, loss, use, modification or disclosure of personal data. The controller must immediately notify the competent supervisory authority of data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

Deleted: ,

Deleted: ,

Deleted: without delay, at least,

Deleted: those

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 of a database and/or an information system or network should be determined by a risk assessment. The more sensitive the data, the more protection is required.

Deleted: given to

Deleted: is

Deleted: are the

Deleted: greater

Deleted: the

Deleted: and

Authorisation and authentication mechanisms are essential to protect personal data, while 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.

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 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 is an integral part of security. Data protection and security may be embedded directly into information systems and processes 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 entire life cycle. This applies 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.

Deleted: S

Privacy-Enhancing Technologies (PETs)

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

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 or the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

National law should provide that supervisory bodies should have investigative and corrective powers. The supervisory authority should be able to investigate complaints and should have regulatory measures in order to impose sanctions where needed.

Deleted: for

Deleted: advisory

Deleted: ,

Deleted: enforcement

Deleted: to enable it

Deleted: ,

Deleted: to

Deleted: or to be able

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 tasks. A supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Deleted: The

Glossary/Definitions

For the purposes of this Guide:

1. "personal data" means any information relating to an identified or identifiable individual ("data subject");
2. "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;
3. "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;
4. "soft data" (evidence based on testimony) means data acquired through testimony of person involved in the investigation;
5. "hard data" (evidence based on documents) means data acquired from official documents or other certified sources;
6. "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;
7. "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;
8. "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;
9. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
10. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
11. 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.
12. "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.
13. "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.

BELGIUM / BELGIQUE

2. Collecte et utilisation des données

§3. Avant et pendant la collecte des données à caractère personnel, il faudrait toujours se demander si de telles données collectées sont nécessaires à l'enquête ou de la prévention et le maintien de l'ordre public. Au stade de la collecte, une plus large mesure de donnée à caractère personnel peut être traitée. Après la collecte, il faut impérativement procéder à une analyse approfondie pour évaluer quelles sont les données qui doivent être conservées et celles qui doivent être effacées.

Comment [0012]: L'ancien libellé prohibe que des données non liées à une enquête en cours soient collectées (si telle est la volonté, il conviendrait d'indiquer que cette recommandation s'applique à la collecte de multiples données relatives à une même personne (big data) – éviter que cela bloque ANPR p.ex.)

3. Utilisation ultérieure des données

§2. 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 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 toutes les données détenues par la police doivent avoir un lien avec une affaire ou une mission spécifique de la police et devraient être traitées en cohérence avec cette enquête ou mission spécifique.

Exemple : les données biométriques recueillies à des fins d'immigration peuvent être traitées, si la loi l'autorise, pour des utilisations répressives (telles que les contrôles des personnes recherchées pour un crime ou un acte terroriste grave). Toute utilisation doit être licite et proportionnée.

Comment [0013]: Le terrorisme est légalement défini mais le terrorisme « grave » est source d'insécurité juridique

4. Information des personnes concernées

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 des informations sur le traitement de ses données et la conservation prolongée de celles-ci, si l'on considère que ces informations peuvent nuire à l'enquête. 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.

Comment [0014]: Prévoir un type de réponse au cas par cas risque d'engendrer un manque d'uniformité et de permettre à un auteur présumé de déduire d'une absence de réponse qu'une enquête est en cours. Une réponse exhaustive et systématique, mais adressée exclusivement à la DPA est préférable

9. Conservation des données

§4. 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 les charges qui pèsent contre elle, ses données sont 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, s'il s'avère qu'au terme des 4 ans l'enquête est toujours en cours et que les données concernant cette personne restent pertinentes, la police devrait être en mesure de les conserver.

Comment [0015]: Le critère de l'acquittement est trop large. Il serait préférable d'indiquer « innocente ». Ceci implique que les décisions de justice soient systématiquement communiquées aux services de police.

11. Communication de données par des services de police à d'autres organismes publics

§2. Des principes plus stricts que ceux prévus au point 10 devraient être respectés lorsque des données sont transmises à d'autres organismes nationaux que des services de police, car la communication de ces données pourrait servir à d'autres fins qu'à des fins policières.

§3. A titre d'exception, la communication à une autre autorité publique peut également être autorisée si elle est prévue par la loi, si elle effectuée dans l'intérêt de la personne concernée, ou si elle est nécessaire pour éviter un risque grave et imminent pour d'autres personnes ou pour l'ordre public ou la sécurité publique.

Comment [0016]: Il s'agit d'une composante de l'ordre public. Il serait préférable d'indiquer « pour l'ordre public ou la sécurité intérieure de l'Etat »

12. Communication de données par la police à des organismes privés

§1. Il peut arriver que, dans des conditions strictes, la police ait besoin de 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. Ce type de communication ne devrait être effectuée qu'aux fins de l'enquête ou d'autres missions importantes de la police, 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.

Comment [0017]: idem

§2. Toute donnée communiquée ne devrait pas être utilisée à d'autres fins que celles pour lesquelles elle a été communiquée ou reçue. La seule exception à cela s'applique lorsque l'autorité expéditrice donne, sur une base légale, son accord pour une autre utilisation et si le traitement est prévu par la loi, est nécessaire et indispensable pour que le destinataire accomplisse sa tâche, est dans l'intérêt de la personne concernée ou pour des raisons humanitaires, ou encore est nécessaire pour prévenir un risque grave et imminent à l'ordre public ou à la sécurité publique et qu'un niveau approprié de protection des données tel que prévu par la Convention 108 est garanti par le destinataire.

Comment [0018]: intérieure de l'Etat ? voir commentaire précédent

16. Interconnexion des fichiers et accès direct (accès en ligne)

§3. 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 applicable le permet qui doit prendre en compte les principes fondamentaux de la protection des données.

Comment [0019]:

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 peut-être pas utile à une enquête et ne devrait donc pas être traitée par la police.

Comment [0020]: le texte ne devrait pas se prononcer sur la pertinence de ce genre d'information

Comment [0021]: distinguer plus clairement accès (consultation) et utilisation. Car l'accès à l'information du Registre national n'est pas disproportionné alors que l'importation de toutes les données pourrait l'être

17. Droits de la personne concernée

§1. 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, dans une mesure compatible avec ses missions, 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.

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 fournir une réponse claire, détaillée et citer des références juridiques pertinentes.

Comment [0022]: Mais pas nécessairement à la personne elle-même (cfr accès indirect)

Exemple : la demande d'accès peut être refusée si une enquête est en cours sur la personne concernée et que l'octroi d'un accès lui permette de compromettre l'enquête.

Toutefois, il est conseillé de se référer à la législation nationale pour veiller à ce que la réponse soit cohérente, et pour éviter que des suspects utilisent cette méthode pour savoir s'ils font l'objet d'une enquête en cours.

§14. Toutes les modifications proposées devraient être étayées par des éléments de preuve. Si les personnes concernées peuvent prouver au moyen de documents officiels du même pays 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.

Comment [0023]: Il ne s'agit pas d'un exemple. Il faudrait sortir cette phrase du cadre

Comment [0024]: Trop restrictif, potentiellement contraire droit de l'UE et au principe du guichet unique dans l'Union

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 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 survey⁴ 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 clear guidance on what the principles imply at an operational level.

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 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 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

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that data processing within the police should be based on predefined, clear and legitimate purposes that it 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. It should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally the data which are processed within the police 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 and the execution of criminal penalties and for the maintenance of public order, including prevention of threats to public security. 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.

Comment [0025]: reflects in general wording the latest EU data protection directive 2016/680

2. Collection of data and use of data

The collection and use 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 or the suspicion thereof) and where personal data is processed for the purpose of the maintenance of public order.

⁴ See Report "[Twenty-five years down the line](#)" – by Joseph A. Cannataci.

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 **explicitly based on law** (clear and publicly available), pursue a legitimate aim and be limited to what is necessary to achieve that legitimate aim.

Comment [0026]: Article 8 of directive 2016/680

Prior to and during the collection of such data the question of whether the personal data collected **may be relevant**, for the investigation **or other abovementioned police task** should always be asked. During collection, provided that all legal requirements are met, larger scale of personal data can be processed.

Comment [0027]: Especially, but not exclusively, in the initial stages there is little guidance as to what data would be shown to be important later on.

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: is necessary

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?'

Comment [0028]: Seldom the police may be sure what data will be needed until a judicial procedure has run its course. The sentence should be rephrased to focus on data that clearly are no relevant to the case, but as that appears in next paragraph, perhaps this one should be deleted.

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 the relevant people.

Deleted: After the collection phase

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.

Deleted: a thorough analysis is needed in order to assess which data are to be retained and which are to be deleted.

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 at the time of collection, unless this is provided for in law (see Art 9 of Convention 108). Subsequent use of data is considered for the use of this guide as a new data processing operation which has to fulfil all the criteria and conditions applicable to the collection and the use of data.

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

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) must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be necessary and proportionate to the legitimate aim pursued.

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 personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set in point 2. The general rule is that 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.

It should be noted however, that any subsequent use of personal data, in particular in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.

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 international good practice and to enhance their exchange of information on the matter with other police bodies. This does not represent any obstacle to the use of data of these persons for police purpose if all legal requirements as put forward in point 2 are met.

Example - Biometric data taken for immigration purposes can be processed for law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Any such use should be lawful and proportionate.

4. 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 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 *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 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.

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. Information provided should include details about the conditions under which exceptions apply to the data subject's rights and how they can submit an appeal against a decision of the data controller in reply to their request.

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. In respect of making information available which highlight data protection and data subjects' rights, this is the responsibility of the data controller to provide.

According to the second obligation of giving data subject specific information regarding their data upon request for access, the data controller has to inform the individuals on the data processing activities that it has pursued with their data. This means that if an individual has its data collected during the course of an investigation, as soon as circumstances safely permit, the police should advise the individual of the data processing if there is such request. The information should be provided in clear and plain language.

The law can provide that the right to be informed may be limited, should providing such information, prejudice the investigation, or another important police mission, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding notification of data processing however should be used only sparingly and where it can be clearly justified.

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 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.

5. 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 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 2,3,4,7 as well as to the data subjects' rights (point 17) in case of some specific data processing activities. In particular it affects those 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 or the protection of the rights and fundamental freedoms of others. Other applicable exceptions are foreseen in Article 3 Convention 108.

If the exception, based on national law 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 the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police.

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 can be shared with national security agencies in respect of national security, for example to prevent a terrorist attack. In order to rapidly identify the perpetrator, police shall cooperate 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 security agencies. 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 (such as judicial authorisation, stricter rules on purpose limitation) with a view of ensuring an enhanced protection to the individual's right to privacy and data protection.

6. 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 reasonably achieved by less intrusive methods.

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, those considerations have to be balanced with cost-effectiveness, use of resources and 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 covert surveillance measures, such as wiretapping.

7. Introduction 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.

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, continuous (i.e. repeated at reasonable intervals) and that it should touch upon every phase of the data processing activity. The relevance of the DPIA shall be checked by 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.

Comment [0029]: Sometimes, the less intrusive methods are not excluded in principle, but cannot be relied upon to be effective. For example, policemen could disseminate the photograph of a lost child in areas where it likely was or could be seen, but with much less efficiency than broadcasting it regionwide on TV.

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.

During the **consultation** 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.

Comment [0030]: clarification and link to next paragraph

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 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 contained and by whom the data is being accessed as well as information on retention of data, log policy and access policy.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data are to be reported to or made available to the data protection authority. 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 would need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed, 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 which is directly linked to relevant databases 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.

Big data and profiling 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 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 potentially and inadvertently interfere with the right to privacy and data protection.

The Council of Europe's Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data⁵ 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:

⁵ Document T-PD(2017)1

T-PD (2017)16

- 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 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 take due account of 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 traditional methods of investigation.
- Its use is necessary and proportionate for police purpose.
- 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.
- Where possible, 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 compatible purpose the data controller should make the data subjects aware of this secondary use.
- Lawfulness of the processing and compliance with the conditions set by Article 8 ECHR should be demonstrated.
- An information security policy should be in place.
- 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.

8. 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. While certain such categories, such as personal data related to offences and criminal proceedings, or biometric data, need to be processed frequently, appropriate 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.

Comment [0031]: To recognize the usual nature of police work.

Deleted: S

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 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. criminal investigation) 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, profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subject. 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 habitants are from the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

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 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.

9. Storage of data

As pointed out in Point 2 data shall be processed until they have served the purpose for which they were collected. 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. 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 or designate 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. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

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 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, 4 years later the evidence 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. 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 revision of the case have also expired. Likewise, if, after 4 years, the investigation is still ongoing 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.

When shaping internal policies 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.

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. This uses a

Comment [0032]: Sometimes there are rules for storage applying equally (e.g. data on both the offenders on the one hand and victims and witnesses on the other hand are included within "live" formal criminal investigation case-file). Another word is also needed to cover the results of query results from (multiple) databases.

Comment [0033]: The example should probably be in a rectangle as are the others.

T-PD (2017)16

classification system to facilitate 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 (if feasible: 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.

10. 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. As a general rule police can 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 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.

11. 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 10 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the communicated data could be used for non-law enforcement purposes.

As an exception, communication 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.

12. 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 missions, 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.

13. International transfer

Any transfer of police data internationally should be limited to police organisations 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 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. 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 "Rules Governing the Processing of Data and its 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) can be applicable⁶ 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

⁶ This is without prejudice to the right of the Committee of Convention 108 and of other instances having such power to assess and to review, if necessary, the level of data protection guaranteed by those multilateral agreements.

T-PD (2017)16

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.

An appropriate level of data protection should be guaranteed if data are to be transferred to countries not participating in 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 with 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 has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

Comment [0034]: In practice, several institutions of a receiving state may be involved. E.g. the first transfer may be necessary to arrest the suspect, while the further transfer may be necessary e.g. to revoke the offender's security clearance, professional licence due to the offence committed and adjudicated.

Deleted: specific

The international transfer of personal data to a non-police 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 police data to a private body residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases where it is provided by legal means and where the gravity of the crime, its trans-border nature and the fact that the involvement of the local police would compromise the purpose of the investigation because of the length of the procedure. 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. 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.

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.

14. 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. The quality of data can be assessed up to the moment of communication.

Example: If personal data is sent that contains incorrect data (personal or otherwise) 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.

15. 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 only exception to this is when the sending authority, based on legal provisions, gives agreement to any further use and if the processing is based on law, is necessary and vital for the recipient to fulfil their task, is in the interest of the data subject or for humanitarian reasons or is necessary to prevent serious and imminent risk to public order or public security and an appropriate level of data protection is guaranteed by the recipient 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 as well).

16. 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 in accordance with domestic legislation 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 proportionate.

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.

17. 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.

T-PD (2017)16

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 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 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.

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 which can only be used if it is vital for the performance of a legal task of law enforcement 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. If restriction was to be used, the data subject still has to have an answer, albeit any answer should take into consideration according national law or practice all circumstances to which the restriction 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 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). In case of a restriction, 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.

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.

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.

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 giving a testimony in a criminal case.

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 same countries' 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 5, 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.

Restrictions to the rights of data subjects 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 refusals provided to 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 to retain 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.

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.

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 is not obliged to 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 decide 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.

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 may seriously interfere with the rights and fundamental freedoms of data subjects.

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.

T-PD (2017)16

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 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.

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 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 is an integral part of security. Data protection and security may be embedded directly into information systems and processes 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-Enhancing Technologies (PETs)

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

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 within the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

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.

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

Comment [0035]: In countries where strict division of powers into legislative, executive and judicial branch is constitutionally enforced, DPA would often be an independent part of the executive branch.

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:

14. "personal data" means any information relating to an identified or identifiable individual ("data subject");
15. "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;
16. "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;
17. "soft data" (evidence based on testimony) means data acquired through testimony of person involved in the investigation;
18. "hard data" (evidence based on documents) means data acquired from official documents or other certified sources;
19. "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

T-PD (2017)16

upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

20. "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;
21. "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;
22. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
23. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
24. 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.
25. "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.
26. "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.

FRANCE

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 étude⁷ 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 continuaient de constituer 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 clairs et concrets sur ce que ces principes impliquent au niveau opérationnel.

Le présent guide a donc été élaboré à cette fin. Il vise à 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 signale les principaux éléments à prendre en compte dans ce contexte.

Ce guide 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 lors de l'utilisation des données à caractère personnel dans le secteur de la police 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 à la protection de la vie privée et à la protection des données.

Pour faciliter la lecture du présent guide, un glossaire des termes utilisés est fourni à la fin du document.

Considérations générales

Le traitement de données devrait être entièrement conforme aux principes de nécessité, de proportionnalité et de limitation de la finalité. Cela signifie qu'il ne devrait être effectué par la police que dans un but prédéfini, précis et légitime, qu'il devrait être nécessaire et proportionné à ces fins légitimes, et qu'il devrait toujours être compatible avec la finalité initialement poursuivie. Il faudrait en outre que ce traitement soit assuré de façon licite, loyale et transparente, et qu'il soit adéquat, pertinent et non excessif par rapport aux finalités. Enfin, les données traitées par la police devraient être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées, ainsi qu'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, principalement aux fins de prévention, d'investigation et de répression des infractions pénales, d'exécution des sanctions pénales et du maintien de l'ordre public. 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.

2. Collecte et utilisation des données

La collecte et l'utilisation de données à caractère personnel à des fins policières devrait se limiter à ce qui est nécessaire à la prévention, l'investigation et la répression d'infractions pénales ainsi qu'à l'exécution de sanctions pénales (pour une infraction pénale déterminée ou la suspicion d'une telle infraction par exemple) et au traitement de données à caractère personnel ayant pour finalité le maintien de l'ordre public.

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

⁷ Voir le rapport « [Twenty-five years down the line](#) » de Joseph A. Cannataci.

Comment [0036]: Question terminologique qui vaut pour l'ensemble du document: l'emploi du conditionnel est-il approprié lorsque le guide pratique rappelle des principes qui constituent des obligations juridiquement contraignantes ? Ne serait-il pas plus approprié d'employer, dans ces cas, le présent de l'indicatif plutôt que le conditionnel, tout en faisant référence aux instruments juridiquement contraignants (CEDH, Convention 108), sans pour autant reproduire précisément les dispositions pertinentes (cf. introduction, al. 4) ?

Comment [0037]: L'exigence d'adéquation, de pertinence et de proportionnalité (non excessivité) devrait se rapporter aux données et non au traitement des données. Ce sont les données faisant l'objet d'un traitement qui doivent répondre à ces exigences et non le traitement en lui-même. Cf. rédaction de l'article 5, sous c) de la Convention 108, reprise à l'article 5§4, sous c), du projet de convention modernisée

Comment [0038]: Proposition de rédaction en conséquence du commentaire précédent.

Comment [0039]: S'agissant d'un projet de guide pratique, il serait utile de clarifier son champ d'application pour préciser les acteurs concernés: police judiciaire et police administrative ? L'investigation, la répression des infractions pénales et l'exécution des sanctions pénales sont des finalités de police judiciaire. La prévention des infractions pénales et le maintien de l'ordre public, qui peuvent conduire à la constatation d'infractions pénales, sont des finalités qui relèvent plutôt de la police administrative.

Field Code Changed

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.

Avant et pendant la collecte des données à caractère personnel, il faudrait toujours se demander si de telles données collectées sont nécessaires à l'enquête. ~~Au stade de la collecte, une plus large mesure de donnée à caractère personnel peut être traitée. Après la collecte, il faut impérativement procéder à une analyse approfondie pour évaluer quelles sont les données qui doivent être conservées et celles qui doivent être effacées.~~

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).

Avant de procéder à la collecte de données à caractère personnel, il convient de 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 découlant des factures téléphoniques : seuls le(s) numéro(s) nécessaire(s) à la période qui fait l'objet de l'enquête et uniquement pour la ou les personnes concernées ne devraient être demandés.

Une liste des numéros de téléphone de la ou des personnes impliquées dans l'infraction présumée peut être obtenue s'il existe des éléments qui indiquent que ces données peuvent servir à l'enquête, mais celles-ci ne peuvent pas être conservées ou traitées si l'analyse montre qu'elles ne sont pas nécessaires pour 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 du moment de la collecte, ~~sauf disposition contraire de la loi~~ (voir article 9 de la Convention 108). 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 applicables à la collecte et l'utilisation des données.

Exemple : les données collectées par la police dans le cadre d'une enquête ne peuvent pas être utilisées pour déterminer l'affiliation politique de la personne concernée.

3. Utilisation ultérieure des données

Tout traitement ultérieur de données par la police (indépendamment du fait que le traitement initial a été mené à des fins policières ou à d'autres fins) doit respecter les obligations ~~légales applicables au traitement~~ de données à caractère personnel : il devrait être prévu par la loi, être nécessaire et proportionné au but légitime poursuivi.

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, conformément aux principes de nécessité et de proportionnalité, dans le cadre des pouvoirs légaux conférés à la police. Cela implique que 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 toutes les données détenues par la police doivent avoir un lien avec une affaire ou une mission spécifique de la police et devraient être traitées en cohérence avec cette enquête spécifique.

Il convient toutefois de noter que toute utilisation ultérieure de données à caractère personnel, concernant notamment les personnes vulnérables, telles que les victimes, les mineurs, les personnes bénéficiant d'une protection internationale, devrait être fondée sur des bases légales solides et faire l'objet d'un examen approfondi, ~~au regard des principes de nécessité et de proportionnalité, qui devrait être assorti de la~~

Comment [0040]: On se focalise sur l'enquête, comme dans les alinéas suivants, ce qui concerne uniquement la police judiciaire et exclut la police administrative. D'où la nécessité de clarifier le champ d'application du guide pratique.

Formatted: Strikethrough

Comment [0041]: Cette phrase risque d'être contreproductive en admettant, par principe, que le test de la pertinence des données soit moins strict au stade de la collecte qu'ultérieurement. Il serait préférable de supprimer cette phrase

Comment [0042]: On revient à l'alinéa 3, 1^{ère} phrase du §2, au stade initial de la collecte. Ne serait-il pas préférable d'insérer cette phrase immédiatement à la suite, avant d'aborder le stade postérieur à la collecte à la fin de l'alinéa 3 et à l'alinéa 4 ?

Comment [0043]: A nuancer car l'article 9 de la Convention exige, pour déroger à ce principe, que la loi constitue une mesure nécessaire dans une société démocratique.

Comment [0044]: Problème de traduction en français. Ces obligations ne sont pas seulement légales, mais aussi conventionnelles (CEDH, Convention 108). Il serait préférable de parler des « règles applicables... »

Formatted: Strikethrough

Formatted: Strikethrough

Comment [0045]: Nouvelle phrase.

Comment [0046]: Cette phrase semble exclure la possibilité d'un traitement ultérieur à des fins historiques, statistiques et scientifiques.

possibilité de demander l'effacement de ces données. Dans les affaires concernant la traite des 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 et d'améliorer la façon dont ils échangent des informations sur la question avec d'autres services de police. Cela ne doit pas constituer un quelconque obstacle à l'utilisation des données de ces personnes à des fins policières si toutes les exigences légales, telles qu'énoncées au point 2, sont remplies.

Exemple : les données biométriques recueillies à des fins d'immigration peuvent être traitées, si la loi l'autorise, pour des utilisations répressives (telles que les contrôles des personnes recherchées pour un crime ou un acte terroriste grave). Toute utilisation doit être licite et proportionnée.

4. 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 communique des informations générales sur le traitement des données qu'il effectue, au public dans son ensemble, et 2) il donne aux intéressés qui en font la demande des informations spécifiques sur le traitement de leurs données à caractère personnel.

L'obligation générale suppose que, en principe, les personnes concernées reçoivent un certain nombre de renseignements, notamment le nom et les coordonnées du responsable du traitement, du sous-traitant et des destinataires, mais aussi des informations relatives à l'ensemble de données à traiter, la finalité du traitement des données, la base légale de ce traitement ainsi que des informations sur leurs droits. Il appartient à ceux qui communiquent ces informations de respecter un juste équilibre entre tous les intérêts concernés et de tenir compte de la nature particulière des fichiers ad hoc ou provisoires et des autres fichiers particulièrement sensibles, tels que les fichiers de renseignement en matière pénale, afin d'éviter de porter gravement préjudice à la police dans l'exercice de ses fonctions.

Les informations données de façon générale au public dans son ensemble devraient permettre de promouvoir leur sensibilisation, de les informer de leurs droits et d'assurer des orientations claires concernant les modalités de leur exercice. Les informations fournies devraient également préciser dans quelles conditions les droits des intéressés peuvent faire l'objet d'exceptions et comment ces personnes peuvent former un recours contre une décision prise, suite à une demande de leur part, par le responsable du traitement des données en réponse à leur demande.

Les sites internet et tout autre média facilement accessible jouent un rôle dans l'information du public. Il est recommandé, en guise de bonne pratique, 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.

Conformément à la seconde obligation consistant à donner des informations spécifiques relatives à ses données à la personne concernée, sur demande, il appartient, en principe, au responsable du traitement de l'informer, des activités de traitement réalisées sur ses données. En clair, cela signifie que si une personne voit ses données collectées au cours d'une enquête, la police doit, en principe, lui communiquer, dès que les circonstances le permettent, les informations sur les activités de traitement de ses données si une telle demande est faite. Les informations doivent être communiquées de manière claire et intelligible.

La loi peut prévoir une limitation au droit d'être informé si la communication de cette information peut être préjudiciable à l'enquête ou à une autre mission policière importante, aux intérêts de l'Etat (tels que la sécurité publique, la sécurité nationale) ou à la protection des droits et libertés d'autrui. Néanmoins, la non-communication d'informations sur le traitement des données ne doit être utilisée que de façon limitée et seulement lorsqu'elle peut être clairement justifiée.

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 des informations sur le traitement de ses données et la conservation prolongée de celles-ci, si l'on considère que ces informations peuvent nuire à l'enquête. 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.

Comment [0047]: Dans le prolongement de la jurisprudence de la CourEDH sur les fichiers de police. Voir, notamment, arrêts du 4 décembre 2008 (S. Marper/RU), du 17 décembre 2009 (BB ea.a./France), du 18 septembre 2014 (Brunet/France) et du 22 juin 2017 (Aycaguer/France).

Deleted: ¶

Formatted: Strikethrough

Comment [0048]: Cette rédaction tend à limiter l'obligation d'information spécifique (aux personnes concernées, et non au public en général), au droit d'accès (information suite à l'initiative des personnes concernées), en excluant systématiquement la possibilité d'une information spécifique à la seule initiative du responsable du traitement. Cette approche n'est-elle pas trop restrictive ? Ne revient-elle pas à empiéter sur les prérogatives des législateurs nationaux ? Les Etats peuvent apporter, par voie législative, des restrictions à l'obligation d'information, pour les nécessités de l'enquête etc... par exemple en limitant le droit d'information au droit d'accès.

Deleted:

Comment [0049]: Qu'entend on concrètement par «là» ?

Comment [0050]: Idem commentaire 13

Comment [0051]: Enoncé du principe contrebalancé par la précision, à l'alinéa suivant, de la possibilité d'apporter des limites à ce principe.

Comment [0052]: Cette obligation d'information vaut, en principe, dès la collecte

Comment [0053]: Idem commentaire 13

5. 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 (elle doit être publique, ouverte, transparente et suffisamment détaillée) et constituent une mesure nécessaire et proportionnée dans une société démocratique. Les exceptions doivent être intégrées au droit national de manière compatible avec la jurisprudence de la CEDH. Les exceptions peuvent être applicables aux principes décrits aux points 2, 3, 4, 7 ainsi qu'aux droits des personnes concernées (point 17) dans le cas de certaines activités spécifiques de traitement de données. Il s'agit principalement des 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 ou la protection des droits et libertés fondamentales d'autrui. L'article 3 de la Convention 108 prévoit que d'autres exceptions puissent être applicables.

Si une exception, fondée sur le droit national, 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. Les finalités dans lesquelles ces exceptions sont utilisées devraient être limitées aux cas où ces règles et principes risqueraient de mettre en danger la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales ou d'autres fins policières.

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.

Exemple : des données 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 activement en suivant une procédure spéciale qui prend en compte le risque imminent pour la vie et la sécurité d'autres personnes et échanger les données à caractère personnel recueillies sur des suspects avec les services de sécurité nationale. Mais s'il n'y a pas de risque d'attentat terroriste, la police devrait communiquer ses données aux services de sécurité nationale conformément à la procédure générale, bien établie en vertu de laquelle des garanties renforcées sont assurées (telles qu'une autorisation judiciaire, des règles plus strictes en matière de limitation de la finalité) en vue d'assurer une protection renforcée aux droits à la vie privée et à la protection des données des individus.

6. Utilisation de techniques spéciales d'enquête ~~spéciales~~

Formatted: Strikethrough

La police devrait toujours choisir les moyens les moins intrusifs de traitement de données durant ses opérations. Dans le cas où elle peut employer des méthodes moins intrusives pour aboutir au but recherché, elle doit les privilégier. 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.

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 réflexion sur des éléments tels que le rapport coût-efficacité, l'utilisation des ressources et l'efficacité.

Exemple : dans une enquête, les preuves de la communication entre deux suspects peuvent être recueillies de diverses façons. Si des interrogatoires, des témoignages 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 secrète, telles que les écoutes.

7. Introduction de nouvelles technologies de l'information

Lorsque de nouveaux moyens techniques de traitement des données deviennent opérationnels, il est conseillé de procéder à une analyse d'impact de la réglementation qui devrait tenir compte de la conformité des nouvelles mesures aux normes de protection de la vie privée et de protection des données.

Si le traitement est 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 continue (c'est-à-dire effectuée à des intervalles raisonnables), et vise chacune des étapes de l'activité de traitement des données. La pertinence de l'EIPD doit être contrôlée à intervalles raisonnables.

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.

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.

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 des renseignements appropriés 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 qui figurent dans le fichier et les destinataires des données. Il faut également fournir des informations sur la conservation des données et la politique applicable en matière d'enregistrement et d'accès.

Exemple : toutes informations détaillées, telles que la finalité ou le responsable du traitement des données, etc. sur les fichiers nationaux de référence qui contiennent des données sur les empreintes devraient être indiquées ou mise à disposition de l'autorité de protection des données. Il est préférable de consulter l'autorité de protection des données durant la procédure législative.

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 devrait faire l'objet de consultations pour que les risques encourus par les droits de l'intéressé soient clairement indiqués. S'il le faut, 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 de prendre 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 », directement reliées aux bases de données pertinentes, utilisées par la police ne doivent pas être directement liées à une base de données nationale des casiers judiciaires ; elles devraient recueillir des informations qui seront ensuite téléchargées dans un environnement informatique sécurisé pour analyses ultérieures.

Big data et profilage 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 police qui décident d'utiliser des sources d'information numériques et des techniques de profilage pour accomplir leur mission judiciaire.

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 potentiellement ou involontairement interférer avec le droit au respect de la vie privée et à la protection des données.

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 mégadonnées⁸ 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 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 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 entraîner une sévère 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 tenir dûment compte des considérations suivantes :

- la vérification de l'exactitude, du contexte et de la pertinence des données s'impose ;
- leur utilisation exige une obligation de rendre des comptes ;
- leur utilisation doit être combinée avec les méthodes d'enquête traditionnelles ;
- leur utilisation est nécessaire et proportionnée aux fins policières
- l'analyse prédictive nécessite notamment une intervention humaine pour évaluer la pertinence de l'analyse et des conclusions ;
- les lignes directrices en matière d'éthique élaborées au niveau national ou international devraient être prises en considération ;
- si possible, 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 compatible, il importe que l'organe responsable du traitement informe les personnes concernées de cette utilisation secondaire ;
- la légalité du traitement des données 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 une politique de sécurité des informations ;
- le responsable du traitement doit veiller à la loyauté du traitement des données à caractère personnel lorsqu'il sert de base à la prise de décisions qui ont des conséquences pour les intéressés et doit s'assurer que les voies administratives et judiciaires permettant de contester ces décisions existent.

Comment [0054]: Il serait utile de rajouter, « une décision affectant une personne ne pouvant être prise sur le seul fondement d'un tel traitement automatisé de données »

⁸ Document T-PD(2017)1

8. 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.

Un juste équilibre des intérêts doit être trouvé pour déterminer si la police est autorisée à traiter des données sensibles et dans quelle mesure. Il serait par exemple conseillé de différencier les situations dans lesquelles les données biométriques sont traitées par la police à des fins d'identification (auquel cas 2 empreintes digitales suffisent) ou dans le cadre d'une enquête pénale (auquel cas 8 à 10 empreintes digitales peuvent être nécessaires). Il est en outre recommandé d'utiliser davantage l'évaluation de l'impact sur la protection des données personnelles (EIPD) afin de s'assurer que des garanties appropriées sont mises en place de manière adéquate. Le responsable du traitement devrait démontrer après évaluation que la finalité du traitement (par exemple l'enquête pénale) ne peut pas être atteinte en utilisant un traitement moins attentatoire au droit au respect de la vie privée et à la protection des données de la personne concernée, et que le traitement de catégories spéciales de données ne présente pas un risque de discrimination pour la personne concernée.

En ce qui concerne ces données, le profilage devrait être évité en règle générale et ne devrait être autorisé que lorsque des garanties appropriées sont mises en place pour contenir le risque potentiel de discrimination ou d'effet juridique défavorable pour la personne concernée. Il peut s'agir notamment de mesures visant à éviter qu'une personne soit soupçonnée d'appartenir à une organisation criminelle parce qu'elle est assimilée à tous les habitants d'un quartier où une organisation criminelle est active et où les habitants ont la même origine ethnique. Il faudrait d'autres critères supplémentaires pour autoriser le traitement des données pour ce motif.

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 religieux (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 sera néanmoins interdit de cibler tous les adeptes d'une religion, seulement sur la base de leur appartenance.

9. 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 qui ne sont plus pertinentes de ce point de vue doivent être effacées, sauf si un traitement ultérieur fondé sur les motifs exposés au point 3 est possible. Les données conservées devraient être adéquates, actualisées, nécessaires, pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées.

Le classement 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. Il convient de mettre en place des garanties pour les personnes qui ne sont pas soupçonnées d'infraction pénale ou qui n'ont pas été condamnées pour une infraction pénale.

Comment [0055]: La rédaction pourrait « durcie » en s'inspirant de la directive 2016/680 :

- Considérant 38 : « tout profilage qui entraîne une discrimination sur la base de données sensibles devrait être interdit en application des articles 21 et 52 de la Charte » ;
- article 11§3 : « tout profilage qui entraîne une discrimination sur la base de données sensibles est interdit, conformément au droit de l'UE »

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 des données à caractère personnel en dehors du délai légal prévu pour la conservation peut constituer une violation grave du droit à la protection de ces données et que les éléments de preuve recueillis ainsi peuvent être considérés comme illégaux. Si la loi relative à un crime spécifique prévoit 4 ans comme période de rétention des données, et si l'individu est retenu par la police seulement sur le fondement 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 les charges qui pèsent contre elle, ses données sont 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, s'il s'avère qu'au terme des 4 ans l'enquête est toujours en cours 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 ce que la procédure judiciaire s'achève (c'est-à-dire [lorsque](#) 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.

Lors de l'élaboration de politiques internes, 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.

Il convient de classer les données 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 (si faisable ; 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.

10. 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. ~~Par principe, En général,~~ la communication de données entre services de police ne devrait 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 communiquer leurs informations que lorsque la demande qui leur en est faite est 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 qui autorisent la communication.

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 soumise au principe de nécessité et de proportionnalité et servir aux fins susmentionnées.

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.

11. 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 aux autorités publiques 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).

Des principes plus stricts que ceux prévus au point 10 devraient être respectés lorsque des données sont transmises à d'autres organismes nationaux que des services de police, car la communication de ces données pourrait servir à d'autres fins qu'à des fins policières.

A titre d'exception, la communication à une autre autorité publique peut également être autorisée si elle est prévue par la loi, si elle effectuée dans l'intérêt de la personne concernée, ou si elle est nécessaire pour éviter un risque grave et imminent pour d'autres personnes ou 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.

12. Communication de données par la police à des organismes privés

Il peut arriver que, dans des conditions strictes, la police ait besoin de 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. Ce type de communication ne devrait être effectuée qu'aux fins de l'enquête ou d'autres missions importantes de la police, 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.

Formatted: Strikethrough

Comment [0056]: L'énoncé de ce principe est le corollaire du principe de finalité : un fichier étant mis en oeuvre pour une finalité déterminée, explicite et légitime, il convient de s'assurer que seules les personnes qui concourent directement à cette finalité aient accès aux données qui y sont enregistrées

T-PD (2017)16

Lorsque la police communique des données aux médias qui diffusent des informations liées à une enquête publique, il importerait d'évaluer si cela est nécessaire et dans l'intérêt public qu'une telle publicité soit permise.

Cette communication devrait avoir lieu au cas par cas, être chaque fois clairement prévue par la loi qui devrait établir la procédure nécessaire (notamment la nécessité d'une autorisation spécifique) à suivre pour qu'une telle communication puisse se produire.

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.

13. Transfert international

Tout transfert international de données devrait être limité à d'autres services de police, être adapté au but poursuivi et prévu par la loi. Dans ce cadre, 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 (concernant 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 communiquer 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.

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. Elle doit notamment prévoir des garanties adéquates 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 appliqués⁹ 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 le motif de celle-ci ainsi que la finalité du transfert de données.

Un niveau de protection approprié des données devrait être garanti lorsque des données sont transférées des pays qui ne sont pas parties à la Convention 108.

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 précises 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

⁹ 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.

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 accepte le transfert. 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 dispose d'une protection juridique adéquate en matière de traitement des données à caractère personnel et garantisse un niveau approprié de protection des données à caractère personnel.

Le transfert international de données à caractère personnel à un service 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 de transfert 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.

Le transfert international de données policières à des organismes privés résidant dans une juridiction différente devrait être évité en règle générale. Ce type de transfert ne peut avoir lieu que dans des cas très exceptionnels dans lesquels cela est prévu par des voies légales et quand la gravité du crime, son caractère transfrontalier et la participation éventuelle de la police locale pourraient nuire à l'objet de l'enquête en raison de la durée de la procédure. 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 doivent être pris en compte. La police locale devrait en 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.

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 le matériel pédopornographique réside dans un autre pays (pays X), il existe alors un risque élevé que la personne quitte le pays X. Dès lors, la police du pays Y peut demander à un fournisseur de services 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.

14. Conditions de la communication

Le responsable du traitement a l'obligation générale de veiller à une haute qualité des données et devrait donc 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, de leur exactitude, de leur actualité et de leur exhaustivité. Cela peut être évalué jusqu'au moment de la communication.

Exemple : les données à caractère personnel qui sont envoyées contiennent des données erronées (données à caractère personnel ou non), cela peut négativement affecter l'enquête, causer préjudice à la personne concernée ou à d'autres personnes impliquées ou qui pourraient être impliquées 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 due à une mauvaise communication du nom du suspect porte gravement atteinte à plusieurs droits de l'homme de la personne concernée et peut affecter l'enquête pénale.

15. Garanties concernant la communication

T-PD (2017)16

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. La seule exception à cela s'applique lorsque l'autorité expéditrice donne, sur une base légale, son accord pour une autre utilisation et si le traitement est prévu par la loi, est nécessaire et indispensable pour que le destinataire accomplisse sa tâche, est dans l'intérêt de la personne concernée ou pour des raisons humanitaires, ou encore est nécessaire pour prévenir un risque grave et imminent à l'ordre public ou à la sécurité publique et qu'un niveau approprié de protection des données tel que prévu par la Convention 108 est garanti par le destinataire.

Exemple : les 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).

16. Interconnexion des fichiers et accès direct (accès en ligne)

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 dans le cadre de la législation nationale qui doit prendre en compte les principes fondamentaux de la protection des données.

Il conviendrait d'élaborer une législation et des indications claires, conformes aux principes de protection des données, pour encadrer ces croisements de bases de données. Ces croisements de base de données devraient être proportionnés.

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.

17. 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.

Comment [0057]: A clarifier en lien avec commentaire 13, en distinguant l'information générale de l'information spécifique. S'agissant de l'information spécifique, son caractère préalable par rapport au droit d'accès n'est pas systématique. En effet, dans la plupart des fichiers de police, les personnes concernées ne bénéficient pas d'une information spécifique, ce qui n'exclut pas le droit d'accès

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 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 au responsable du traitement. Le responsable du traitement des données évaluera la demande et toute restriction éventuelle qui ne peut être appliquée que dans la mesure où elle serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection de la personne concernée ou des droits et libertés d'autrui. Il répondra directement à la personne concernée. Si une dérogation est appliquée, la personne concernée doit tout de même avoir une réponse, quoique la réponse doit prendre en considération selon le droit national ou la pratique établie toutes les circonstances selon lesquelles la dérogation est appliquée.

S'il s'agit d'un accès 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 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 autorisées légalement). Dans le cas d'une restriction, 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.

Il faudrait que les dispositions en vigueur prévoient 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.

Exemple : la demande d'accès peut être refusée si une enquête est en cours sur la personne concernée et que l'octroi d'un accès lui permette de compromettre l'enquête. Toutefois, il est conseillé de se référer à la législation nationale pour veiller à ce que la réponse soit cohérente, et pour éviter que des suspects utilisent cette méthode pour savoir s'ils font l'objet d'une enquête en cours.

Le droit d'une personne concernée de pouvoir modifier toute donnée inexacte détenue à son sujet est un droit essentiel. La personne concernée qui découvre des données inexactes, excessives ou non pertinentes devrait avoir le droit de les contester et de veiller à ce qu'elles soient modifiées ou supprimées.

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.

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.

Comment [0058]: A clarifier sur la distinction entre restriction et dérogation et sur les motifs de celles-ci.

T-PD (2017)16

Toutes les modifications proposées devraient être étayées par des éléments de preuve. Si les personnes concernées peuvent prouver au moyen de documents officiels du même pays 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.

La police peut avoir besoin, conformément à ce qui est prévu au point 5, de ne pas donner d'informations ou de ne pas accorder un 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.

Les restrictions 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 une 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, la personne concernée ou 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.

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.

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 fautive, les services de police peuvent juger utile de conserver cette fautive déclaration et les informations qu'elle comprenait.

Au lieu de supprimer la déclaration dont la fausseté a été démontrée, ils peuvent ajouter au fichier concerné une déclaration rectificative claire.

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.

Exemple : une lettre de refus envoyée par la police doit contenir le nom, l'adresse, l'adresse internet, etc. de toutes les instances de recours possibles.

À chaque fois qu'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.

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 fichier de police a fait l'objet d'une vérification. À défaut, l'autorité de contrôle peut décider de communiquer les données du fichier à la personne concernée. En outre, la juridiction compétente peut avoir le pouvoir d'ordonner l'accès aux données du fichier, leur rectification ou leur suppression.

18. Sécurité des données

La police doit prendre des mesures adéquates de sécurité pour lutter 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 peuvent gravement porter atteinte aux droits et libertés fondamentales des personnes concernées.

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) afin d'évaluer les risques pour les droits de la 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 droit au respect de la vie privée fait partie intégrante de la sécurité. La protection et la sécurité des données peuvent être directement intégrées dans les systèmes et processus d'information 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.

T-PD (2017)16

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.

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. Le « respect de la vie privée dès la conception » suppose la mise en œuvre de technologies de renforcement de la protection de la vie privée qui permettent aux utilisateurs de mieux protéger leurs données à caractère personnel. Ces technologies empêchent le traitement excessif des données à caractère personnel sans réduire les capacités fonctionnelles du système informatique.

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.

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.

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 membres 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 ou à l'exécutif d'une administration nationale. Il devrait disposer des ressources suffisantes pour exécuter ses tâches et fonctions.

La législation nationale doit conférer à cet organe des pouvoirs de conseils, d'enquête et des pouvoirs répressifs lui permettant de mener une enquête à la suite d'une plainte, d'appliquer des mesures réglementaires ou d'infliger des sanctions le cas échéant.

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.

Glossaire/définitions

Aux fins du présent guide :

1. « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (« la personne concernée ») ;
2. « 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 ;
3. « 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 ou son authentification ;
4. « données subjectives » (preuve fondée sur un témoignage) : données acquises par le biais de témoignages de personnes impliquées dans l'enquête ;
5. « données objectives » (preuve fondée sur un document) : données acquises provenant de documents officiels ou d'autres sources certifiées ;
6. « 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 ;
7. « 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 ;
8. « 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 ;
9. « 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 ;
10. « 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. ;
11. « 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 ;
12. « 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.
13. « 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.

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 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 survey¹⁰ 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 clear guidance on what the principles imply at an operational level.

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 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 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

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

20. 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 and the execution of criminal penalties and for the maintenance of public order. 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.

21. Collection of data and use of data

The collection and use of personal data for police purposes should be limited to what 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: that which

Comment [0059]: It is still not clear what this clarification (in the sense of "that means" (i.e.) is supposed to add here. This addition should only be kept if it is introduced by "e. g." (in the sense of "for example").

¹⁰ See Report "[Twenty-five years down the line](#)" – by Joseph A. Cannataci.

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.

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. During collection, provided that all legal requirements are met, larger scale of personal data can be processed. After the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be deleted.

Police 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).

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 the relevant people.

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 at the time of collection, unless this is provided for in law (see Art 9 of Convention 108). Subsequent use of data is considered for the use of this guide as a new data processing operation which has to follow all basic principles mentioned before, especially those of necessity and proportionality.

Example: If not provided for to do so by law, police data collected for an investigation in which the political affiliation of the suspect was not relevant cannot then be used to determine the political affiliation of the concerned person.

22. Subsequent use of data

Every subsequent processing of data by police (irrespective of the fact that the original processing has been carried out for a police purpose or for other purposes) for 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 necessary and proportionate to the legitimate aim pursued.

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 the purpose personal data subsequently is used for should be linked to a police purpose and that the data processing must fulfil the criteria and conditions set out in point 2. The general rule is that all data held by police should have a link to a case or specific task of the police and should be processed in relation with this.

It should be noted however, that any subsequent use of personal data, in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.

Comment [0060]: BKAm: The scale of data processed is primarily a question of proportionality.

Comment [0061]: The data-minimisation principle as such is not reflected in the EU Police Directive and does not reflect the evolution of new technical capabilities ("big data" type analysis). Furthermore, the principles of necessity and non-excessiveness related to the purpose already reflect the idea behind this sentence.

We there propose to include a reference to the main data protection principles without mentioning the data minimization principle as such:

Police shall ensure at all stages of the processing of personal data for it to be adequate, relevant and not excessive in relation to the purposes for which they are processed and should not [...]"

Deleted: should apply the data-minimisation principle at all stages of the processing and

Deleted:

Deleted:

Comment [0062]: This might create misunderstandings: The very advantage of the concept of subsequent - purpose-changing - use of personal data is that it does not have to be collected once more for the changed purpose - otherwise it would not be a "subsequent use". It might be clearer to use the proposed wording.

Deleted: fulfil all the criteria and conditions applicable to the collection and the use of data

Deleted: P

Comment [0063]: This sentence does not seem to have added value.

Deleted: ,

Deleted: p

Comment [0064]: It is still unclear why a justification for processing "in an unstructured manner" is needed in this context. Is "unstructured manner" supposed

Deleted: mission

Deleted: , in particular

Comment [0065]: The added value of this sentence is still unclear as always a legal basis is needed for further processing

Comment [0066]: It is unclear what this call for enhanced exchange between police bodies is supposed to add to the subject.

Deleted: In cases such as trafficking in human beings, drug trafficking, sexual exploitation, where victims' data may subsequently be used also when the ...

Deleted: ¶

Example - Biometric data taken for immigration purposes can be processed for law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Any such use should be lawful and proportionate.

23. 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 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 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 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.

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. Information provided should include details about the conditions under which exceptions apply to the data subject's rights and how they can submit an appeal against a decision of the data controller in reply to their request.

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. In respect of making information available which highlight data protection and data subjects' rights, this is the responsibility of the data controller to provide.

According to the second obligation of giving data subject specific information regarding their data upon request for access, the data controller has to inform the individuals on the data processing activities that it has pursued with their data. This means that if an individual has its data collected during the course of an investigation, as soon as circumstances safely permit, the police should advise the individual of the data processing if there is such request. The information should be provided in clear and plain language.

The law can provide that the right to be informed may be limited, should the provision, 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 data processing however should be used only sparingly and where it can be clearly justified.

Example - For the purpose of covert monitoring of a high risk sex offender, data processing and long-term data retention may be justified without notifying the individuals without request - if foreseen in domestic law - or informing them upon request for access 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.

- Deleted: providing
- Deleted: ,
- Deleted: mission
- Comment [0067]: "notification" implies informing the data subject also in cases where there is no request.
- Deleted: notification
- Deleted:
- Deleted: of
- Deleted: informing

24. 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 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 2,3,4,7 as well as to the data subjects' rights (point 17) in relation to certain purposes. In particular it affects those activities undertaken for

- Comment [0068]: What does this entail?
- Deleted: in case of some specific data processing activities

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 tasks of the police, and other essential objectives of general public interest or the protection of the rights and fundamental freedoms of others. Other applicable underlying purposes for exceptions are foreseen in Article 3 Convention 108.

If the exception, based on national law, is applied by the police it should be applied for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being applied. The aim of using exceptions by the police should be limited to cases where the use of those rules and principles would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police.

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.

Comment [0069]: Art 3 CONV 108 does not foresee any exceptions.

Deleted: used

Deleted: used

Deleted: used

↓

Comment [0070]: This remains to be no valid "example" for an exception from data subjects' rights. What is it meant to illustrate?

25. 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, 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, those considerations have to be balanced with cost-effectiveness, use of resources and 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 covert surveillance measures, such as wiretapping.

Deleted: Example: Police data can be shared with national security agencies in respect of national security, for example to prevent a terrorist attack. In order to rapidly identify the perpetrator, police shall cooperate 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 security agencies. 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 (such as judicial authorisation, stricter rules on purpose limitation) with a view of ensuring an enhanced protection to the individual's right to privacy and data protection.

Deleted: ¶

26. Introduction 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.

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, continuous (i.e. repeated at reasonable intervals) and that it should touch upon every phase of the data processing activity. The relevance of the DPIA shall be checked by 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. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights.

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 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 contained and by whom the data is being accessed as well as information on retention of data, log policy and access policy.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data could be reported to or made available 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 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 glasses used by police which is directly linked to relevant databases 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.

Big data and profiling in the police

Technological advancements, 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 potentially and inadvertently interfere with the right to privacy and data protection.

The Council of Europe's Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data¹¹ 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:

Comment [0071]: The text above does not advise mandatory consultation. The example should not go beyond the text.

Comment [0072]: That is a different issue (role of the DPA in the legislative process) that has not been touched upon in the text above.

Deleted: are to

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

Deleted: .

Comment [0073]: The question how gathered information is treated is different than the question as to how and where smart glasses should be connected.

Comment [0074]: the national criminal record database is not embedded in a secure IT environment?

Deleted: es

¹¹ Document T-PD(2017)1

- 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 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 take due account of 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 traditional methods of investigation.
- Its use is necessary and proportionate for police purpose.
- 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.
- Where possible, 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 compatible purpose the data controller should make the data subjects aware of this secondary use.
- Lawfulness of the processing and compliance with the conditions set by Article 8 ECHR should be demonstrated.
- An information security policy should be in place.
- 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.

27. 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, or it is for crime investigation purpose. 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 (e.g. criminal investigation) 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, profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subject. 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 habitants share the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

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

Comment [0075]: Still, the vast majority of the points mentioned here are valid not only in a "big data" context.

Deleted: (where 2 fingerprints would suffice)

Deleted: (where 8 to 10 fingerprints would be needed)

Deleted: i

Deleted: e

Deleted: are from

particular religious group, it could be of importance to process data specific to the followers of this 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.

28. Storage of data

As pointed out in Point 2 data shall be processed until they have served the purpose for which they were collected. 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. 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 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. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

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 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. ↓
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 revision of the case have also expired. Likewise, if, after 4 years, the investigation is still ongoing 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.

When shaping internal policies and 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.

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. This uses a classification system to facilitate 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.

Comment [0076]: It is not clear at all what is meant here.

Deleted: 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, 4 years later the evidence based solely on this data could possibly be considered as unlawful by the court.

Deleted: ¶

Personal data collected by police for administrative purposes must be kept (if feasible: 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.

29. 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. As a general rule police can 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 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.

30. 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 10 should be followed when data are to be transmitted domestically outside of the police sector.

As an exception, communication 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 unless the providing body consents, based on legal provisions, to a subsequent use for other purposes.

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.

Deleted: m

Comment [0077]: It is inherent to such communication that data transferred outside the police sector will probably be used for non-law-enforcement purposes. We ask for clarification.

Deleted: as there is a risk that the communicated data could be used for non-law enforcement purposes

Comment [0078]: from which rule?

31. 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, 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: missions

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.

32. International transfer

Any transfer of police data internationally should be limited to police organisations 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 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. 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 "Rules Governing the Processing of Data and its 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) can be applicable¹² 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.

Comment [0079]: IVB1: Ergänzung ist zu streichen, denn wird anderen europäischen Rechtsakten und der Rechtsprechung des EuGH (siehe insb. zuletzt zu PNR) nicht gerecht.

Deleted: ,

Deleted: as far as possible and practicable,

An appropriate level of data protection should be ascertained (e. g. through a guarantee given by the receiving party) if data are to be transferred to countries not participating in Convention 108.

Deleted: guaranteed

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.

¹² This is without prejudice to the right of the Committee of Convention 108 and of other instances having such power to assess and to review, if necessary, the level of data protection guaranteed by those multilateral agreements.

Example - Further onward transfer of data should only be allowed if this is necessary for the same specific 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 with 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 has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

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 police data to a private body residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases where it is provided by legal means and where the gravity of the crime, its trans-border nature and the fact that the involvement of the local police would compromise the purpose of the investigation because of the length of the procedure. 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. 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.

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.

33. 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. The quality of data can be assessed up to the moment of communication.

Example: If personal data is sent that contains incorrect data (personal or otherwise) 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.

34. Safeguards for communication

T-PD (2017)16

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 only exception to this is when the sending authority, based on legal provisions, gives consent to any further use and if the processing is based on law, is necessary and vital for the recipient to fulfil their task, is in the interest of the data subject or for humanitarian reasons or is necessary to prevent serious and imminent risk to public order or public security and an appropriate level of data protection is guaranteed by the recipient as foreseen by Convention 108.

Deleted: agreement

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).

35. 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 in accordance with domestic legislation 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 proportionate.

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.

36. 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 if no exception is applicable.

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 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 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.

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 which can only be used if it is vital for the performance of a legal task of law enforcement 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. If restriction was to be used, the data subject still has to have an answer, albeit any answer should take into consideration according national law or practice all circumstances to which the restriction 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 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). In case of a restriction, 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.

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.

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.

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, 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 giving a testimony in a criminal case.

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 same countries’ 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.

It may be necessary for the police, as dealt with under point 5, 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.

Restrictions to the rights of data subjects 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 refusals provided to 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.

Comment [0080]: excessive processing or processing of irrelevant data is not the same as amending incorrect data. Different scenarios should not be mixed here.

IVBI:
Wir stimmen mit dem BMI überein, dass “amend” sich auf “incorrect” bezieht. Die Passage zu “excessive or irrelevant” data müsste sich dann aber bei dem Recht auf Löschung wiederfinden/dorthin verschoben werden.

Deleted: excessive or irrelevant

Deleted: ,

Deleted: or deleted

Deleted: or delete them.

T-PD (2017)16

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 to retain 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.

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

Deleted: um

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.

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 is not obliged to 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 decide 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.

37. 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 may seriously interfere with the rights and fundamental freedoms of data subjects.

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.

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 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 is an integral part of security. Data protection and security may be embedded directly into information systems and processes 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-Enhancing Technologies (PETs)

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

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.

38. 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.

T-PD (2017)16

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 or the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

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.

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:

27. "personal data" means any information relating to an identified or identifiable individual ("data subject");
28. "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;
29. "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;
30. "soft data" (evidence based on testimony or other personal assessment) means data acquired through testimony of person involved in the investigation;
31. "hard data" (evidence based on documents or facts) means data acquired from official documents or other certified sources;
32. "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;
33.  
34. "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;
35. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
36. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
37. 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.
38. "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.
39. "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.

Comment [0081]: The term is not used in the guide.

Deleted: 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

IRELAND / IRLANDE

Ireland’s Comments on Revised Draft Practical Guide on the use of personal data in the Police Sector

Ireland’s Comments on Revised Draft Practical Guide on the use of personal data in the Police Sector

Collection of data and use of data

2. Collection of data and use of data

The collection and use 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 or the suspicion thereof) and where personal data is processed for the purpose of the maintenance of public order.

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. During collection, provided that all legal requirements are met, larger scale of personal data can be processed. After the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be deleted.

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 those purposes, unless this is provided for in law (see Art 9 of Convention 108). Subsequent use of data is considered for the use of this guide as a new data processing operation which has to fulfil all the criteria and conditions applicable to the collection and the use of data.

3. Subsequent use of data

It should be noted however, that any subsequent use of personal data, in particular in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.

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 international good practice and to enhance their exchange of information on the matter with other police bodies. This does not represent any obstacle to the use of data of these persons for police purpose if all legal requirements as put forward in point 2 are met.

4. Providing information to data subjects

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,

Comment [W82]: This appears too narrow. We are concerned that this may have implications for DNA databases and it doesn't seem to take account of the fact that an individual may be involved in more than one offence.

Comment [W83]: It is understood that this sentence is intended to mean that at the outset of an investigation, the collection of large amounts of personal data may be justified/necessary. Perhaps it could be reworded to clarify the intended meaning.

Deleted: the original purpose at the time of collection

Comment [W84]: The purpose of this sentence is not clear.

Comment [W85]: The purpose of this paragraph is not clear.

Comment [W86]: We would question the inclusion of this reference to data processor; the police may engage different data processors for different purposes e.g. they may engage a translation service, a shredding company, etc. Is it appropriate or necessary to provide information in relation to those processors to data subjects?

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.

...

According to the second obligation of giving data subject specific information regarding their data upon request for access, the data controller has to inform the individuals on the data processing activities that it has pursued with their data. This means that if an individual has ~~its~~ his or her data collected during the course of an investigation, as soon as circumstances safely permit, the police should advise the individual of the data processing if there is such request. The information should be provided in clear and plain language.

5. Exceptions from the application of data protection principles

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 17) in case of some specific data processing activities. In particular it affects those 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 or the protection of the rights and fundamental freedoms of others. Other applicable exceptions are foreseen in Article 3 Convention 108.

If the exception, based on national law 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 the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police.~~

~~Example: Police data can be shared with national security agencies in respect of national security, for example to prevent a terrorist attack. In order to rapidly identify the perpetrator, police shall cooperate 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 security agencies. 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 (such as judicial authorisation, stricter rules on purpose limitation) with a view of ensuring an enhanced protection to the individual's right to privacy and data protection.~~

7. Introduction of new data processing technologies

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 consult with~~ the supervisory authority ~~in every case~~ 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.

During the consultation process 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 contained and by whom the data is being accessed as well as information on retention of data, log policy and access policy.

~~Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data are to be reported to or made available to the data protection authority. Data protection authority is preferably to be consulted during the legislative procedure.~~

Comment [W87]: This reference appears to be incorrect.

Comment [W88]: Perhaps another word could be used here e.g. being processed.

Comment [W89]: The first sentence goes beyond the text and the purpose of the second sentence is not clear as the police would not be responsible for the preparation of legislation.

Example - Introducing an automatic facial recognition system would need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed, 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.

8. 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 **nature** 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.

Comment [W90]: Would 'ordinary' be a more appropriate word?

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 to ensure that the appropriate safeguards are put in place adequately. The data controller should assess and demonstrate whether the purpose of the processing **:-e.g.** criminal investigation) 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.

Comment [W91]: This sentence does not seem appropriate most personal data processed by the police would relate to 'offences, criminal proceedings and convictions and related security measures'.

Regarding these data, profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subject. 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 **habitants individuals** are from the same ethnic origin. There should be additional criteria to allow the processing of data on this ground.

9. Storage of data

There should, **as far as possible**, be a clear distinction in how police store 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. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

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, 4 years later the evidence based solely on this data could possibly be considered as unlawful by the court.

Comment [W92]: Is there text missing here e.g. should there be a reference to 'personal data'?

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 revision 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 ~~revision~~ 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.

When shaping internal policies 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.

Comment [W93]: This sentence is not very clear, perhaps highlighted text could be moved to the end of the sentence.

Data should, **as far as possible**, 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. This uses a classification system to facilitate 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.

12. 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 ~~missions~~ functions, 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.

13. International transfer

Example - Further onward transfer of data should only be allowed if this is necessary for the same specific 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 ~~with~~ 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 has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

Comment [W94]: Would it be possible to clarify this sentence?

The international transfer of police data to a private body **residing** in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases where it is provided by legal means and where the gravity of the crime, its trans-border nature and the fact that the involvement of the local police would compromise the purpose of the investigation because of the **length of the procedure**. 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. 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.

Comment [W95]: This word doesn't appear to be necessary.

Comment [W96]: Is this the only reason that personal data might need to be transferred to a private body?

14. 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 data it is always advisable to double-check the quality of data, if it is correct, up-to-date, complete. The quality of data can be assessed up to the moment of communication.

17. Data subject's rights

Example: If a data subject asks the police ~~en~~ **about** 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.

In respect of direct access, the data subject can **direct their** request **for** access to the controller of the files. The data controller will assess the request and any possible restriction which can only be used if it is ~~vital~~ **necessary** for the performance of a legal task of law enforcement 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. If restriction was to be used, the data subject still has to have an answer, albeit any answer should take into consideration according national law or practice all circumstances to which the restriction 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 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). In case of a restriction, the same communication should be made possible as in case of a direct access.

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 giving a testimony in a criminal case.

Restrictions to the rights of data subjects 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 refusals provided to 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.

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 is not obliged to 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 decide 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.

18. Data security

Police authorities are advised, where necessary, to conduct a 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.

Privacy-by-Design

Privacy is an integral part of security. Data protection and security may be embedded directly into information systems and processes 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.

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.~~

Comment [W97]: What does 'lawfulness of the data subject's personal data' mean? Perhaps the text could be clarified.

Comment [W98]: It is presumed that this sentence is designed to acknowledge the fact that the right to request rectification doesn't apply to witness statements. Perhaps this could be clarified.

Comment [W99]: Could this sentence be clarified e.g. Any decision to refuse a data subject's request should be provided in writing (including by electronic means).

Comment [W100]: This sentence needs to be clarified as it appears to suggest that a supervisory authority can release personal data to a data subject where the police decide that it shouldn't be released. However in such a case, the role of the supervisory authority should be to request the police to release the data. The police could then decide whether to release the data or to appeal the decision to a court or tribunal as appropriate. In the absence of an appeal, it would be open to the supervisory authority to apply to the courts to have its decision enforced.

Comment [W101]: The meaning of this sentence is not clear; should it state 'Privacy by design is ...?'

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 or the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

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.

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

Comment [W102]: This goes beyond Convention 108.

Glossary/Definitions

4. ~~“soft data” (evidence based on testimony) means data acquired through testimony of person involved in the investigation;~~

Comment [W103]: This definition should be left to individual States.

5. ~~“hard data” (evidence based on documents) means data acquired from official documents or other certified sources;~~

Comment [W104]: This definition should be left to individual States?

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 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 survey¹³ 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 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 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

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that data processing within the police should be based on predefined, clear and legitimate purposes [set in the law](#), that it 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. It should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally the data which are processed within the police 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 [specific](#) purposes of the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties and for the maintenance of public order. 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 for the purpose of prevention, investigation and prosecution of criminal offences and the execution of criminal

Deleted: that which

penalties (i.e. to a specific criminal offence or the suspicion thereof) and „for the purpose of the maintenance of public order.

Deleted: where personal data is processed

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.

Comment [00105]: we may want to move this paragraph to the general introduction

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. During collection, provided that all legal requirements are met, larger scale of personal data can be processed. After the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be deleted.

Comment [00106]: this sentence is not clear, in particular the reference to "larger" (than what?) scale of personal data". Either we delete it or we try to explain better what we mean.

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).

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 the relevant people.

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 at the time of collection, unless this is provided for in law (see Art 9 of Convention 108). Subsequent use of data is considered for the use of this guide as a new data processing operation which has to fulfil all the criteria and conditions applicable to the collection and the use of data.

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

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) must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be necessary and proportionate to the legitimate aim pursued by the police.

Due to the nature of data processing, it is possible that personal data collected for one purpose are used for another. However, 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 personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set in point 2. The general rule is that 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: to use

Deleted: ,

It should be noted however, that any subsequent use of personal data, in particular in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.

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 international good practice and to enhance their exchange of information on the matter with other police bodies. This does not represent any obstacle to the use of data of these persons for police purpose if all legal requirements as put forward in point 2 are met.

Example - Biometric data taken for immigration purposes can be processed for law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Any such use should be lawful and proportionate.

4. 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 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 upon request on the processing of their personal data.

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 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: ,

Deleted: also, most importantly,

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.

Deleted: information provided

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.

Deleted: In respect of making information available which highlight data protection and data subjects' rights

Deleted: this

According to the second obligation of giving data subject specific information regarding their data upon request for access, the data controller has to inform the individuals on the data processing activities that it has pursued with their data. This means that also in case an individual has its data collected during the course of an investigation, as soon as circumstances safely permit, the police should inform the individual of the data processing if there is such request. The information should be provided in clear and plain language.

Deleted: if

Deleted: advise

The law can provide that the right to be informed may be limited, should providing such information, prejudice the investigation, or another important police mission, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding notification of data processing however should be used only sparingly and where it can be clearly justified.

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 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.

5. 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 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 2,3,4,7 as well as to the data subjects' rights (point 17) in case of some specific data processing activities. In particular it affects those 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 or the protection of the rights and fundamental freedoms of others. Other applicable exceptions are foreseen in Article 3 of Convention 108.

Comment [00107]: not sure the structure of the sentence is clear

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

Deleted: based

Deleted: on

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 can be shared with national security agencies in respect of national security, for example to prevent a terrorist attack. In order to rapidly identify the perpetrator, police shall cooperate 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 security agencies. 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 (such as judicial authorisation, stricter rules on purpose limitation)_with a view of ensuring an enhanced protection to the individual's right to privacy and data protection.

6. 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, 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, those considerations have to be balanced with cost-effectiveness, use of resources and efficiency of investigations.

Comment [00108]: we are missing a point here: we don't say that the balancing must consider the protection of fundamental rights and the right to privacy.

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 covert surveillance measures, such as wiretapping.

7. Introduction 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.

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

T-PD (2017)16

that the assessment of risk is not static, but takes into account the specific case, continuous (i.e. repeated at reasonable intervals) and that it should touch upon every phase of the data processing activity. The relevance of the DPIA shall be checked by 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. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights.

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 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 contained and by whom the data is being accessed as well as information on retention of data, log policy and access policy.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data are to be reported to or made available to the data protection authority. Data protection authority is preferably to be consulted during the legislative procedure.

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 would need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed, 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 which is directly linked to relevant databases 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.

Big data and profiling 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 police who are turning to digital sources and profiling techniques to perform their legal tasks.

Comment [00109]: although the consultation of DPA during the legislative procedure is undoubtedly important I am not sure it should be said here as this is a guidance for operators not governments. Maybe we could refer to that in different terms

Deleted: should

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: potentially and inadvertently

The Council of Europe's Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data¹⁴ 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 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 take due account of 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 traditional methods of investigation to complement the conclusions drawn.
- Its use is necessary and proportionate for police purpose.
- 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.
- Where possible, 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 compatible purpose the data controller should make the data subjects aware of this secondary use.
- Lawfulness of the processing and compliance with the conditions set by Article 8 ECHR should be demonstrated.
- An information security policy should be in place.
- 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.

Comment [00110]: This sentence is not clear.

Comment [00111]: the sentence should be expanded. Necessary and proportionate in a democratic society?

Comment [00112]: not clear.

Comment [00113]: we should add a reference to the need for transparency of algorithm in use and of the purposes pursued to avoid discriminatory action.

8. 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 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. criminal investigation) 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, profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subject. 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 habitants are from the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

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 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.

9. Storage of data

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

Deleted:

Deleted:

There should be a clear distinction in how police store 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. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

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 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, 4 years later the evidence 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. 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 revision of the case have also expired. Likewise, if, after 4 years, the investigation is still ongoing and their data is still relevant to it, the police should be able to retain it.

Deleted:

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.

When shaping internal policies 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.

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. This uses a classification system to facilitate 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 (if feasible: 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.

10. 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. As a general rule police can 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 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.

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

T-PD (2017)16

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 10 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the communicated data could be used for non-law enforcement purposes.

As an exception, communication 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.

12. 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 missions, 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.

13. International transfer

Any transfer of police data internationally should be limited to police organisations 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 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. 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 "Rules Governing the Processing of Data and its 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) can be applicable¹⁵ 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 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: ,

An appropriate level of data protection should be guaranteed if data are to be transferred to countries not participating in 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 specific 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 with 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 has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

The international transfer of personal data to a non-police 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.

15

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

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 police data to a private body residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases where it is provided by legal means and where the gravity of the crime, its trans-border nature and the fact that the involvement of the local police would compromise the purpose of the investigation because of the length of the procedure. 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. 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.

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.

14. 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. The quality of data can be assessed up to the moment of communication.

Example: If personal data, that contains incorrect data (personal or otherwise) is 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

15. 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 only exception to this is when the sending authority, based on legal provisions, gives agreement to any further use and if the processing is based on law, is necessary and vital for the recipient to fulfil their task, is in the interest of the data subject or for humanitarian reasons or is necessary to prevent serious and imminent risk to public order or public security and an appropriate level of data protection is guaranteed by the recipient as foreseen by Convention 108.

Comment [00114]: not easy to read. In particular it is not clear whether the conditions listed are all necessary or alternative.

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).

16. 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 in accordance with domestic legislation 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 proportionate.

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.

17. 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 should, in principle, be free of charge.

Deleted: (as the right to information)

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 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.

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 which can only be used if it is vital for the performance of a legal task of law enforcement 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. If restriction was to be used, the data subject still has to have an answer, albeit any answer should take into consideration according national law or practice all circumstances to which the restriction 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

T-PD (2017)16

regarding the availability and lawfulness 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). In case of a restriction, 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.

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.

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.

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 giving a testimony in a criminal case.

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 same countries' 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 5, 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.

Restrictions to the rights of data subjects 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 refusals provided to 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 to retain 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.

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.

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 is not obliged to 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 decide 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.

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 may seriously interfere with the rights and fundamental freedoms of data subjects.

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 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.

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 implement measures in respect of:

- equipment access control,
- data media control,
- storage control,

T-PD (2017)16

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

Privacy-by-Design

Privacy is an integral part of security. Data protection and security may be embedded directly into information systems and processes 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-Enhancing Technologies (PETs)

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

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 or the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

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.

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:

1. “personal data” means any information relating to an identified or identifiable individual (“data subject”);
2. “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;
3. “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;
4. “soft data” (evidence based on testimony) means data acquired through testimony of person involved in the investigation;
5. “hard data “ (evidence based on documents) means data acquired from official documents or other certified sources;
6. “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;
7. “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;
8. “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;
9. “recipient” means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
10. “processor” means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
11. 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.
12. “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.
13. “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.

Formatted: English (U.S.)

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 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 survey¹⁶ 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 clear guidance on what the principles imply at an operational level.

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

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that data processing within the police should be based on predefined, clear and legitimate purposes that it 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. It should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally the data which are processed within the police should be accurate and up-to-date to ensure the highest data quality possible.

39. 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 and the execution of criminal penalties. 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.

40. Collection of data and use of data

The collection and use 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 or the suspicion thereof).

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

Deleted: ,

Comment [00115]: We suggest to delete the 'maintenance of public order' throughout as it overly broadens the scope of specific rules for police to areas which should be covered by general data protection rules.

Deleted: and maintenance of public order

Deleted: and for the maintenance of public order

Deleted: and where personal data is processed for the purpose of the maintenance of public order

Comment [00116]: It is always an interference, but the interference can be justified.

Deleted: can

¹⁶ See Report "[Twenty-five years down the line](#)" – by Joseph A. Cannataci.

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.

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. During collection, provided that all legal requirements are met, larger scale of personal data can be processed. After the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be 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).

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 the relevant people.

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 at the time of collection, unless this is provided for in law (see Art 9 of Convention 108). 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 applicable to the collection and the use of data.

Deleted: use

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

41. Subsequent use of data

Every subsequent processing of data by police for police purposes (irrespective of the fact that the original processing has been carried out for police purpose or for other purposes) must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be necessary and proportionate to the legitimate aim pursued.

Due to the nature of data processing, and the fact that it is technically possible to use personal data collected for one purpose for another purpose, personal data collected and retained for police purposes should not be kept and processed in an unstructured manner unless there is a legal basis, a legitimate interest and an operational reason within the legal powers of the police to do this. This means that personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set in point 2. The general rule is that 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: , a legal basis

Deleted:

Deleted: for

It should be noted however, that any subsequent use of personal data, in particular in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.

Comment [00117]: We don't really understand the message anymore and the whole section is moving far from being "practical".
What does it mean: "to use in an unstructured manner"? Can you use data in a structured manner if you do not have a legal basis, legitimate interest and operational reason? What is the relation between these three? How does "legal basis" differ from "solid legal grounds"? These paragraph should be clarified or deleted.

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 international good practice and to enhance their exchange of information on the matter with other police bodies. This does not represent any obstacle to the use of data of these persons for police purpose if all legal requirements as put forward in point 2 are met.

Example - Biometric data taken for immigration purposes can be processed for law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Any such use should be lawful, proportionate and subject to specific rules on access to data collected for a non-law enforcement purposes by the law enforcement authorities.

Comment [00118]: Doesn't it apply to all processing?

Deleted: and

42. 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 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 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 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 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. Information provided should include details about the conditions under which exceptions apply to the data subject's rights and how they can submit an appeal against a decision of the data controller in reply to their request.

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. In respect of making information available which highlight data protection and data subjects' rights, this is the responsibility of the data controller to provide.

According to the second obligation of giving data subject specific information regarding their data, the data controller has to inform the individuals on the data processing activities that it has pursued with their data. This means that if an individual has its data collected during the course of an investigation, as soon as circumstances safely permit, the police should advise the individual of the data processing if there is such request. The information should be provided in clear and plain language.

Comment [00119]: The information here should be provided proactively by the police, and not only after the request for access has been received. Further, more detailed information will be provided once data subject exercises his or her right to access.

Deleted: upon request for access

The law can provide that the right to be informed may be limited, should providing such information, prejudice the investigation, or another important police mission, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding notification of data processing however should be used only sparingly and where it can be clearly justified.

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 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.

43. 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 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 2,3,4,7 as well as to the data subjects' rights (point 17) in case of some specific data processing activities. In particular it affects those

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 or the protection of the rights and fundamental freedoms of others. Other applicable exceptions are foreseen in Article 3 Convention 108.

Comment [00120]: These are exclusions from the scope. Given the next paragraph, we suggest deleting or placing it lower, at the end of this section.

If the exception, based on national law, 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 the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties.

Comment [00121]: This is too broad as an objective.

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: or other missions of the police

Example: Police data can be shared with national security agencies in respect of national security, for example to prevent a terrorist attack. In order to rapidly identify the perpetrator, police shall cooperate 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 security agencies. However if there is no such risk, police should share its data with national security agencies according to general, well-established procedure in which stronger safeguards are put in place (such as judicial authorisation) with a view of ensuring an enhanced protection to the individual's right to privacy and data protection.

Comment [00122]: What 'special procedures' do you have in mind?

Deleted: of terrorist attack

44. Use of special investigative techniques

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

Comment [00123]: Purpose limitation is a basic principle of data protection and we shouldn't leave the impression you can derogate from it. If we say "stricter rules" here we imply that there are "less strict rules on purpose limitation" in the "special procedure" above, which shouldn't be the case.

The distinction between the two cases referred to in the box is not clear. Indeed, in both cases, one would need a law, explicitly providing for a possibility to use data for other purposes and formulating the conditions. What is meant is probably that in such special cases law can authorise sharing under less stringent conditions than in other cases. We suggest to reformulate the text accordingly.

Deleted: , stricter rules on purpose limitation

With 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, those considerations have to be balanced with cost-effectiveness, use of resources and efficiency of investigations.

Comment [00124]: A bit confusing: in this chapter, you are discussing the electronic surveillance, while the definition of the special investigative techniques given in the end of the document seems very broad...

Deleted: The police should always adopt the least intrusive means of data processing during its operations.

Deleted: increasingly sophisticated

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 covert surveillance measures, such as wiretapping.

Comment [00125]: A bit confusing. The definition of "covert surveillance" at the end of the document is very broad, "discreet surveillance" seems to fall within. Why don't you directly refer to wiretapping in this example? This is the only place where you use "covert surveillance" (in other places you are referring to "covert monitoring"), is the use of this term necessary in the guide?

45. Introduction 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.

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, continuous (i.e. repeated at reasonable intervals) and that it should touch upon every phase of the data processing activity. The relevance of the DPIA shall be checked by 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. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights.

Comment [00126]: Do you want to use 'supervisory authority' or 'data protection authority'?
The Protocol to the Convention 108 refers to "supervisory authorities"

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 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 contained and by whom the data is being accessed as well as information on retention of data, log policy and access policy.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data are to be reported to or made available to the data protection authority. 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 would need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed, 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 which is directly linked to relevant databases 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.

Big data and profiling 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 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 potentially and inadvertently interfere with the right to privacy and data protection.

The Council of Europe's Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data¹⁷ 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:

¹⁷ Document T-PD(2017)1

- 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 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 take due account of 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 traditional methods of investigation.
- Its use is necessary and proportionate for police purpose.
- 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.
- Where possible, 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 compatible purpose the data controller should make the data subjects aware of this secondary use.
- Lawfulness of the processing and compliance with the conditions set by Article 8 ECHR should be demonstrated.
- An information security policy should be in place.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals and that administrative and judicial means exist for individuals to challenge those decisions.

46. 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 nature, 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.

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 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. criminal investigation) 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, decisions based solely on profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subject. 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 habitants are from the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

Comment [00127]: Doesn't it depend on the concrete situation? "Traditional methods" are not defined, can we be sure that they will always be less intrusive? I suggest deleting.

Comment [00128]: Doesn't it apply to all data processing (principle of minimisation: Art. 5 requires that data must be "adequate, relevant and not excessive in relation to the purposes for which they are stored")? I suggest reformulation, so as to remind/stress the importance of this principle, but make it clear that it applies in all cases, not only in the "big data" context

Comment [00129]: Also "where possible", I presume? In line with a previous section on information provided to the data subject.

Comment [00130]: Again, not sure why this would be specific to "big data".

Comment [00131]: Idem.

Deleted: e

Comment [00132]: If you mean that the security standards should be high, there is no need for this confusing sentence. Such processing still has to be prescribed by law.

Deleted: Sensitive data can, however, be processed to protect the vital interest of the data subject or of another person.

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 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.

47. Storage of data

As pointed out in Point 2 data shall be processed until they have served the purpose for which they were collected. 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. 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 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. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

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 necessary to achieve the purpose of the prevention, investigation and prosecution of criminal offences and execution of criminal penalties,

Deleted: 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, 4 years later the evidence 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. 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 revision of the case have also expired. Likewise, if, after 4 years, the investigation is still ongoing 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.

When shaping internal policies 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.

Comment [00133]: Isn't it obvious?

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.

Deleted: This uses a c

Deleted: to

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 separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by the law.

Deleted: (if feasible: logically and physically)

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

48. 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. As a general rule police can 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.

The communication of personal data in general should be subject to the principle of necessity and proportionality and has to serve the above mentioned purposes.

Deleted: and where personal data is processed for the purpose of the maintenance of public order

Comment [00134]: Again, this is a general principle. We understood at the plenary meeting that the paper would include a general part were all cross-cutting issues (such as the principles) would be mentioned/discussed. Further sections might contain such mentions only as reminders or while specifying how it applies in a given context (like "big data") or to a specific type of processing (e.g. sharing)

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.

49. 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).

Deleted: mutual

Stricter principles than those set forth in Point 10 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the communicated data could be used for non-law enforcement purposes.

As an exception, communication 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.

50. 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, 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: or other important police missions

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.

51. International transfer

Any transfer of police data internationally should be limited to police organisations 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 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 or the execution of criminal penalties and whether the sharing of the data is necessary to perform its specific task.

Deleted: ,

Deleted: and the maintenance of public order

Deleted: ,

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. 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 "Rules Governing the Processing of Data and its 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) can be applicable¹⁸ 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.

Comment [00135]: "can be applicable as to ensure" is not very clear. Perhaps: "To this effect, the sending authority may take into account notably safeguards resulting from international transfers framework such as Interpol's "Rules Governing the Processing of Data and its 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)."

An appropriate level of data protection should be guaranteed if data are to be transferred to countries not participating in Convention 108.

¹⁸ This is without prejudice to the right of the Committee of Convention 108 and of other instances having such power to assess and to review, if necessary, the level of data protection guaranteed by those multilateral agreements.

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 specific 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 with 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 has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

The international transfer of personal data to a non-police 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 police data to a private body residing 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 law enforcement work, provided by legal means and where the crime is of a trans-border nature and where the involvement of the local police would compromise the purpose of the investigation because of the length of the procedure. 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. 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: gravity of the crime

Deleted: , its

Deleted: fact that the

Comment [00136]: We re-drafted the sentence because it was not finished and it was not possible to understand it fully.

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.

52. 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. The quality of data can be assessed up to the moment of communication.

Example: If personal data is sent that contains incorrect data (personal or otherwise) 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.

53. Safeguards for communication

T-PD (2017)16

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 only exception to this is when the sending authority, based on legal provisions, gives agreement to any further use and if the processing is based on law, is necessary and vital for the recipient to fulfil their task, is in the interest of the data subject or for humanitarian reasons or is necessary to prevent serious and imminent risk to public order or public security and an appropriate level of data protection is guaranteed by the recipient 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 as well).

54. 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 in accordance with domestic legislation 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 proportionate.

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.

55. 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 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 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.

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 which can only be used if it is vital for the performance of a legal task of law enforcement 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. If restriction was to be used, the data subject still has to have an answer, albeit any answer should take into consideration according national law or practice all circumstances to which the restriction 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 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). In case of a restriction, 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.

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.

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.

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 giving a testimony in a criminal case.

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 same countries’ 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 5, 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.

Restrictions to the rights of data subjects 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 refusals provided to 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.

T-PD (2017)16

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 to retain 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.

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.

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 is not obliged to 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 decide 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.

56. 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 may seriously interfere with the rights and fundamental freedoms of data subjects.

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 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.

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 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 is an integral part of security. Data protection and security may be embedded directly into information systems and processes 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-Enhancing Technologies (PETs)

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

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.

57. 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.

T-PD (2017)16

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 or the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

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.

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:

40. "personal data" means any information relating to an identified or identifiable individual ("data subject");
41. "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;
42. "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;
43. "soft data" (evidence based on testimony) means data acquired through testimony of person involved in the investigation;
44. "hard data" (evidence based on documents) means data acquired from official documents or other certified sources;
45. "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;
46. "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;
47. "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;
48. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
49. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
50. 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.
51. "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.
52. "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.

Comment [00137]: Where do these definitions come from? They are hardly used in the text, are these terms necessary?

PORTUGAL

Projet de guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police

Commentaires et suggestions rédactionnelles au document T-PD (2016)02rev8 du 12 juillet.

Note :

Nous suivons la numérisation de chaque document et indiquons le paragraphe dans chaque numéro où se trouve le texte objet de suggestion.

2. Collecte et utilisation des données

« La collecte et l'utilisation de données à caractère personnel à des fins policières devrait se limiter à ce qui est nécessaire à la prévention, l'investigation et la répression d'infractions pénales ainsi qu'à l'exécution de sanctions pénales et au traitement de données à caractère personnel ayant pour finalité le maintien de l'ordre public. »

On propose donc **d'éliminer tout ce qui est entre parenthèse dans ce paragraphe.**

« 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. »

On propose d'éliminer tout ce qui est entre parenthèse dans ce paragraphe. Nous considérons que l'exemple donné n'est pas le meilleur ni réellement nécessaire.

3. Utilisation ultérieure des données

« Exemple : les données biométriques recueillies à des fins d'immigration peuvent être traitées, si la loi l'autorise, pour des utilisations répressives telles que les contrôles des personnes recherchées pour un crime, **par exemple la criminalité grave et organisée et le terrorisme.** Toute utilisation doit être licite et proportionnée. »

Nous proposons cette rédaction.

4. Information des personnes concernées

« 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 des informations sur le traitement de ses données et la conservation prolongée de celles-ci, si l'on considère que ces informations peuvent nuire à l'enquête. **Le devoir d'informer l'intéressé doit être satisfait aussitôt que possible dans le cadre de la procédure pénale. L'information peut être transmise directement à la personne concernée où, si cela n'est pas possible où souhaité, à son représentant légale.** »

Nous proposons cette rédaction.

6. Utilisation de techniques d'enquête spéciales

«La police **doit** toujours choisir les moyens les moins intrusifs de traitement de données durant ses opérations. Dans le cas où elle peut employer des méthodes moins intrusives pour aboutir au but recherché, elle doit les privilégier. ~~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.~~ »

L'utilisation du mot « doit » se justifie parce qu'il s'agit d'un devoir en hommage aux principes applicables, notamment celui de la proportionnalité.

Je suggère effacer la dernière phrase. Ce qui était nécessaire dire, c'est déjà dit. La protection de données à caractère personnel ne doit pas interférer dans l'activité de la police pour dire qu'elle technique elle doit utiliser dès que les normes e principes de protection de données soit respectés.

7. Introduction de nouvelles technologies de l'information

~~« Lorsque de nouveaux moyens techniques de traitement des données deviennent opérationnels, il est souhaitable de procéder à la respective réglementation si nécessaire. L'application des nouveaux moyens techniques doit être assujettie à des analyses d'impact. »~~

On suggère cette rédaction. La phrase telle qu'elle était n'était pas claire. L'analyse d'impact en question est celle de cette technologie.

Un exemple : l'utilisation des drones peut être tout-à-fait intéressante pour les medias et bien aussi pour autres secteurs d'activité, mais elle est la cause de pas mal de préoccupations en ce qui concerne la protection de la vie privé, entre autres préoccupations, notamment, par exemple, en ce qui concerne les dangers pour l'aviation civile. En vue de cela ont procédé à la réglementation de son utilisation.

~~« Exemple : la mise en place d'un système de reconnaissance faciale automatique devrait faire l'objet de consultations pour que les risques encourus par les droits de l'intéressé soient clairement indiqués. S'il le faut, 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. »~~

Peut-être on pourrait éliminer la première phrase. Non pas parce qu'elle soit incorrecte, mais parce la deuxième contient ce qui est permanent, étant la première un exemple d'une certaine technologie, intéressante, pertinente aujourd'hui mais, peut-être obsolète d'un un futur proche. Le principe de la neutralité serait aussi invocable pour justifier qu'on soit détaillé, par exemple sur l'utilisation des données biométriques, sans toutefois identifier telle ou telle technologie biométrique.

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 que l'Internet des choses présente en matière de sécurité, cette technologie

T-PD (2017)16

exige de prendre 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. »

La première phrase n'a pas de sens. La police utilise l'Internet donc il y a l'Internet des choses ?! L'expression « Internet des choses » n'intervienne que, parce que précisément des choses, les plus diverses (une caméra, un véhicule, notamment des drones, etc.), ayant la capacité de traiter information à caractère personnelle de façon autonome en utilisant le réseau, en faisant l'envoi des données à caractère personnelle aux officiers de police ou à la police en tant qu'institution.

C'est-à-dire, il n'y a pas d'Internet des choses quand il s'agit seulement de communication de données entre personnes.

« Exemple : compte tenu de possibles problèmes de sécurité, les « lunettes intelligentes », directement reliées aux bases de données pertinentes, utilisées par la police ne doivent pas être directement liées à une base de données nationale des casiers judiciaires ; elles devraient recueillir des informations qui seront ensuite téléchargées dans un environnement informatique sécurisé pour analyses ultérieures. »

L'exemple est intéressant mais plus que de ce centrer sur tel ou tel « chose » du réseau (lunettes intelligentes, drones où autre, y inclus l'appareil de télévision domestique), je crois qu'il faut surtout dire que l'Internet des choses pose des problèmes accrus de sécurité complexes relatives au fonctionnement de la chose en soit et ceux relatives à la sécurité du réseau en lui-même.

Big data et profilage dans les services de police

On suggère qu'on fasse le renvoi pour nos documents sur le profilage (Recommandation CM/Rec(2010)13 du Comité des Ministres aux Etats membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage) et les méga données (Lignes directrices sur la protection des personnes à l'égard du traitement des données à caractère personnel à l'ère des méga données).

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 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 survey¹⁹ 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 clear guidance on what the principles imply at an operational level.

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, the essential objectives of general public interest (prevention, investigation and prosecution of criminal offences, the execution of criminal penalties and maintenance of public order) are followed in the respect of the fundamental 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

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that data processing within the police should be based on predefined, clear and legitimate purposes that it 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. It should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally the data which are processed within the police 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 and the execution of criminal penalties and for the maintenance of public order. 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 that which is necessary for the purpose of prevention, investigation and prosecution of criminal offences and the execution of criminal

Comment [00138]: The idea of balance is disputable, as it puts on equal level 'objectives' and fundamental rights. Rather than opposing them, we would suggest to present them as complementary.

The police objective shall always be one of a general interest. Once this is the case, then the interference should be proportionate which means an assessment takes into account the advantages of the measure which serves the public interest and its impact on the fundamental rights.

Deleted: a balance is struck between

Deleted: ,

Deleted: and the

Deleted: for

¹⁹ See Report "[Twenty-five years down the line](#)" – by Joseph A. Cannataci.

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.

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 (foreseeable and publicly accessible), pursue a legitimate aim and be limited to what is necessary to achieve that legitimate aim.

Prior to and during the collection of such data the question of whether such collection and processing is necessary for the investigation should always be asked. During collection, provided that all legal requirements are met, larger scale of personal data can be processed. After the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be 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. For instance, 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).

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). Subsequent use of data is considered for the use of this guide as a new data processing operation which has to fulfil all the criteria and conditions applicable to the collection and the use of data.

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

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) must meet the applicable legal requirements for the processing of personal data: it should be provided by a law, which is foreseeable and accessible, and the processing should be necessary and proportionate to the legitimate aim pursued.

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 personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set in point 2. The general rule is that 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.

It should be noted however, that any subsequent use of personal data, in particular in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.

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

Comment [00139]: We consider it does constitute an interference in itself, the thing is whether this interference is legally acceptable. The CJEU doctrine and the ECtHR take the same approach when it comes to the storage of data by public authorities. See for instance EDPS 'necessity toolkit', section II.5 and section III, step 2 for the references to case-law as to what constitutes an interference (https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en)

Art. 29 WP has also adopted an opinion on this issue: Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector

Deleted: can

Deleted: clear

Deleted: available

Deleted: the personal data collected

Comment [00140]: Redrafted to clarify that necessity applies already at the stage of collection.

Deleted: In this context

Comment [00141]: Following the case-law (see also the recent Tele2 judgement), there must be a link, between the offence and the people suspected to be involved in the offence. We would suggest to use this expression.

Deleted: for the relevant

Deleted: people

Comment [00142]: Previous version mentioned 'strictly' necessary. We are not sure why this was deleted. We would support that this is brought back in the text.

Deleted: foreseen

Comment [00143]: The wording is not clear in our view. The basis is purpose limitation, with exceptions. We suggest deleting and replacing as follows:
"personal data collected for law enforcement purposes should in principle be used exclusively for the purposes identified and should not be used in any way that is incompatible with the original purpose at the time of collection.
Any other use of the data for another purpose should be framed by the law and subject to strict conditions and guarantees."

more severe crime can override the interest of prosecuting less severe crimes, it is advisable for the police to look at international good practice and to enhance their exchange of information on the matter with other police bodies. This does not represent any obstacle to the use of data of these persons for police purpose if all legal requirements as put forward in point 2 are met.

Example - Biometric data taken for immigration purposes can be processed for law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Any such use should be proportionate.

Deleted: lawful and

4. 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 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 *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 excepted if a restriction applies, taking 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: ,

Comment [00144]: We should also stress that as soon as information can be given without jeopardising the purpose of the data use, it should be provided to the data subjects (ECtHR, Zakharov v. Russia, para. 287, Szabo and Vissy v. HU, para. 86)

Deleted: provided should strike the balance

Deleted: between all interests concerned and also, most importantly

Deleted: e

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. Information provided should include details about the conditions under which exceptions apply to the data subject's rights and how they can submit an appeal 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. In respect of making information available which highlight data protection and data subjects' rights, this is the responsibility of the data controller to provide.

According to the second obligation of giving data subject specific information regarding their data *upon request* for access, the data controller has to inform the individuals on the data processing activities that it has pursued with their data. This means that if an individual has its data collected during the course of an investigation, as soon as circumstances safely permit, the police should advise the individual of the data processing if there is such request. The information should be provided in clear and plain language.

Formatted: Font: Italic

The law can provide that the right to be informed may be limited, should providing such information prejudice the investigation, or another important police mission, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding notification of data processing however should be used only sparingly and where it can be clearly justified.

Deleted: ,

Comment [00145]: Is this stated in law/jurisprudence? This looks very wide.

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.

Comment [00146]: Is such example broadly acknowledged? We would rather support an example referring to 'dormant' terrorist cells.

5. 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 have to be incorporated into national legislation in a manner compatible with the ECtHR jurisprudence.

Comment [00147]: We suggest to use the language of the ECtHR 'foreseeable and accessible law'

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 17) in case of some specific data processing activities. In particular it affects those 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 or the protection of the rights and fundamental freedoms of others. Other applicable exceptions are foreseen in Article 3 Convention 108.

If the exception, based on national law 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 for instance providing information under data protection principles would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police.

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 can be shared with national security agencies in respect of national security, for example to prevent a terrorist attack. In order to rapidly identify the perpetrator, police shall cooperate 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 security agencies. In such a case, police should share its data with national security agencies according to general, well-established procedures foreseen by law, including strong safeguards, (such as, depending on the nature of the case, judicial authorisation, strict rules on purpose limitation)

6. 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, it must be remembered that 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, those considerations have to be balanced with cost-effectiveness, use of resources and 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 covert surveillance measures, such as wiretapping.

7. Introduction 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.

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.

Deleted: ,

Deleted: the use of those rules and principles

Comment [LA148]: This is very broad. We suggest deleting or clarifying.

Deleted: However if there is no risk of terrorist attack

Deleted: in which

Deleted: er

Deleted: are put in place

Comment [00149]: The example gave the impression that exceptions can always be used, even when there is no urgent national security issue, as long as procedures are foreseen. This would empty the principles from their substance.

Comment [00150]: In addition, we wonder whether this example is realistic with data sharing often taking place the other way around, i.e. the national security agencies share data with the police when there is an imminent risk of such a terrorist attack. See if the example should be kept or adapted.

Deleted: er

Deleted: with a view of ensuring an enhanced protection to the individual's right to privacy and data protect

Deleted: on

Comment [00151]: There is always an interference, see our comment above

Deleted: can

Deleted:

Comment [00152]: It is not clear which "considerations" are meant here. Moreover, while a measure shall be effective to be necessary in the language of the ECHR, the cost-effectiveness alone would not justify the selection of one measure against another one. We would suggest to avoid reference to cost-effectiveness and use of resources, unless we can better explain it.

Comment [00153]: The intrusive - or less intrusive - character of the measures is not clear. Why is discreet surveillance less intrusive than covert surveillance or wiretapping?

Deleted: continuous (i.e

Deleted: .

Deleted:)

Deleted: every

Deleted: by

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. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights if measures are not taken to mitigate such risks.

Comment [00154]: But the use of such new technologies should be foreseen by law, and data protection authorities should be consulted at that stage. We suggest clarifying this, also in the example below (see also comment).

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 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 contained 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 are to be reported to or made available to the data protection authority. The Data protection authority is preferably to be consulted during the legislative procedure.

Comment [00155]: The connection of this sentence with the rest of the example is not clear. It seems that it is about a DPIA on a specific processing activity, but the last sentence refers to a legislative process which seems more general.

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

We suggest clarifying the articulation between prior consultation on police draft legislation and specific DPIAs.

Example - Introducing an automatic facial recognition system would need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed, 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 which is directly linked to relevant databases 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.

Comment [00156]: We do not understand how glasses directly connected to a database should not be connected to a database. We suggest deleting the first half of that part of the sentence. The kind of database referred to is not clear either.

Big data 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.

Deleted: in the police

Big data technologies enable bulk collection and analysis of a vast quantity of data generated by various sources, such as electronic communication services and wearable devices, aggregated with other bulk data. This could potentially and inadvertently interfere with the right to privacy and data protection.

Deleted: s

The Council of Europe's Guidelines on the protection of individuals with regard to the processing of personal

data in a world of Big Data²⁰ 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 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.

Comment [00157]: And lead also to unlawful data processing (lack of legal basis...)

Where big data relies on personal data, data controllers should take due account of 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 traditional methods of investigation.
- Its use is necessary and proportionate for police purpose.
- 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 the exceptions mentioned in point 5, 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 make the data subjects aware of this secondary use.
- Lawfulness of the processing – including possible further use - and compliance with the conditions set by Article 8 ECHR should be demonstrated.
- An information security policy should be in place.
- 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.

Deleted: Where possible

Comment [00158]: This could be interpreted a contrario as allowing incompatible further use without informing the data subject.

Deleted: compatible

8. 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.

Comment [00159]: Safeguards is quite important, perhaps more detailed guidance should be given. It is a bit misleading as processing sensitive data separately is not enough in itself as safeguard.

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 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. criminal investigation) 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, profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal

Comment [00160]: The same as above, we should give more precise guidance what appropriate safeguard means.

²⁰ Document T-PD(2017)1

effect significantly affecting the data subject. 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 inhabitants are from the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

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.

9. Storage of data

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

Comment [00161]: How is it in line with point 3. on 'subsequent use of data'?

There should be a clear distinction in how police store 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. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

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 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.

Comment [00162]: Same comment as on p. 2: we suggest to reinsert 'strictly' necessary.

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, 4 years later the evidence 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. 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 revision of the case have also expired. Likewise, if, after 4 years, the investigation is still ongoing 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.

When shaping internal policies 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.

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. This uses a classification system to facilitate 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.

Deleted: if feasible

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

10. 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. As a general rule police can 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 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.

11. 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 10 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the communicated data could be used for non-law enforcement purposes.

As an exception, communication 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.

12. 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 missions, 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.

13. 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 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.

Deleted: organisations

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 "Rules Governing the Processing of Data and its 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

T-PD (2017)16

Cybercrime Convention (CETS No. 185) can be applicable²¹ 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.

An appropriate level of data protection should be guaranteed if data are to be transferred to countries not participating in 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 specific 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 has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

Deleted: with

The international transfer of personal data to a non-police 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 police data to a private body residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases where it is provided by legal means and where the emergency, the gravity of the crime, its trans-border nature and the fact that the involvement of the local police would compromise the purpose of the investigation because of the length of the procedure. 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. 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.

Comment [00163]: This is about a transfer TO a private body, while the rest of the paragraph seems to be about the transfer FROM a private body.

Comment [00164]: This is typically argued when information is requested FROM A PRIVATE BODY rather than FROM THE POLICE because of delays in public procedures.

The text should be clarified and made consistent with the first sentence of the paragraph.

In addition, we have serious doubts about the proportionality of such a procedure, which circumvents the formal channels for exchange of data (including international agreements).

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.

14. 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

²¹ This is without prejudice to the right of the Committee of Convention 108 and of other instances having such power to assess and to review, if necessary, the level of data protection guaranteed by those multilateral agreements.

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 checked at source before being communicated and their degree of accuracy or reliability indicated. The quality of data can be assessed up to the moment of communication.

Comment [00165]: This was a useful precision in a previous version, so we would advise maintaining it.

Example: If personal data is sent that contains incorrect data (personal or otherwise) 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: ¶

15. 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 only exception to this is when the sending authority, based on legal provisions, gives agreement to any further use and if the processing is based on law, is necessary and vital for the recipient to fulfil their task, is in the interest of the data subject or for humanitarian reasons or is necessary to prevent serious and imminent risk to public order or public security and an appropriate level of data protection is guaranteed by the recipient 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 as well).

16. 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 in accordance with domestic legislation 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 proportionate.

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 the police.

17. 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 personal data and on the

Comment [00166]: We suggest to structure a bit more this part to make it more readable:

1. . right to information
2. . right of access
3. . right of rectification
4. . right of erasure

T-PD (2017)16

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 [avoiding to use 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 (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 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 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.

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 which can only be used if it is vital for the performance of a legal task of law enforcement 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. If restriction was to be used, the data subject still has to have an answer, albeit any answer should take into consideration according national law or practice all circumstances to which the restriction is applicable.

Comment [00167]: Considering moving the next 'example' here.

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 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). In case of a restriction, 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.

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.

Comment [00168]: This is not an example of what is said just above, but an exception to it. It is more connected to what is said higher above (last but 4th paragraph on page 12). We suggest to move it there or delete it as it does not bring much added value.

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.

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 giving a testimony in a criminal case.

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 same countries' 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 5, 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.

Restrictions to the rights of data subjects 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 refusals provided to 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.

Comment [00169]: This is not very clear: if kept, it should be illustrated by an example.

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 **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: require

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.

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

Deleted: um

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.

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 is not obliged to 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 decide 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.

Comment [00170]: This could be shortened as repetitive, and/or moved above.

Comment [00171]: When is it serious? What are the criteria? Who will decide whether it seriously interfere with rights? If it is the controller who can decide, it would cause a conflict of interest.

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 may **seriously** interfere with the rights and fundamental freedoms of data subjects.

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."

T-PD (2017)16

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 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.

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 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 is an integral part of 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-Enhancing Technologies (PETs)

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

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 **independent** 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 or the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

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.**

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 **and resources** to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Comment [00172]: This is drafted more for the glossary than as a guidance. Consider moving the part to the glossary or making more concrete suggestions.

Comment [00173]: An important element of independence is that the authority cannot be instructed and cannot accept instruction from anybody.

The president/commissioner of the authority cannot be resigned before the official term of office ends.

For further information please see: ECJ decisions: C-518/07. against Germany; C-614/10. against Austria, C-288/12. against Hungary

Comment [00174]: We suggest to add that these tools shall be efficient and enforceable.

Glossary/Definitions

For the purposes of this Guide:

53. "personal data" means any information relating to an identified or identifiable individual ("data subject");
54. "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;
55. "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;
56. "soft data" (evidence based on testimony) means data acquired through testimony of person involved in the investigation;
57. "hard data" (evidence based on documents) means data acquired from official documents or other certified sources;
58. "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;
59. "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;
60. "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;
61. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
62. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
63. 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.
64. "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.
65. "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.

**INTERNATIONAL COMMITTEE OF THE RED CROSS / COMITÉ INTERNATIONAL DE LA
CROIX-ROUGE (ICRC / CICR)**

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 survey²² 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 clear guidance on what the principles imply at an operational level.

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 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 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

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that data processing within the police should be based on predefined, clear and legitimate purposes that it 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. It should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally the data which are processed within the police 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 and the execution of criminal penalties and for the maintenance of public order. 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 that which is necessary for the purpose of prevention, investigation and prosecution of criminal offences and the execution of criminal

²² See Report "[Twenty-five years down the line](#)" – by Joseph A. Cannataci.

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.

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.

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. During collection, provided that all legal requirements are met, larger scale of personal data can be processed. After the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be 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).

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 the relevant people.

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 at the time of collection, unless this is provided for in law (see Art 9 of Convention 108). Subsequent use of data is considered for the use of this guide as a new data processing operation which has to fulfil all the criteria and conditions applicable to the collection and the use of data.

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

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) must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be necessary and proportionate to the legitimate aim pursued.

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 personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set in point 2. The general rule is that 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.

It should be noted however, that any subsequent use of personal data, in particular in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.

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 international good practice and to enhance their exchange of information on the matter with other police bodies. This does not represent any obstacle to the use of data of these persons for police purpose if all legal requirements as put forward in point 2 are met.

Example - Biometric data taken for immigration purposes can be processed for law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Any such use should be lawful and proportionate.

4. 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 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 *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 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.

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. Information provided should include details about the conditions under which exceptions apply to the data subject's rights and how they can submit an appeal against a decision of the data controller in reply to their request.

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. In respect of making information available which highlight data protection and data subjects' rights, this is the responsibility of the data controller to provide.

According to the second obligation of giving data subject specific information regarding their data upon request for access, the data controller has to inform the individuals on the data processing activities that it has pursued with their data. This means that if an individual has its data collected during the course of an investigation, as soon as circumstances safely permit, the police should advise the individual of the data processing if there is such request. The information should be provided in clear and plain language.

The law can provide that the right to be informed may be limited, should providing such information, prejudice the investigation, or another important police mission, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding notification of data processing however should be used only sparingly and where it can be clearly justified.

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 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.

5. 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 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 2,3,4,7 as well as to the data subjects' rights (point 17) in case of some specific data processing activities. In particular it affects those 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 or the protection of the rights and fundamental freedoms of others. Other applicable exceptions are foreseen in Article 3 Convention 108.

If the exception, based on national law 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 the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police.

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 can be shared with national security agencies in respect of national security, for example to prevent a terrorist attack. In order to rapidly identify the perpetrator, police shall cooperate 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 security agencies. 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 (such as judicial authorisation, stricter rules on purpose limitation)with a view of ensuring an enhanced protection to the individual's right to privacy and data protection.

6. 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, 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, those considerations have to be balanced with cost-effectiveness, use of resources and 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 covert surveillance measures, such as wiretapping.

7. Introduction 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.

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, continuous (i.e. repeated at reasonable intervals) and that it should touch upon every phase of the data processing activity. The relevance of the DPIA shall be checked by 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. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights.

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 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 contained and by whom the data is being accessed as well as information on retention of data, log policy and access policy.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data are to be reported to or made available to the data protection authority. 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 would need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed, 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 which is directly linked to relevant databases 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.

Big data and profiling 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 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 potentially and inadvertently interfere with the right to privacy and data protection.

The Council of Europe's Guidelines on the protection of individuals with regard to the processing of personal

data in a world of Big Data²³ 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 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 take due account of 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 traditional methods of investigation.
- Its use is necessary and proportionate for police purpose.
- 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.
- Where possible, 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 compatible purpose the data controller should make the data subjects aware of this secondary use.
- Lawfulness of the processing and compliance with the conditions set by Article 8 ECHR should be demonstrated.
- An information security policy should be in place.
- 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.

8. 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 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. criminal investigation) 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, profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal

²³ Document T-PD(2017)1

effect significantly affecting the data subject. 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 inhabitants are from the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

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 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.

9. Storage of data

As pointed out in Point 2 data shall be processed until they have served the purpose for which they were collected. 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. 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 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. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

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 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, 4 years later the evidence 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. 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 revision of the case have also expired. Likewise, if, after 4 years, the investigation is still ongoing 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.

When shaping internal policies 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.

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. This uses a classification system to facilitate 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 (if feasible: 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.

10. 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. As a general rule police can 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 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.

11. 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 10 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the communicated data could be used for non-law enforcement purposes.

As an exception, communication 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.

12. 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 missions, 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.

13. International transfer

Any transfer of police data internationally should be limited to police organisations 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 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. 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 "Rules Governing the Processing of Data and its 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

T-PD (2017)16

No. 185) can be applicable²⁴ 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.

An appropriate level of data protection should be guaranteed if data are to be transferred to countries not participating in 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 specific 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 with 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 has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

The international transfer of personal data to a non-police 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 police data to a private body residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases where it is provided by legal means and where the gravity of the crime, its trans-border nature and the fact that the involvement of the local police would compromise the purpose of the investigation because of the length of the procedure. 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. 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.

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.

14. 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

²⁴ This is without prejudice to the right of the Committee of Convention 108 and of other instances having such power to assess and to review, if necessary, the level of data protection guaranteed by those multilateral agreements.

transferring it is always advisable to double-check the quality of data, if it is correct, up-to-date, complete. The quality of data can be assessed up to the moment of communication.

Example: If personal data is sent that contains incorrect data (personal or otherwise) 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.

15. 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 only exception to this is when the sending authority, based on legal provisions, gives agreement to any further use and if the processing is based on law, is necessary and vital for the recipient to fulfil their task, is in the interest of the data subject or for humanitarian reasons or is necessary to prevent serious and imminent risk to public order or public security and an appropriate level of data protection is guaranteed by the recipient 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 as well).

16. 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 in accordance with domestic legislation 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 proportionate.

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.

17. 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

T-PD (2017)16

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 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 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.

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 which can only be used if it is vital for the performance of a legal task of law enforcement 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. If restriction was to be used, the data subject still has to have an answer, albeit any answer should take into consideration according national law or practice all circumstances to which the restriction 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 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). In case of a restriction, 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.

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.

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.

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 giving a testimony in a criminal case.

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 same countries' 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 5, 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 may be imposed by national law for important objectives of general public interest including humanitarian purposes.](#)

Restrictions to the rights of data subjects 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 refusals provided to 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 to retain 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.

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.

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 is not obliged to 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 decide 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.

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 may seriously interfere with the rights and fundamental freedoms of data subjects.

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

Comment [00175]: This point was raised during the last T-PD meeting and there was no objection to it. This suggestion is in line with recital 73 of the GDPR. Indeed, there may be instances where legislation limits data subjects' rights in relation to humanitarian purposes.

T-PD (2017)16

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 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.

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 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 is an integral part of security. Data protection and security may be embedded directly into information systems and processes 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-Enhancing Technologies (PETs)

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

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 or the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

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.

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:

66. "personal data" means any information relating to an identified or identifiable individual ("data subject");
67. "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;
68. "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;
69. "soft data" (evidence based on testimony) means data acquired through testimony of person involved in the investigation;
70. "hard data" (evidence based on documents) means data acquired from official documents or other certified sources;
71. "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;
72. "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;
73. "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;
74. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
75. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
76. 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.
77. "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.
78. "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.

INTERPOL

Comments INTERPOL Data Protection Office dd.20170720

Provisions subject to amendments**Section 2. Collection of data and use of data, paragraph 3:**

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. During collection, provided that all legal requirements are met, larger scale of personal data can be processed. After the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be deleted.

Section 13. International transfer, paragraph 3:

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. 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 "Rules Governing the Processing of Data" and its "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) can be applicable²⁵ 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.

Comment [00176]: Comments

20170720.IDPO

INTERPOL Data Protection Office noted in its earlier comments that the practical guide had very rightly expanded the scope of application to predictive policing which has been developing as an important area of today's police work. In this regard, the first sentence and especially "... whether the personal data collected is necessary for the investigation should always be asked" could be deemed to be more narrow than the scope set out in section 1 (scope) which has clearly been expanded to predictive policing as they provide a more realistic representation of the diverse missions of LEAs. It is important to ensure that the rest of the document is consistent with these amendments.

Comment [00177]: The exact title is: "INTERPOL's Rules on the Processing of Data".

Comment [00178]: The Rules relating to the Control of Information and Access to INTERPOL's Files were abrogated at the 85th INTERPOL General Assembly (Nov 2016) and replaced by the "STATUTE OF THE COMMISSION FOR THE CONTROL OF INTERPOL'S FILES"

²⁵ This is without prejudice to the right of the Committee of Convention 108 and of other instances having such power to assess and to review, if necessary, the level of data protection guaranteed by those multilateral agreements.

NATIONAL INSTITUTE FOR TRANSPARENCY, ACCESS TO INFORMATION AND PERSONAL DATA PROTECTION / INSTITUT NATIONAL DE TRANSPARENCE, ACCES A L'INFORMATION ET PROTECTION DES DONNEES DU MEXIQUE (INAI)

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 survey²⁶ 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 clear guidance on what the principles imply at an operational level.

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 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 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

All data processing has to comply with the necessity, proportionality and purpose limitation principles. This implies that data processing within the police should be based on predefined, clear and legitimate purposes that it 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. It should furthermore be adequate, relevant and non-excessive in relation to the purposes. Finally the data which are processed within the police 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 and the execution of criminal penalties and for the maintenance of public order. Where 'police' is used in the text, it

²⁶ See Report "[Twenty-five years down the line](#)" – by Joseph A. Cannataci.

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 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 or the suspicion thereof) and where personal data is processed for the purpose of the maintenance of public order.

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.

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. During collection, provided that all legal requirements are met, larger scale of personal data can be processed. After the collection phase a thorough analysis is needed in order to assess which data are to be retained and which are to be 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).

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 the relevant people.

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 at the time of collection, unless this is provided for in law (see Art 9 of Convention 108). Subsequent use of data is considered for the use of this guide as a new data processing operation which has to fulfil all the criteria and conditions applicable to the collection and the use of data.

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

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) must meet the applicable legal requirements for the processing of personal data: it should be foreseen by law, and the processing should be necessary and proportionate to the legitimate aim pursued.

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 personal data subsequently used should be linked to a police purpose and must fulfil the criteria and conditions set in point 2. The general rule is that 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.

Comment [00179]: It is suggested to recognize the principle of responsibility.

Comment [00180]: It is suggested to specify the final destination of the personal data (blocking / deletion).

It should be noted however, that any subsequent use of personal data, in particular in respect of vulnerable individuals such as victims, minors, or of those enjoying international protection should be based on solid legal grounds and thorough analysis.

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 international good practice and to enhance their exchange of information on the matter with other police bodies. This does not represent any obstacle to the use of data of these persons for police purpose if all legal requirements as put forward in point 2 are met.

Example - Biometric data taken for immigration purposes can be processed for law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Any such use should be lawful and proportionate.

4. 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 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 *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 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.

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. Information provided should include details about the conditions under which exceptions apply to the data subject's rights and how they can submit an appeal against a decision of the data controller in reply to their request.

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. In respect of making information available which highlight data protection and data subjects' rights, this is the responsibility of the data controller to provide.

According to the second obligation of giving data subject specific information regarding their data upon request for access, the data controller has to inform the individuals on the data processing activities that it has pursued with their data. This means that if an individual has its data collected during the course of an investigation, as soon as circumstances safely permit, the police should advise the individual of the data processing if there is such request. The information should be provided in clear and plain language.

The law can provide that the right to be informed may be limited, should providing such information, prejudice the investigation, or another important police mission, state interests (such as public security, national security) or the protection of the rights and freedoms of others. Withholding notification of data processing however should be used only sparingly and where it can be clearly justified.

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 if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved, the

Comment [00181]: It is suggested to clarify that during the exchange of personal information, all persons involved in the process will observe the obligation of confidentiality.

Comment [00182]: It is suggested that the data subject be informed about this situation when his / her personal data are collected

data subject should be informed about the fact that she or he was subject to such a measure.

5. 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 have to be incorporated into national legislation in a manner compatible with the ECtHR jurisprudence.

Comment [00183]: It is suggested to clarify that the purpose should also be determined clearly.

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 17) in case of some specific data processing activities. In particular it affects those 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 or the protection of the rights and fundamental freedoms of others. Other applicable exceptions are foreseen in Article 3 Convention 108.

If the exception, based on national law 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 the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other missions of the police.

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 can be shared with national security agencies in respect of national security, for example to prevent a terrorist attack. In order to rapidly identify the perpetrator, police shall cooperate 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 security agencies. 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 (such as judicial authorisation, stricter rules on purpose limitation) with a view of ensuring an enhanced protection to the individual's right to privacy and data protection.

6. 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.

Comment [00184]: It is suggested to clarify that, regardless of the method(s) for an investigation, the data controller is obliged to comply with the general principles of personal data protection, unless a law exempts such compliance.

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, those considerations have to be balanced with cost-effectiveness, use of resources and 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 covert surveillance measures, such as wiretapping.

7. Introduction 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.

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, continuous (i.e. repeated at reasonable intervals) and that it should touch upon every phase of the data processing activity. The relevance of the DPIA shall be checked by 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. It may do so if the DPIA it previously conducted demonstrates a significantly high risk to the individual's rights.

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 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 contained and by whom the data is being accessed as well as information on retention of data, log policy and access policy.

Example: Detailed information on national reference files such as purpose, data controller etc. containing fingerprint data are to be reported to or made available to the data protection authority. 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 would need consultation in order to obtain a clear picture of the risks to individual's rights. Where needed, 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 which is directly linked to relevant databases 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.

Big data and profiling 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 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 potentially and inadvertently interfere with the right to privacy and data protection.

The Council of Europe's Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data²⁷ 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 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 take due account of 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 traditional methods of investigation.
- Its use is necessary and proportionate for police purpose.
- 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.
- Where possible, 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 compatible purpose the data controller should make the data subjects aware of this secondary use.
- Lawfulness of the processing and compliance with the conditions set by Article 8 ECHR should be demonstrated.
- An information security policy should be in place.
- 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.

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

²⁷ Document T-PD(2017)1

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.

Comment [00185]: It is suggested to emphasize the establishment of measures that prevent the most insignificant information leakage.

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 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. criminal investigation) 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, profiling should be avoided as a general rule and should only be permitted where appropriate safeguards have been put in place to tackle the potential risk of discrimination or of adverse legal effect significantly affecting the data subject. 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 habitants are from the same ethnical origin. There should be additional criteria to allow the processing of data on this ground.

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 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.

9. Storage of data

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

Comment [00186]: It is suggested to add "in a definitive and safe way".

There should be a clear distinction in how police store 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. Safeguards should be in place for persons who are not suspected of having committed, or have not been convicted of, a criminal offence.

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 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, 4 years later the evidence 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. 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 revision of the case have also expired. Likewise, if, after 4 years, the investigation is still ongoing 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.

When shaping internal policies 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.

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. This uses a classification system to facilitate 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 (if feasible: 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.

10. 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. As a general rule police can 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 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.

11. 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 10 should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the communicated data could be used for non-law enforcement purposes.

As an exception, communication 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.

12. 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 missions, 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.

13. International transfer

Any transfer of police data internationally should be limited to police organisations 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 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. 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 "Rules Governing the Processing of Data and its 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) can be applicable²⁸ 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.

An appropriate level of data protection should be guaranteed if data are to be transferred to countries not participating in 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 specific 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 with 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 has, in place, appropriate legal protection in terms of personal data processing and can guarantee an appropriate level for the protection of personal data.

The international transfer of personal data to a non-police 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.

²⁸ This is without prejudice to the right of the Committee of Convention 108 and of other instances having such power to assess and to review, if necessary, the level of data protection guaranteed by those multilateral agreements.

The international transfer of police data to a private body residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases where it is provided by legal means and where the gravity of the crime, its trans-border nature and the fact that the involvement of the local police would compromise the purpose of the investigation because of the length of the procedure. 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. 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.

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.

14. 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. The quality of data can be assessed up to the moment of communication.

Example: If personal data is sent that contains incorrect data (personal or otherwise) 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.

15. 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 only exception to this is when the sending authority, based on legal provisions, gives agreement to any further use and if the processing is based on law, is necessary and vital for the recipient to fulfil their task, is in the interest of the data subject or for humanitarian reasons or is necessary to prevent serious and imminent risk to public order or public security and an appropriate level of data protection is guaranteed by the recipient 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 as well).

16. 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.

Comment [00187]: It is suggested to clarify that the private parties that receive police data are subject to the legal framework on personal data protection applicable to them.

Comment [00188]: It is suggested to establish a standard that requires data controllers to have secure channels of communication or transfers that allow him to keep the confidentiality, integrity and availability of personal data.

Comment [00189]: It is suggested to consider that the exception derives from the consent of the data subject, and not from the consent of the sending authority, since the processing of personal data is subject to the original purpose.

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 in accordance with domestic legislation 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 proportionate.

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.

17. 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 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 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.

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 which can only be used if it is vital for the performance of a legal task of law enforcement 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. If restriction was to be used, the data subject still has to have an answer, albeit any answer should take into consideration according national law or practice all circumstances to which the restriction 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 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). In case of a restriction, 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.

T-PD (2017)16

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.

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.

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.

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 giving a testimony in a criminal case.

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 same countries' 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 5, 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.

Restrictions to the rights of data subjects 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 refusals provided to 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 to retain 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.

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.

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 is not obliged to 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 decide 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.

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 may seriously interfere with the rights and fundamental freedoms of data subjects.

Comment [00190]: It is suggested that the affected data subjects be also notified.

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 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.

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 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 is an integral part of security. Data protection and security may be embedded directly into information systems and processes 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-Enhancing Technologies (PETs)

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

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 or the executive branch of a national administration. It should have sufficient resources to perform its tasks and duties.

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.

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:

79. "personal data" means any information relating to an identified or identifiable individual ("data subject");

80. "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;
81. "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;
82. "soft data" (evidence based on testimony) means data acquired through testimony of person involved in the investigation;
83. "hard data" (evidence based on documents) means data acquired from official documents or other certified sources;
84. "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;
85. "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;
86. "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;
87. "recipient" means a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available;
88. "processor" means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller.
89. 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.
90. "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.
91. "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.