COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 15 June / juin 2017 T-PD(2017)06Mos

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 À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

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

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

Directorate General of Human Rights and Rule of Law /

Direction générale Droits de l'Homme et État de droit

TABLE OF CONTENTS / TABLE DES MATIERES

T-PD(2017)06mos

AUSTRIA / AUTRICHE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 18 May 2017 T-PD (2016)02rev5

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

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

Austrian comments

Directorate General of Human Rights and Rule of Law

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied for ensuring the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").

Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed implementation and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[1] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide 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 their practical application.

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 public safety and public security, 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.

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

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 in a fair, transparent and lawful manner and should 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, i.e. 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.

2. Collection of data and use of data

The processing 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 processing of personal data for law enforcement purposes constitutes an interference with the right to privacy and right to protection of personal data and as such any interference *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.

If police collect personal data it must fit into the legislative framework and should always be in connection with on-going investigations. 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, any "useful" 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 out of purpose. 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).

Comment [001]: the innocence can only be confirmed by a court; data proving the innocence of a data subject may be relevant in the light of Art. 6.2. ECHR; it is therefore suggested to replace this example by another one.

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 strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for law enforcement 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 national law.

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 must meet the same 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.

As it is very easy to use personal data collected for one purpose for another purpose, personal data collected and retained of an individual for police purposes should not be kept and processed in an unstructured manner unless there is a legal basis and operational reason for this. The general rule is that all data held by police have to have a direct link to an investigation and have to be processed in relation with this specific investigation. However in exceptional cases where there is an additional criterion which can validate the legitimacy of the processing the data can be stored in a less structured manner. For example recidivists' data or data related to the members of a terrorist group can be retained longer and in a less structured manner in respect of crime they are charged or convicted of. However even in these cases any subsequent use of personal data, in particular of vulnerable individuals such as victims, minors, disabled people, or enjoying international protection should be based on solid legal grounds and thorough analysis.

In difficult cases such as trafficking in human beings, drug trafficking, sexual exploitation, where victims can often also be 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.

Example - Biometric data taken for immigration purposes can be processed for other law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Conversely, for minor theft (such as theft of a magazine) searches into the DNA registry held for immigration purposes would not be seen as appropriate and would be unlikely to meet the proportionality principle.

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, prior to the data processing, 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 specific 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 can 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 would be the responsibility of the data controller ~~or the processor~~ to provide.

Comment [002]: providing information is always the task of the controller.

According to the second obligation of giving data subject specific information regarding their data, the data controller has to inform the individuals upon request 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. Such provision of information to the data subject may be carried out as provided for under national law. The information should be provided in clear and plain language.

It should be noted, however, that the police do not need to advise the individual of the data processing if they believe that providing this information may prejudice the investigation, for example by allowing them to abscond or destroy evidence. Withholding notification of data processing 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 as to the extent that the data are necessary for this purpose, and that informing the individual would potentially prejudice an on-going or planned investigation.

Comment [003]: It is unclear why this type of processing would justify "long-term data retention".

5. Exceptions

Exceptions can only be used if foreseen by law and constitute a necessary and proportionate measure in a democratic society. This latter means that the measure the exception is based on should be public, open and transparent and in addition detailed enough. Furthermore, the exception can only be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. Finally the measures used have to be subject to a proper external oversight.

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 19) 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 or the protection of the rights and fundamental freedoms of others.

Exceptions to those rules and principles can also be applied if their application would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other essential objectives of general interests.

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.

While it is a perfectly legitimate aim for a state to protect its national security, and therefore for the police to investigate individuals and groups involved in activities such as terrorism, this cannot lead to the permanent, non-controlled and unlimited wiretapping of an individual's mobile phone (*Zakharov vs. Russia case*[2]) or to the use of special investigative techniques (point 6) with only governmental oversight (*Szabó vs. Hungary case*[3]).

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 share personal data stored on identified suspects with national security agencies. However if there is no risk of terrorist attack, police should not share its data with national security agencies as the purpose limitation principle would be infringed.

6. Use of special investigative techniques

The police should always choose the most efficient and straightforward method(s) for an investigation. 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 right to privacy and personal data and with other human rights. When deciding upon the method of investigation, those considerations have to be balanced with cost-effectiveness, use of resources and efficiency of investigations.

[2] ECHR Roman Zakharov v. Russia, 47143/06
[3] ECHR Szabó and Vissy v. Hungary, 37138/14

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. Use of new data processing technologies

It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance to existing privacy and data protection standards.

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 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 supervisory 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 [004]: It is suggested to add "data protection" because "supervisory authority" is not defined in the annex; it should be clear that a "supervisory authority" in this context refers to the data protection authority.

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.

Following consultation, the data controller should implement any necessary measures and safeguards that have been agreed prior to starting the processing operations.

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

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: National reference files containing fingerprint data should have a valid legal basis. Detailed information on the files, such as purpose, data controller etc. should be reported to or made available to the supervisory authority.

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

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

Example: In light of their potential security vulnerabilities smart glass used by police should not be directly connected to a national criminal record data base; they should gather information which is to be downloaded to a secure IT environment for further analysis.

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 way of processing data could potentially cause collateral interference, impacting on individual's fundamental rights, such as 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 Data[4] 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 limited to serious crime.
- 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.
- 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.
- Expertise should be ensured both in operating the big data analytics and in processing the results of the analysis.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals.

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

Comment [005]: It is suggested to add "sensitive data" because the guide sometimes refers to sensitive data.

Comment [006]: those data are per definition em (see e.g. Art. 10 Directive 2016/280) not sensitive data.

[4] Document T-PD(2017)1

opinions, trade-union membership, religious or other beliefs, health or sexual life can only be processed if additional safeguards are prescribed by law. 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.

A careful balance of interest is necessary to determine whether or not and to which extent the police would process sensitive data. A greater use of ~~Privacy Impact Assessment (PIA)~~Data Protection Impact Assessment (DPIA) is recommended in order to ensure that the additional 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.

Comment [007]: See point 7 which speaks of DPIA; for the sake of uniformity DPIA should be used throughout the text.

The collection of data on individuals solely on the basis of sensitive data which is not prescribed by law is prohibited.

Regarding these data, profiling should be avoided as a general rule and should only be permitted where significant additional safeguards have been put in place to tackle the potential risk of discrimination. 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 such as frequent communication with the known members of the group, etc. to allow the processing of data on this ground.

Example - Processing data on purely 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

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 foreseen by law *and* is deemed relevant for a purpose which is not incompatible with the original processing purpose. 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 strictly necessary to achieve the purpose of the investigation.
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. 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~~ may 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. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

Comment [008]: There are, in many legal systems, deadlines for re-opening cases (revision). It is therefore suggested to replay "shall" by "may" because if a data subject is acquitted but the case is re-opened later, it would be better for the police to still have the data. Data should definitely be deleted after the expiry of revision period.

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 judiciary 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 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, firearms certificates and lost property.

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 the investigations they are pursuing. The communication of personal data in general should be subject to the principle of necessity and proportionality and has to serve the purpose of the investigation.

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.

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

Communication of data to any other public bodies is allowable if there is a legal basis to do so. Mutual assistance 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).

Communication to any other public authority is also allowed if it is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to public order or 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 domestically to private bodies. This communication has to be based in law, has to serve the purpose of investigation and can only be done by the authority which is processing the data for the purpose of investigation. Such communication ~~must be subject to additional requirements, such as authorisation of the supervisory body or a magistrate, and~~ should 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.

Comment [009]: Such an obligation does not exist in all national legal systems.

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 and/or authorisation 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 communication 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 and communication, 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.

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 of great use 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.

Communication should always ensure an appropriate level of data protection if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

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

Example - Further onward transfer of data should only be allowed if this is necessary for the same 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 private party 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 a legal measure 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. 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 [0010]: Such evidence gathering touches upon the sovereignty of states and should only be possible if foreseen in a legal instrument

Example: In an investigation 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.

Comment [0011]: The Austrian DPA strongly recommends not use this example because this question is sensitive and touches upon state sovereignty. The use MLATs should be the rule.

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.

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 such cross-referencing of databases.

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 strictly 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 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. The police can if provided by national law refuse to respond to manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a refusal.

It is possible to charge a reasonable administrative fee for the request, if national law permits.
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 the right of access provided for is indirect, the data subject may direct their request to the supervisory authority, which 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).

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. 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.
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 which might jeopardise an investigation and should therefore be excluded for its duration.

Restrictions to the communication of data should only apply to the extent necessary and interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis.

Any 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 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 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.

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 is an essential requirement to ensure safe and appropriate access to data.

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

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

Privacy-by-Design

Privacy 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 has to be established outside of the ~~executive~~ police power and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Comment [0012]: It is suggested to replace “executive” by “police” because in some states the supervisory authority is also part of the “executive branch” (and not part of the judiciary or the legislative branch)

Glossary/Definitions

For the purposes of this Guide:

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

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

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

d. “soft data” means data acquired through testimony of person involved in the investigation;

e. “hard data “means data acquired from official documents or other certified sources;

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

g. “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;

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

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

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

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

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

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

BELGIUM / BELGIQUE

T-PD(2017)06mos

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 18 mai 2017 T-PD (2016)02rev5

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

Projet de guide pratique sur l'utilisation de données à caractère personnel par la police

Direction générale Droits de l'Homme et État de droit

Introduction

La Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel par la police énonce un ensemble général de principes à appliquer dans ce secteur pour garantir le respect du droit à la protection des données et de la vie privée 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 sa mise en œuvre que de sa pertinence. En 2010, le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) a décidé de réaliser une étude[5] sur l'utilisation de données à caractère personnel par la police dans l'ensemble de l'Europe. Cette évaluation a montré que les principes de la Recommandation (87)15 constituaient un point de départ approprié pour élaborer des réglementations s'appliquant à cette question au niveau local et que l'élaboration d'un guide pratique sur l'utilisation de données à caractère personnel par la police, sur la base des principes énoncés par la recommandation, 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 problèmes les plus importants qui peuvent découler 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 leur application pratique.

Ces principes généraux et leurs conséquences pratiques visent à ce qu'un juste équilibre soit trouvé entre différents intérêts durant le travail de la police, tels que la sûreté ou la sécurité publique, 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.

[5] Voir le rapport « Twenty–five years down the line » de Joseph A. Cannataci

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 loyale, transparente et licite, et qu'il soit adéquat, pertinent et non excessif par rapport aux finalités. Enfin, les données traitées par la police devraient être exactes et actualisées pour que leur qualité soit optimale.

1. Champ d'application

Les principes énoncés dans le présent guide s'appliquent au traitement de données à caractère personnel à des fins policières, plus précisément aux fins de prévention, d'investigation et de répression des infractions pénales et d'exécution des sanctions pénales. 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.

Comment [0013]: Attention, les missions des services de police ne sont pas uniquement limitées aux missions de répression des infractions pénales. La recommandation vise également le maintien de l'Ordre public

2. Collecte et utilisation des données

Le traitement 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 par exemple).

Comment [0014]: Voir commentaire ci-avant. Ajouter le maintien de l'ordre public

Le traitement des données à caractère personnel à des fins policières constitue une ingérence dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel et toute ingérence doit par conséquent être fondée 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.

Il importe que la collecte de données à caractère personnel par la police soit conforme au cadre législatif et toujours liée à des enquêtes en cours. 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, toute donnée à caractère personnel « utile » peut être traitée à condition que toutes les obligations légales la concernant soient respectées. 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 correspondent pas 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 : en cas d'écoutes téléphoniques, les services de répression ne devraient demander que le(s) numéro(s) nécessaire(s) à la période qui fait l'objet de l'enquête et uniquement pour la ou les personnes concernées. 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 strictement 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, sauf disposition contraire de la législation nationale.

Comment [0015]: L'objectif n'est-il pas le principe de limitation de la finalité. On pourrait éventuellement préciser qu'il s'agit de l'application de l'exception prévue à l'art. 9 de la convention 108 ?

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 doit respecter les mêmes obligations légales que celles qui s'appliquent au traitement de données à caractère personnel : il devrait être prévu par la loi, être nécessaire et proportionné au but légitime poursuivi.

Comme les données à caractère personnel collectées dans une finalité précise peuvent être très facilement utilisées pour une autre finalité, les données d'une personne recueillies à des fins policières ne devraient pas être conservées et traitées d'une façon non structurée, sauf s'il existe une base légale et une justification opérationnelle à cela. La règle générale est que toutes les données détenues par la police doivent avoir un lien direct avec l'enquête et doivent être traitées en cohérence avec cette enquête spécifique. Cependant, dans des cas exceptionnels dans lesquels un critère supplémentaire vient valider la légitimité du traitement, les données peuvent être conservées dans une forme structurée plus souple. Par exemple, les données de récidivistes ou les données relatives à des membres d'un groupe terroriste peuvent être conservées plus longtemps et dans une forme structurée plus souple au vu du type d'infraction pour lesquelles ils sont poursuivis ou condamnés. Toutefois, même dans ces cas, l'utilisation ultérieure des données à caractère personnel, en particulier de personnes vulnérables, telles que les victimes, les mineurs, les personnes handicapées, les personnes en difficulté ou bénéficiant d'une protection internationale, devrait être fondée sur des bases légales solides et faire l'objet d'un examen approfondi.

Dans des affaires difficiles concernant la traite des êtres humains, le trafic de drogue, l'exploitation sexuelle, etc., dans lesquelles les victimes peuvent souvent aussi être également des suspects et où 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.

Exemple : les données biométriques recueillies à des fins d'immigration peuvent être traitées, si la loi l'autorise, pour d'autres utilisations répressives (telles que les contrôles des personnes recherchées pour un crime ou un acte terroriste grave). À l'inverse, pour les vols mineurs (tels que le vol d'une revue), les recherches dans le fichier ADN détenu à des fins d'immigration ne seront pas considérées comme appropriées et pourraient pas ailleurs ne pas satisfaire le principe de proportionnalité.

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 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 peuvent disposer~~reçoivent~~ un certain nombre de renseignements avant le traitement des données, 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.

Comment [0016]: Il faut éviter de créer des processus administratif (donner un formulaire,…) uniquement. Un accès via internet devrait pouvoir être suffisant.

Les informations données de façon générale au public dans son ensemble devraient permettre de promouvoir leur sensibilisation, de les informer de leurs droits et des 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 peuvent jouer 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 devrait être de la responsabilité du responsable du traitement ou du sous-traitant 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, il appartient au responsable du traitement de l'informer, sur demande, 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 lui communiquer, dès que les circonstances le permettent, les informations sur les activités de traitement de ses données. La communication de ces informations à la personne concernée peut être effectuée telle qu'elle est prévue dans le droit interne. Les informations doivent être communiquées de manière claire et intelligible.

Il convient toutefois de souligner que la police n'a pas à faire cette démarche si elle estime que la communication de cette information à l'intéressé peut être préjudiciable à l'enquête, par exemple parce qu'elle lui permettra de prendre la fuite ou de détruire des éléments de preuve. 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, dans la mesure où ces données sont nécessaires à cette fin, si l'on considère que ces informations peuvent nuire à l'enquête.

5. Exceptions

Les exceptions ne peuvent être utilisées que si elles sont prévues par la loi et constituent une mesure nécessaire et proportionnée dans une société démocratique. Cela signifie que la mesure sur laquelle l'exception est fondée est publique, ouverte, transparente et suffisamment détaillée. En outre, l'exception ne peut être utilisée que pour les objectifs légitimes énumérés et uniquement lorsque cela est nécessaire et proportionné pour atteindre le but poursuivi. Enfin, les mesures utilisées doivent être soumises à un contrôle externe approprié.

Les exceptions peuvent être applicables aux principes décrits aux points 2, 3, 4, 7 ainsi qu'aux droits des personnes concernées (point 19) 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 ou la protection des droits et libertés fondamentales d'autrui.

Des exceptions à ces règles et principes peuvent également se justifier si leur exécution met en danger la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales ou d'autres objectifs essentiels d'intérêt général.

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.

Il est parfaitement légitime pour un État de protéger sa sécurité nationale et donc pour la police d'enquêter sur des personnes participant à des activités terroristes, mais cet objectif ne saurait justifier la décision de procéder à des écoutes téléphoniques permanentes, non contrôlées et illimitées du téléphone portable d'un individu (*affaire Zakharov c. Russie*[6]) ou d'utiliser des techniques d'enquête spéciales (point 6) uniquement contrôlées par le gouvernement (*affaire Szabó c. Hongrie*[7]).

Exemple : des données policières peuvent être échangées avec des services de sécurité nationale s'il existe une menace réelle et imminente pour la sécurité nationale, par exemple pour déjouer un attentat terroriste. Afin d'identifier rapidement l'auteur de l'attentat, la police doit coopérer activement avec les services de sécurité nationale et échanger les données à caractère personnel recueillies sur des suspects. Mais s'il n'y a pas de risque d'attentat terroriste, la police ne devrait pas communiquer

[6] CEDH Roman Zakharov v. Russie, 47143/06
[7] CEDH Szabó and Vissy v. Hongrie, 37138/14

ses données aux services de sécurité nationale car cela serait contraire au principe de la limitation de la finalité.

Comment [0017]: L'exemple nous semble trop restrictif car il se focalise uniquement sur des menaces concrètes et oublie les autres obligations de communication entre département tels que visées ci-après. Dans le cadre des missions respectives de chacun, un échange de données doit rester possible.

6. Utilisation de techniques d'enquête spéciales

La police devrait toujours choisir la ou les méthodes les plus efficaces et les plus simples pour une enquête. Les méthodes les moins intrusives, dans le cas où elles peuvent être employées pour aboutir au but recherché, devraient être privilégiées. L'emploi de techniques spéciales d'enquête ne peut être envisagé que si le même résultat ne peut être obtenu par des méthodes moins intrusives.

Les progrès techniques ont rendu la surveillance électronique plus facile, mais il ne faut pas oublier que leur utilisation est une ingérence dans le droit au respect de la vie privée, le droit à la protection des données à caractère personnel et d'autres droits fondamentaux. 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.

7. Utilisation 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 pour les actions envisagées. Il est recommandé que l'évaluation des risques ne soit pas statique, mais 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 contrôle 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.

À l'issue de ces consultations, le responsable du traitement devrait mettre en œuvre les mesures et les garanties nécessaires convenues avant de procéder au traitement 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

Il convient, pendant le processus de consultation, de communiquer des renseignements appropriés à l'autorité de contrôle, 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 : les fichiers nationaux de référence qui contiennent des données sur les empreintes digitales doivent être conformes à la législation nationale. Toute information détaillée sur les fichiers, tel que leur finalité ou le responsable du traitement des données, etc., devrait être indiquée ou mise à disposition de l'autorité de contrôle.

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 exemple, au moyen d'un GPS et de caméras corporelles) par internet montrent que la technologie de l'internet des objets est déjà opérationnelle. En raison des vulnérabilités qu'elle peut présenter, 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 » 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 risque d'entraîner une ingérence collatérale qui peut avoir des répercussions sur les droits fondamentaux d'une personne, tel que le droit au respect de la vie privée et le droit 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 du big data[8] 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;

[8] Document T-PD(2017)1

- la quantité croissante de données détenues dans des bases de données peut entrainer 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 limitée à des formes graves de criminalité ;
- 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 ;
- 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 ;
- l'analyse du big data et le traitement des résultats de cette analyse devraient être effectués par des personnes expertes en la matière ;
- veiller à la loyauté du traitement des données à caractère personnel lorsque la prise de décisions qui ont des conséquences pour les intéressés repose sur l'utilisation du big data.

Comment [0018]: Pas forcément un acte positif pour informer, mais la personne doit pouvoir disposer de cette communication. On pourrait modifier le texte comme suit : « ait informé »

8. Traitement portant sur des catégories particulières de données

Comment [0019]: Attention à la terminologie : particulières, spéciales, sensibles en fonction du texte. Il faudrait reprendre la terminologie de la convention 108, à savoir « catégories particulières »

Les catégories ~~spéciales~~ particulières 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 des protections supplémentaires sont prévues par la loi. 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 ».

Comment [0020]: Les données concernant les infractions et les procédures ne sont pas des catégories particulières (voir art. 6 convention 108)

Un juste équilibre des intérêts doit être trouvé pour déterminer si la police est autorisée à traiter des ~~données sensibles~~catégories particulières et dans quelle mesure. Il est en outre recommandé d'utiliser davantage l'évaluation de l'impact sur le respect de la vie privée (EIPD) afin d'être sûr que des protections supplémentaires sont mises en place de manière adéquate. Le responsable du traitement devrait démontrer après évaluation que la finalité du traitement (p.ex. l'enquête pénale) ne peut pas être atteinte en utilisant un traitement qui affecte moins le droit au respect de la vie privée et le droit à la protection des données de la personne concernée, et que le traitement de catégories ~~spéciales~~ particulières de données ne présente pas un risque de discrimination pour la personne concernée.

La collecte de données sur des personnes fondée seulement sur des données à caractère sensible qui ne serait pas prévue par la loi est interdite.

En ce qui concerne ces données (~~sensibles~~catégories particulières), le profilage devrait être évité en règle générale et ne devrait être autorisé que lorsque des garanties supplémentaires importantes sont mises en place pour contenir le risque potentiel de discrimination. 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 tels que la communication fréquente avec des membres connus du groupe, etc., pour autoriser le traitement des données pour ce motif.

Exemple : le traitement de données pour des motifs purement 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

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 est prévu par la loi *et* est considéré comme pertinent pour une fin qui n'est pas incompatible avec le but initial du traitement. 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.

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 strictement nécessaires pour atteindre l'objectif de l'enquête.

Les motifs de conservation et de traitement des données devraient être réexamines 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.

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 façon de réexaminer la période 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). De même, s'il s'avère qu'au bout de 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 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 logiquement et/ou physiquement des données collectées à des fins policières. La police peut y accéder lorsque c'est nécessaire et autorisé par la loi.

Comment [0021]: Attention aux développement IT, il y a lieu d'être « a »technologique et rester neutre. Il ne faudrait pas rentrer dans des détails de cet aspect.

Parmi les données administratives figurent, par exemple, les listes de données relatives aux titulaires de licences ou les données relatives aux ressources humaines, aux permis de port d'arme et à la perte d'un bien.

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. 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 devraient ne communiquer~~nt~~ 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 des enquêtes qu'ils mènent, ou dans le cadre de leurs missions. En général, la communication de données à caractère personnel doit être soumise au principe de nécessité et de proportionnalité et servir aux fins de l'enquête.

Comment [0022]: Attention, pas uniquement pour les enquêtes répressives, mais dans le cadre de toutes les missions des services de police (prévention, investigation et répression)

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 en général 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 principes plus stricts devraient être respectés lorsque des données sont transmises à d'autres organismes nationaux que des services de police, car la communication pourrait servir à d'autres fins que la répression.

La communication de données à d'autres organismes publics ne devrait être autorisée que dans un cadre légal. L'entraide prévue par la loi entre services de répression et organismes publics permet à ces derniers d'avoir accès à des données policières essentielles à leurs fonctions et tâches (par exemple dans leurs enquêtes ou d'autres attributions légales conformes au droit interne).

La communication à une autre autorité publique est également autorisée si elle est effectuée dans l'intérêt certain de la personne concernée, ou si elle est nécessaire pour éviter un risque grave et imminent 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 a des tiers privés

Il peut arriver que, dans des conditions strictes, la police ait besoin, au niveau national, de communiquer des données à des organismes privés. Cette communication doit être prévue par la loi, servir aux fins de l'enquête et être effectuée uniquement par l'autorité qui traite les données à cette fin. Elle doit faire l'objet de garanties supplémentaires telles que l'autorisation de l'organe de contrôle ou d'un magistrat, et ne devrait être effectuée qu'aux fins de l'enquête, 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.

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. Cette communication devrait avoir lieu au cas par cas, être chaque fois clairement prévue par la loi ou faire l'objet d'une autorisation.

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

Toute communication internationale de données devrait être limitée à d'autres services de police, être adaptée au but poursuivi et prévue 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 et la communication.

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 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 très utiles pour veiller à ce que tout transfert de données soit légalement justifié t 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.

La communication de données devrait toujours être effectuée avec un niveau de protection suffisant des données lorsqu'elle est effectuée à destination de pays qui ne sont pas parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (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 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.

Comment [0023]: Il n'y a pas lieu d'être aussi restrictif. Les accords internationaux sont plus larges

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 tiers 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 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. 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 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 criminelle.

15. Garanties concernant la communication

Il est de la plus haute importance que les principes de nécessité et de limitation de la finalité soit applicable à toute communication intérieure 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 pour l'ordre public ou la sécurité publique.

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 criminelle 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.

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 strictement 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 des

conditions particulières dont il est assorti (voir point 4). L'autorité de contrôle peut contribuer à la diffusion publique des informations nécessaires.

La police devrait fournir une réponse, même aux questions d'ordre général posées par les intéressés sur les activités de traitement de leurs données à caractère personnel, mais elle peut utiliser des formulaires pour faciliter la communication.

Exemple : si une personne concernée demande à la police des informations sur le traitement de ses données à caractères personnel, la police 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. La police peut refuser de répondre aux demandes manifestement infondées ou excessives, notamment lorsque leur caractère répétitif justifie un tel refus.

Il est possible de facturer des frais administratifs raisonnables pour la demande si la législation nationale le prévoit.

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 un accès aux fichiers. 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.

S'il s'agit d'un accès indirect, la personne concernée peut adresser sa demande à l'autorité de contrôle qui traitera la demande en son nom et procédera à des vérifications sur la disponibilité et la légalité 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).

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 avant toute autorisation d'accès à des données et de même s'il 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. 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.

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 de ne pas donner d'informations ou de ne pas accorder un droit d'accès qui pourrait compromettre une enquête (voir le point 5). La divulgation de ces données devrait donc être exclue pendant toute la durée de l'enquête.

Les restrictions imposées à la communication de données 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) et 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 fournir un extrait de son casier judiciaire. Or la fourniture d'une copie ou d'une communication écrite n'est peut-être pas dans son intérêt; 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 fausse, les services de police peuvent juger utile de conserver cette fausse 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 il dispose en cas de refus, comme le dépôt d'un recours auprès de l'autorité de contrôle 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, 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'incidence des incidents de sécurité 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 à une évaluation de l'impact sur le respect de la vie privée de la personne concernée s'agissant 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.

Un délègue à la protection des données (DPD) au sein de police peut jouer un rôle essentiel dans la réalisation de vérifications internes et l'évaluation de la légalité du traitement. Cette fonction contribue au renforcement de la protection de la sécurité des données. En outre, ce délègue 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 '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 est essentiel pour garantir un accès sécurisé et adéquat aux données.

Le responsable du traitement des données met 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

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 des fichiers. Cette approche, appelle respect de la vie privée dès la conception, favorise dès le début la protection de la vie privée et des données. Elle peut être mise en place au moyen d'un logiciel et/ou d'un matériel informatique. Elle suppose une analyse des risques, une approche fondée sur un cycle de vie complet et une vérification rigoureuse.

Il importe que les responsables du traitement veillent à ce que la protection de la vie privée et des données soit rigoureusement prise en compte aux premiers stades d'un projet, puis tout au long de son cycle de vie. C'est tout particulièrement le cas lorsqu'on conçoit un nouveau système informatique d'enregistrement de données à caractère personnel ou d'accès à celles-ci, lorsqu'on élabore une législation, une politique ou une stratégie ayant des répercussions sur la vie privée et lorsqu'on met en place un partage des informations qui utilise des données à de nouvelles fins.

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 à l'élaboration ou la conception d'un nouveau système informatique, ou à 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 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 par 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 instituée en dehors du pouvoir exécutif et 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 :

a. « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (« la personne concernée ») ;

b. « données génétiques » : toutes les données concernant les caractéristiques génétiques d'une personne qui ont été héritées ou acquises durant la phase de développement prénatal, tels qu'elles résultent d'une analyse d'un échantillon biologique de la personne concernée : analyse chromosomique, analyse d'ADN ou d'ARN ou analyse de tout autre élément permettant d'obtenir des informations équivalentes ;

c. « données biométriques » : données résultant d'un traitement technique spécifique des données concernant les caractéristiques physiques, biologiques ou physiologiques d'une personne et qui permettent son identification ou son authentification ;

d. « donnés subjectives » : données acquises par le biais de témoignages de personnes impliquées dans l'enquête ;

e. « données objectives » : données acquises provenant de documents officiels ou d'autres sources certifiées ;

f. « traitement de données » : toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données. Lorsqu'un traitement automatisé n'est pas utilisé, le traitement de données désigne une opération ou un ensemble d'opérations effectuées sur des données à caractère personnel présentes dans un ensemble structuré de ces données qui sont accessibles ou récupérables selon des critères spécifiques ;

g. « 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 ;

h. «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;

i. « 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;

j. «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. ;

k. « Internet des objets » (Internet stylisé des objets ou 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 ;

l. « surveillance discrète » : 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.

m. « 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.

CROATIA / CROATIE

To the Secretariat of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD),

Further to your e-mail bellow, in view of the forthcoming 34th plenary meeting of the Consultative Committee (Strasbourg, 19-21 June 2017), please find the following comments on the "Draft practical guide on the use of personal data in the police sector" given by the Ministry of the Interior of the Republic of Croatia:

"In the part that deals with the international transfer of data („*13. International transfer*") particularities should be considered when personal data is supplied to foreign police agencies especially to those police bodies in the countries that have not ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

Namely, practice sometimes necessitates that personal data is supplied through contact points for the delivery of such data (for example through diplomatic or other representations or through the ministry of foreign affairs). We believe that the text of the Practical guide should point out that the delivery of personal data is possible to such bodies as well against confirmation that the body which will process personal data will be just the police agency of the state that has sent the request.

Furthermore, we believe that it should be stressed in the text of the Guide draft, in the part that deals with the rights of the data subject („*17. Data subject's rights*") that the data controller should have the option, along with the possibility of asking for additional information that is necessary to verify the identity of the data subject, to ask of the data subject even before information is supplied, to state information or processing activities to which the request for access, correction or deletion of personal data refers to especially in cases in which the data controller handles larger amounts of information that refers to the data subject.

Lastly, as regards reporting a personal data violation to the supervisory body, („*18. Data security*") we believe that the duty of the data controller to immediately report in case of violation of personal data to the supervisory body must be prescribed by cogent provisions in the personal data protection legislation.

Namely, the legislation in force in Croatia on the protection of personal information does not prescribe such an obligation of the data controller although certain documents (e.g. National Strategy for Cybersecurity and the Action Plan for the Implementation of the Strategy) suggest such a course of action.

We believe therefore that the text of the Guide should take into consideration the fact that national regulations on personal data protection in various states regulate differently actions of data controllers in case of security incidents that include personal data i.e. do not prescribe the duty of the data controller to report to the supervising body for the protection of personal data as well."

T-PD(2017)06mos

DENMARK / DANEMARK

Strasbourg, 18 May 2017 T-PD (2016)02rev5

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

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

Comment [0024]: General remark: In our opinion the draft guide still needs a thorough revision before it can be considered for adoption. Our main concerns are:
-The description of the ideas on further processing for other purposes is too narrow and does not reflect the regulation in the EU data reform package.
- The wording in the draft guide is often not clear.

Directorate General of Human Rights and Rule of Law

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied for ensuring the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").

Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed implementation and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[9] 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 their practical application.

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 public safety and public security, 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.

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

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 in a fair, transparent and lawful manner and should 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, i.e. for the purposes of the prevention, ~~,~~detection, 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.

21. Collection of data and use of data

The processing 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).

The processing of personal data for law enforcement purposes constitutes an interference with the right to privacy and right to protection of personal data and as such any interference *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.

If police collect personal data it must fit into the legislative framework and should always be in connection with on-going investigations+. 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, any "useful" 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 out of purpose~~. 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 strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for law enforcement 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 national law.

Comment [0025]: The wording of this sentence is not clear.

Example: Police data collected for an investigation 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 must meet the same 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.

As it is very easy to use personal data collected for one purpose for another purpose, personal data collected and retained of an individual for police purposes should not be kept and processed in an unstructured manner unless there is a legal basis and operational reason for this. The general rule is that all data held by police have to have a direct link to an investigation and have to be processed in relation with this specific investigation. However in exceptional cases where there is an additional criterion which can validate the legitimacy of the processing the data can be stored in a less structured manner. For example recidivists' data or data related to the members of a terrorist group can be retained longer and in a less structured manner in respect of crime they are charged or convicted of. However even in these cases any subsequent use of personal data, in particular of vulnerable individuals such as victims, minors, disabled people, or enjoying international protection should be based on solid legal grounds and thorough analysis.

In difficult cases such as trafficking in human beings, drug trafficking, sexual exploitation, where victims can often also be 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.

Example - Biometric data taken for immigration purposes can be processed for other law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Conversely, for minor theft (such as theft of a magazine) searches into the DNA registry held for immigration purposes would not be seen as appropriate and would be unlikely to meet the proportionality principle.

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 and if possible, the data subjects are provided with~~,~~ ~~prior to the data processing,~~ 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 specific 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 can 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 would be the responsibility of the data controller or the processor to provide.

According to the second obligation of giving data subject specific information regarding their data, the data controller has to inform the individuals upon request 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

Comment [0026]: It is unclear what "subsequent processing" refers to – see comment to point 2. Does this also cover processing by other law enforcement data controllers?

Comment [0027]: What is meant by "unstructured manner"?

data processing. Such provision of information to the data subject may be carried out as provided for under national law. The information should be provided in clear and plain language.

It should be noted, however, that the police do not need to advise the individual of the data processing if they believe that providing this information may prejudice the investigation, for example by allowing them to abscond or destroy evidence. Withholding notification of data processing should be used only ~~sparingly and~~ where it can be clearly justified.

Comment [0028]: It is enough that 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 as to the extent that the data are necessary for this purpose, and that informing the individual would potentially prejudice an on-going or planned investigation.

24. Exceptions

Comment [0029]: The structure of this guide is not clear. We suggest that this point is moved to a later point.

Exceptions can only be used if foreseen by law and constitute a necessary and proportionate measure in a democratic society. This latter means that the measure the exception is based on should be public, open and transparent and in addition detailed enough. Furthermore, the exception can only be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. Finally the measures used have to be subject to a proper external oversight.

Comment [0030]: A reference should be made to point 19 “external control”.

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects’ rights (point 19) 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 or the protection of the rights and fundamental freedoms of others.

Exceptions to those rules and principles can also be applied if their application would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other essential objectives of general interests.

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.

While it is a perfectly legitimate aim for a state to protect its national security, and therefore for the police to investigate individuals and groups involved in activities such as terrorism, this cannot lead to the permanent, non-controlled and unlimited wiretapping of an individual’s mobile phone (*Zakharov vs. Russia case*[10]) or to the use of special investigative techniques (point 6) with only governmental oversight (*Szabó vs. Hungary case*[11]).

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 share personal data stored on identified suspects with national security agencies. However if there is no risk of terrorist attack, police should not share its data with national security agencies as the purpose limitation principle would be infringed.

Comment [0031]: This is not accurate – there can be other reasons of national security besides the fight against terrorism.

25. Use of special investigative techniques

The police should always choose the most efficient and straightforward method(s) for an investigation. 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 right to privacy and personal data and with other human rights. When deciding upon the method of investigation, those considerations have to be balanced with cost-effectiveness, use of resources and efficiency of investigations.

[10] ECHR Roman Zakharov v. Russia, 47143/06
[11] ECHR Szabó and Vissy v. Hungary, 37138/14

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.

26. Use of new data processing technologies

It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance to existing privacy and data protection standards.

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 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 supervisory 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.

Following consultation, the data controller should implement any necessary measures and safeguards that have been agreed prior to starting the processing operations.

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

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: National reference files containing fingerprint data should have a valid legal basis. Detailed information on the files, such as purpose, data controller etc. should be reported to or made available to the supervisory authority.

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

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

Example: In light of their potential security vulnerabilities smart glass used by police should not be directly connected to a national criminal record data base; they should gather information which is to be downloaded to a secure IT environment for further analysis.

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 way of processing data could potentially cause collateral interference, impacting on individual's fundamental rights, such as 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 Data[12] 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 limited to serious crime.~~
- Predictive analysis that aims at identifying individuals and singling out individuals for intrusive measures 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.
- 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 – subject to relevant exceptions – 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.
- Expertise should be ensured both in operating the big data analytics and in processing the results of the analysis.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals.

Comment [0032]: What is meant by this?

Comment [0033]: The wording limits the use of big data too much.

Comment [0034]: The concept "predictive analysis" is used in this sentence without any further clarification or definition.

Comment [0035]: This distinction should be reflected in regards to "predictive analysis"

[12] Document T-PD(2017)1

27. Processing of special categories of 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 additional safeguards are prescribed by law. 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.

A careful balance of interest is necessary to determine whether or not and to which extent the police would process sensitive data. A greater use of Privacy Impact Assessment (PIA) is recommended in order to ensure that the additional 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.

The collection of data on individuals solely on the basis of sensitive data which is not prescribed by law is prohibited.

Regarding these data, profiling should be avoided as a general rule and should only be permitted where significant additional safeguards have been put in place to tackle the potential risk of discrimination. 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 such as frequent communication with the known members of the group, etc. to allow the processing of data on this ground.

Comment [0036]: It should be reflected that only profiling that produces an adverse legal effect concerning the data subject or significantly affects him or her is to be prohibited.

Example - Processing data on purely 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.

28. Storage of data

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 foreseen by law *and* is deemed relevant for a purpose which is not incompatible with the original processing purpose. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

Comment [0037]: Further processing – even for incompatible purposes – is possible if provided for by law and respects the principle of proportionality.

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 ~~strictly~~ necessary to achieve the purpose of the investigation.

Comment [0038]: "Strictly" is required when processing sensitive personal data. This should be reflected in the text or "strictly" should be deleted.

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. 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, a national rule could prescribe that 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. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judiciary 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 where 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~~ sould entail the use of 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~~ should, where possible and not otherwise deemed necessary, be kept logically and physically separate from data collected for police purposes. Those data can be accessed by police when necessary and allowed by the law.

Comment [0039]: What is meant by this? Is it not possible to keep personal data for administrative purposes on the same server as other data?

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

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 the investigations they are pursuing. The communication of personal data in general should be subject to the principle of necessity and proportionality and has to serve the purpose of the investigation.

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.

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

Communication of data to any other public bodies is allowable if there is a legal basis to do so. Mutual assistance 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).

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

31. Communication of data by the police to private parties

There may be occasions when, under strict conditions, the police can communicate data domestically to private bodies. This communication has to be based in law and in accordance with the requirements of the general principles relating to processing of personal data.~~, has to serve the purpose of investigation and can only be done by the authority which is processing the data for the purpose of investigation~~. Such communication ~~must~~ may be subject to additional requirements, such as authorisation of the supervisory body or a magistrate, and should 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.

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 and/or authorisation for any such communication to occur.

Example - When the police ~~communicate~~ share data, intelligence, criminal tends etc. 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 communication 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 and communication, 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.

~~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 of great use 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.

Communication should always ensure an appropriate level of data protection if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

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

Example - Further onward transfer of data should only be allowed if this is necessary for the same 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 private party residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases 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. 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 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

Comment [0040]: We suggest that this point is merged with point 14.

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.

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 such cross-referencing of databases.

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 strictly 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, and if the police find that there is a right to access, the police 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. The police can refuse to respond to manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a refusal.

It is possible to charge a reasonable administrative fee for the request, if national law permits.
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 the right of access provided for is indirect, the data subject may direct their request to the supervisory authority, which 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).

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. 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.

Comment [0041]: We suggest that this point is merged with point 4 (should it not be 14 as above ?)

Comment [0042]: It is not clear what is meant with "provide for direct access"? Does this mean that a data subject should have access to the systems operated by the police?

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.
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 which might jeopardise an investigation and should therefore be excluded for its duration.

Restrictions to the communication of data should only apply to the extent necessary and interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis.

Any refusals provided to a data subject's request should be provided in writing (including by electronic means). The response should to the extent suitable in light of investigative purposes etc. 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.~~

Comment [0043]: This is reflected below.

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 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 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 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 PIA 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.~~

Comment [0044]: This is already mentioned on page 5 and 7.

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 is an essential requirement to ensure safe and appropriate access to data.

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

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

Privacy-by-Design

Privacy 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.

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 has to be established outside of the executive power and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

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

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

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

~~d. “soft data” means data acquired through testimony of person involved in the investigation;~~

~~e. “hard data “means data acquired from official documents or other certified sources;~~

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

g. “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;

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

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

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

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

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

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

Comment [0045]: As a general remark the definitions are not in line the EU General Data Protection Regulation.

Comment [0046]: It would be better to refer to commonly accepted definitions such as data based on personal assessments and data based on facts.

T-PD(2017)06mos

GERMANY (Gouvernment) /
ALLEMAGNE (Gouvernement)

Strasbourg, 18 May 2017 T-PD (2016)02rev5

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

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

Directorate General of Human Rights and Rule of Law

Comment [0047]: General remarks: In our view the draft still needs a thorough revision before it can be considered for adoption. The main concerns are the following:

1. Some basic ideas reflected in the draft are not state-of-the-art. It is already not clear which rights are to be protected: the right to privacy or the right to data protection? Where are the differences?

2. The important sphere of police work regarding threats to public security is not covered at all in this paper.

3. The ideas covering the further processing of data for other purposes are partly too narrow and do not reflect the rationale behind the EU Data reform package, namely Directive (EU) 2016/680.

4. Sometimes the examples used do not help in understanding what was said before or indicate an even stricter point of view than expressed in the text before.

Please find below detailed comments to different parts of the text.

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be ~~applied~~ taken into account 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").

Comment [0048]: In the context of a CoE recommendation the wording "to be applied" and "implementation" (see next paragraph) should be changed regarding the non-binding character of recommendations.

Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed ~~implementation~~ observance and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[13] 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 their practical application.

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 public safety and public security, 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.

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

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~~ in principle be in compliance with the original purpose. Further processing for other purposes should be allowed only when provided for in national law and when necessary and proportionate. The data processing should be carried out in a fair, transparent and lawful manner and should 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, i.e. 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.

2. Collection of data and use of data

The processing 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).

The processing of personal data for law enforcement purposes constitutes an interference with the right to privacy and right to protection of personal data and as such any interference *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.

If police collect personal data it must fit into the legislative framework and should ~~always~~ in principle be in connection with on-going investigations. 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, any "useful" 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 ~~out of purpose~~not needed to meet the purposes 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 ~~strictly~~ necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for law enforcement 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 national law.

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

Comment [0049]: This is to reflect that further processing for other purposes has to be possible also in a police environment.

Comment [0050]: A very important part of police work is not covered by this wording: the prevention of threats to public security.

Comment [0051]: What does this mean ("processing only in relation to a specific criminal offence")? The example does not seem to be helpful.

Comment [0052]: What is meant by "it": The collection? The police? How does something fit into a legislative framework? It is suggested to rephrase the sentence as follows: "The collection of personal data by the police must have a legal basis and should [...]".

Comment [0053]: This wording might lead to misunderstandings: The collection of data as one part of data processing has to meet the necessity requirements. Therefore it is - strictly speaking - not legally possible to collect everything that is "useful". The necessity requirement is to be met in every phase of the data processing. It is suggested to rephrase the sentence.

Comment [0054]: It is not clear what the qualification "strictly" is supposed to mean in this context.

Comment [0055]: It is not clear what exactly is meant here: Does the purpose of the further processing have to be **any other** "law enforcement" purpose (ex: further processing for purposes of another investigation) OR does the processing have to be in line with the "**original** purpose at the time of collection" and thus limiting the possibility of further processing within the law enforcement context? The example given indicates the first assumption.

3. Subsequent use of data

Every subsequent processing of data by police must meet the same legal requirements as for the original processing of personal data: it should be foreseen by law, and the processing should be necessary and proportionate to the legitimate aim pursued.

As it is very easy to use personal data collected for one purpose for another purpose, personal data collected and retained of an individual for police purposes should not be kept and processed in an unstructured manner unless there is a legal basis and operational reason for this. The general rule is that all data held by police have to have a direct link to an investigation and have to be processed in relation with this specific investigation. However in exceptional cases where there is an additional criterion which can validate the legitimacy of the processing the data can be stored in a less structured manner. For example recidivists' data or data related to the members of a terrorist group can be retained longer and in a less structured manner in respect of crime they are charged or convicted of. However even in these cases any subsequent use of personal data, in particular of vulnerable individuals such as victims, minors, disabled people, or enjoying international protection should be based on solid legal grounds and thorough analysis.

In difficult cases such as trafficking in human beings, drug trafficking, sexual exploitation, where victims can often also be 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.

Example - Biometric data taken for immigration purposes can be processed for other law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Conversely, for minor theft (such as theft of a magazine) searches into the DNA registry held for immigration purposes would not be seen as appropriate and would be unlikely to meet the proportionality principle.

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 and if applicable ~~and appropriate~~, the data subjects are provided with, ~~prior to the data processing,~~ 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 ~~specific~~ 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 can 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 would be the responsibility of the data controller or the processor to provide.

According to the second obligation of giving data subjects specific information regarding their data upon a request for access, the data controller has to inform the individuals ~~upon request~~ on the data processing activities that it has pursued with their data. This means that if ~~an individual has its~~ data has been 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 a request. ~~Such provision of~~

Comment [0056]: Does this ("subsequent use") refer to the same situation as in point 2 at the end?

Comment [0057]: What is that supposed to mean?

Comment [0058]: Are there indications that personal data are processed in an "unstructured manner" in CoE Member States? What does "unstructured" mean?

Comment [0059]: This reasoning contradicts the legal existence of systems allowing for building a biometrics-based repository of data for identification purposes on EU and EU MS level (processing of basic identity data of individuals and attached to that information on investigations concerning those individuals).

Comment [0060]: See comment above! The question as to whether all data processed have to be linked to an investigation (investigation-centered approach) or not is not an issue of structured/unstructured but rather an issue of how data holdings are structured.

Comment [0061]: Longer than it would be when applying the necessity and proportionality principles?

Comment [0062]: What does that mean? How are terrorism cases ("these cases"?) linked to subsequent use of relevant data of - e. g. - victims?

Comment [0063]: What does that mean? How are terrorism cases ("these cases"?) linked to subsequent use of relevant data of - e. g. - victims?

Comment [0064]: How does this paragraph fit into the subject matter "subsequent use"?

Comment [0065]: The immigration purpose is not a law enforcement purpose per se and thus is no "other law enforcement purpose".

Comment [0066]: The example does not seem practical: Are there **DNA** registries which are **held for immigration purposes** at all? Moreover, the applicable law might

Comment [0067]: The information does not necessarily have to be provided "prior" to the processing.

Comment [0068]: Which files?

~~information to the data subject may be carried out as provided for under national law~~. The information should be provided in clear and plain language.

It should be noted, however, that the police do not need to advise the individual of the data processing if they believe that providing this information may prejudice the investigation, for example by allowing them to abscond or destroy evidence. Withholding notification of data processing 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 as to the extent that the data are necessary for this purpose, and that informing the individual would potentially prejudice an on-going or planned investigation.

5. Exceptions

Exceptions can only be used if foreseen by law and if they constitute a necessary and proportionate measure in a democratic society. This latter means that the ~~measure~~ law ~~the exception is based on~~ should be public, open and transparent and in addition detailed enough. Furthermore, the exception can only be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. Finally the measures used have to be subject to a proper external oversight.

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 19) 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 or the protection of the rights and fundamental freedoms of others.

Exceptions to those rules and principles can also be applied if their application would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other essential objectives of general interests.

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.

While it is a perfectly legitimate aim for a state to protect its national security, and therefore for the police to investigate individuals and groups involved in activities such as terrorism, this cannot lead to the permanent, non-controlled and unlimited wiretapping of an individual's mobile phone (*Zakharov vs. Russia case*[14]) or to the use of special investigative techniques (point 6) with only governmental oversight (*Szabó vs. Hungary case*[15]).

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 share personal data stored on identified suspects with national security agencies. However if there is no risk of terrorist attack, police should not share its data with national security agencies as the purpose limitation principle would be infringed.

6. Use of special investigative techniques

The police should always choose the most efficient and straightforward method(s) for an investigation. 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 right to privacy and personal data and with other human rights. When deciding upon the method of

[14] ECHR Roman Zakharov v. Russia, 47143/06
[15] ECHR Szabó and Vissy v. Hungary, 37138/14

Comment [0069]: How else?

Comment [0070]: This is just one example that does not have to be highlighted here.

Comment [0071]: Two different things are mixed here: The exception from the duty to inform the data subject also applies when the processing has not been necessary. The necessity can be challenged by the data subject at a later stage.

Comment [0072]: Exceptions from which provisions/principles? This paragraph should be restructured, as its present structure is difficult to understand.

Comment [0073]: The word "measure" is confusing. It is suggested to replace the word "measure" by the word "law".

Comment [0074]: Doesn't this apply to all data processing activities?

Comment [0075]: Please clarify what is meant here (independent data protection authorities etc.)?

Comment [0076]: The references to the various points do not contribute to a good legibility of the text. It is not easy to figure out which principles are actually meant. It is therefore suggested to rephrase the sentence and to name the principles.

Comment [0077]: The wording appears to be confusing and should be changed.

Comment [0078]: Here some activities are mentioned that are not part of traditional police activities.

Comment [0079]: There is no reason to highlight these particular cases here. What concrete exceptions from which principles are illustrated by these cases?

Comment [0080]: An example for what? An exception from which principle?

Comment [0081]: This is incorrect: Besides the fight against terrorism, there can be other reasons of national security that could justify the transfer of personal data from the police to the national security agencies.

Comment [0082]: This is clearly not a data protection issue.

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. Use of new data processing technologies

It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance with~~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. Taking into account the specific case, i~~I~~t might be advisable~~is recommended t~~that the assessment of risk is not static, but 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 in~~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 supervisory authority has an important role in advising which risks are involved for data ~~protection~~ subjects 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~~subjects.

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.

Following consultation, the data controller should consider carefully to implement any necessary measures and safeguards that have been recommended by the supervisory authority ~~agreed prior to starting the processing operations.~~

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.

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: National reference files containing fingerprint data should have a valid legal basis. Detailed information on the files, such as purpose, data controller etc. should be reported to or made available to the supervisory authority.

Comment [0083]: Does that involve some kind of "agreement procedure" between the controller and the DPA?

Comment [0084]: It is suggested to move this paragraph further above for chronological reasons. The paragraph above concerns the situation **after** consultation ("Following consultation..."). Paragraphs like this one which concern the time before, i.e. the consultation process, should therefore be placed above.

Comment [0085]: That is self-evident and has no direct link to the information to be provided.

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

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

Example: In light of their potential security vulnerabilities smart glass used by police should not be directly connected to a national criminal record data base; they should gather information which is to be downloaded to a secure IT environment for further analysis.

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 way of processing data could potentially cause collateral interference, impacting on individual's fundamental rights, such as 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 Data[16] 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 limited to serious crime.
- 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.
- 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.
- Expertise should be ensured both in operating the big data analytics and in processing the results of the analysis.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals.

Comment [0086]: Can these examples (GPS, bodycams) really be considered as IoT?

Comment [0087]: This has to be defined/explained.

Comment [0088]: With what?

Comment [0089]: This is also relevant in a "non big data" context.

Comment [0090]: It is highly questionable if the use of big data functionalities should be limited in such a way. Big data functionalities can help detecting networks related to widespread crime that itself might not be considered as being "serious".

Comment [0091]: This is also relevant in a "non big data" context

[16] Document T-PD(2017)1

8. Processing of special categories of 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 additional safeguards are prescribed by law. 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.

A careful balance of interest is necessary to determine whether or not and to which extent the police would process sensitive data. A greater use of Privacy Impact Assessment (PIA) is recommended in order to ensure that the additional 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.

The collection of data on individuals solely on the basis of sensitive data which is not prescribed by law is prohibited.

Comment [0092]: It is suggested to rephrase the sentence because the message of the current wording is unclear.

Regarding these data, profiling should be avoided as a general rule and should only be permitted where significant additional safeguards have been put in place to tackle the potential risk of discrimination. 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 such as frequent communication with the known members of the group, etc. to allow the processing of data on this ground.

Comment [0093]: It is doubtful that frequent communication could justify the processing of special categories of data.

Example - ~~Processing data on purely religious beliefs would not be allowed.~~ To target all followers of a religion, purely because they were members of that religion, would be strictly prohibited. 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

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 foreseen by law *and* is deemed relevant for a purpose which is not incompatible with the original processing purpose. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.

Comment [0094]: If the law provides for it, further processing even for incompatible purposes is possible provided that the law respects the principle of proportionality.

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 ~~strictly~~ necessary to achieve the purpose of the investigation.
The grounds for retention and processing should be reviewed periodically. The unlawful processing of personal data ~~outside of the legal framework allowed for the retention~~ 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. 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. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judiciary 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 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, firearms certificates and lost property.

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 the investigations they are pursuing. The communication of personal data in general should be subject to the principle of necessity and proportionality and has to serve the purpose of the investigation.

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.

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

Communication of data to any other public bodies is allowable if there is a legal basis to do so. Mutual assistance 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).

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

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

Comment [0095]: Stricter than in which cases? Isn't there a contradiction regarding the previous sentence?

Comment [0096]: It is - in most cases - inherent to the communication of data to other public bodies that it is used for non-law-enforcement purposes! This might be in line with the applicable legal framework.

Comment [0097]: This paragraph basically repeats the first sentence of this chapter and therefore can be deleted.

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 domestically to private bodies. This communication has to be based in law, has to serve the purpose of investigation and can only be done by the authority which is processing the data for the purpose of investigation. Such communication may~~ust~~ be subject to additional requirements, such as authorisation of the supervisory body or a magistrate, and should 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.

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 and/or authorisation 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 communication 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 and communication, 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.

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 of great use 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.

Communication should always ensure an appropriate level of data protection if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

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

Example - Further onward transfer of data should only be allowed if this is necessary for the same 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 private party residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases 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. 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 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.

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 such cross-referencing of databases.

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 strictly 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 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. The police can refuse to respond to manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a refusal.

Comment [0098]: This sentence should be moved as it is placed between two sentences which deal with fees for the request of information.

It is possible to charge a reasonable administrative fee for the request, if national law permits.
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 the right of access provided for is indirect, the data subject may direct their request to the supervisory authority, which 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).

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. 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.
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 which might jeopardise an investigation and should therefore be excluded for its duration.

Restrictions to the communication of data should only apply to the extent necessary and interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis.

Any 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 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 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 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 PIA 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.

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 is an essential requirement to ensure safe and appropriate access to data.

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

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

Privacy-by-Design

Privacy 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 has to be established outside of the executive power and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

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

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

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

d. “soft data” means data acquired through testimony of person involved in the investigation;

e. “hard data “means data acquired from official documents or other certified sources;

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

g. “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;

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

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

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

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

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

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

Comment [0099]: The definitions are not in line with the EU General Data Protection Regulation (Article 4 nos. 13 and 14) and should be adjusted.

Comment [00100]: These definitions are not commonly accepted. Moreover, it is doubtful if this differentiation works. It would be better to distinguish between data based on personal assessments and data based on facts (see Directive (EU) 2016/680).

Comment [00101]: It does not appear necessary to define this term in the present Practical Guidelines.

GERMANY / ALLEMAGNE (DPA)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 18 May 2017 T-PD (2016)02rev5

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

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

Directorate General of Human Rights and Rule of Law

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied for ensuring the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").

Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed implementation and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[17] 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 their practical application.

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 public safety and public security, 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.

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

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 in a fair, transparent and lawful manner and should 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, i.e. 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.

2. Collection of data and use of data

The processing 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).

The processing of personal data for law enforcement purposes constitutes an interference with the right to privacy and right to protection of personal data and as such any interference *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.

If police collect personal data it must fit into the legislative framework and should always be in connection with on-going investigations. 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, any "useful" 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 out of purpose. 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 strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for law enforcement 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 national law.

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 must meet the same 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.

As it is very easy to use personal data collected for one purpose for another purpose, personal data collected and retained of an individual for police purposes should not be kept and processed in an unstructured manner unless there is a legal basis and operational reason for this. The general rule is that all data held by police have to have a direct link to an investigation and have to be processed in relation with this specific investigation. However in exceptional cases where there is an additional criterion which can validate the legitimacy of the processing the data can be stored in a less structured manner. For example recidivists' data or data related to the members of a terrorist group can be retained longer and in a less structured manner in respect of crime they are charged or convicted of. However even in these cases any subsequent use of personal data, in particular of vulnerable individuals such as victims, minors, disabled people, or enjoying international protection should be based on solid legal grounds and thorough analysis.

In difficult cases such as trafficking in human beings, drug trafficking, sexual exploitation, where victims can often also be 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.

Example - Biometric data taken for immigration purposes can be processed for other law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Conversely, for minor theft (such as theft of a magazine) searches into the DNA registry held for immigration purposes would not be seen as appropriate and would be unlikely to meet the proportionality principle.

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, prior to the data processing, 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 specific 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 can 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 would be the responsibility of the data controller or the processor to provide.

According to the second obligation of giving data subject specific information regarding their data, the data controller has to inform the individuals upon request 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. Such provision of information to the data subject may be carried out as provided for under national law. The information should be provided in clear and plain language.

It should be noted, however, that the police do not need to advise the individual of the data processing if they believe that providing this information may prejudice the investigation, for example by allowing them to abscond or destroy evidence. Withholding notification of data processing 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 as to the extent that the data are necessary for this purpose, and that informing the individual would potentially prejudice an on-going or planned investigation.

5. Exceptions

Exceptions can only be used if foreseen by law and constitute a necessary and proportionate measure in a democratic society. This latter means that the measure the exception is based on should be public, open and transparent and in addition detailed enough. Furthermore, the exception can only be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. Finally the measures used have to be subject to a proper external oversight.

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 19) 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 or the protection of the rights and fundamental freedoms of others.

Exceptions to those rules and principles can also be applied if their application would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other essential objectives of general interests.

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.

While it is a perfectly legitimate aim for a state to protect its national security, and therefore for the police to investigate individuals and groups involved in activities such as terrorism, this cannot lead to the permanent, non-controlled and unlimited wiretapping of an individual's mobile phone (*Zakharov vs. Russia case*[18]) or to the use of special investigative techniques (point 6) with only governmental oversight (*Szabó vs. Hungary case*[19]).

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 share personal data stored on identified suspects with national security agencies. However if there is no risk of terrorist attack, police should not share its data with national security agencies as the purpose limitation principle would be infringed.

6. Use of special investigative techniques

The police should always choose the most efficient and straightforward method(s) for an investigation. 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 right to privacy and personal data and with other human rights. When deciding upon the method of investigation, those considerations have to be balanced with cost-effectiveness, use of resources and efficiency of investigations.

[18] ECHR Roman Zakharov v. Russia, 47143/06
[19] ECHR Szabó and Vissy v. Hungary, 37138/14

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. Use of new data processing technologies

It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance to existing privacy and data protection standards.

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 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 supervisory 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.

Following consultation, the data controller should implement any necessary measures and safeguards that have been agreed prior to starting the processing operations.

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

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: National reference files containing fingerprint data should have a valid legal basis. Detailed information on the files, such as purpose, data controller etc. should be reported to or made available to the supervisory authority.

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

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

Example: In light of their potential security vulnerabilities smart glass used by police should not be directly connected to a national criminal record data base; they should gather information which is to be downloaded to a secure IT environment for further analysis.

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 way of processing data could potentially cause collateral interference, impacting on individual's fundamental rights, such as 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 Data[20] 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 limited to serious crime.
- 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.
- 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.
- Expertise should be ensured both in operating the big data analytics and in processing the results of the analysis.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals.

[20] Document T-PD(2017)1

8. Processing of special categories of 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 additional safeguards are prescribed by law. 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.

A careful balance of interest is necessary to determine whether or not and to which extent the police would process sensitive data. A greater use of Privacy Impact Assessment (PIA) is recommended in order to ensure that the additional 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.

The collection of data on individuals solely on the basis of sensitive data which is not prescribed by law is prohibited.

Regarding these data, profiling should be avoided as a general rule and should only be permitted where significant additional safeguards have been put in place to tackle the potential risk of discrimination. 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 such as frequent communication with the known members of the group, etc. to allow the processing of data on this ground.

Example - Processing data on purely 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

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 foreseen by law *and* is deemed relevant for a purpose which is not incompatible with the original processing purpose. 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 strictly necessary to achieve the purpose of the investigation.
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. 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. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judiciary 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 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, firearms certificates and lost property.

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 the investigations they are pursuing. The communication of personal data in general should be subject to the principle of necessity and proportionality and has to serve the purpose of the investigation.

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.

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

Communication of data to any other public bodies is allowable if there is a legal basis to do so. Mutual assistance 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).

Communication to any other public authority is also allowed if it is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to public order or 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 domestically to private bodies. This communication has to be based in law, has to serve the purpose of investigation and can only be done by the authority which is processing the data for the purpose of investigation. Such communication must be subject to additional requirements, such as authorisation of the supervisory body or a magistrate, and should 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.

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 and/or authorisation 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 communication 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 and communication, 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.

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 of great use 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.

Communication should always ensure an appropriate level of data protection if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

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

Example - Further onward transfer of data should only be allowed if this is necessary for the same 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 private party residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases 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. 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 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.

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 such cross-referencing of databases. Regarding the principle of proportionality, this should be ensured by limiting the admissibility of cross-referencing to a catalogue of serious crimes and should not be allowed in any criminal investigation.

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 strictly 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 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. The police can refuse to respond to manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a refusal.

It is possible to charge a reasonable administrative fee for the request, if national law permits.
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 the right of access provided for is indirect, the data subject may direct their request to the supervisory authority, which 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).

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. 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.
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 which might jeopardise an investigation and should therefore be excluded for its duration.

Restrictions to the communication of data should only apply to the extent necessary and interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis.

Any 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 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 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 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 PIA 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.

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 is an essential requirement to ensure safe and appropriate access to data.

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

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

Privacy-by-Design

Privacy 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 has to be established outside of the executive power and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

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

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

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

d. “soft data” means data acquired through testimony of person involved in the investigation;

e. “hard data “means data acquired from official documents or other certified sources;

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

g. “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;

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

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

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

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

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

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

IRELAND / IRLANDE

Ireland's Comments

General

Ireland is concerned that the guide may in practice have the effect of overtaking and replacing in certain respects Recommendation 87(15) despite the T-PD deciding in 2014 that the Recommendation itself should not be updated.

We are concerned that the practical guide concentrates on individual criminal investigations and doesn't take account of the work of the police in the prevention of criminal offences and the maintenance of public order.

It is not always clear what principle is being explained. In some cases the guide goes beyond the provisions set out in the Recommendation.

In some cases the guide appears to go beyond the proposed updated Convention 108 and the EU law enforcement Directive ((EU) 2016/680).

In our opinion, this document is not ready for adoption at the T-PD meeting.

Will this document be sent to the G-RJ for consideration before adoption?

Detailed comments are set out in track changes below.

T-PD(2017)06mos

Strasbourg, 18 May 2017 T-PD (2016)02rev5

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

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

Directorate General of Human Rights and Rule of Law

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied for ensuring the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").

Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed implementation and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[21] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide 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 their practical application.

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 public safety and public security, 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.

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

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~~ in principle be in compliance with the original purpose. Further processing for other purposes should be allowed only when provided for in national law and when necessary and proportionate. The data processing should be carried out in a fair, transparent and lawful manner and should 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, i.e. 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.

2. Collection of data and use of data

The processing 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).

The processing of personal data for law enforcement purposes ~~constitutes an interference with the right to privacy and right to protection of personal data and as such any interference~~ *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.

If police collect personal data it must fit into the legislative framework and should always be in connection with on-going investigations. 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, any "useful" 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 only process data that is relevant and not excessive in relation to the purposes for which they are processed ~~apply the data minimisation principle at all stages of the processing~~ and should not continue to process data which are no longer necessary for those purposes. ~~out of purpose~~. 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 ~~strictly~~ necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for law enforcement 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 national law.

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

Comment [00102]: It is suggested that a sentence should be added to state that the requirement to carry out processing in a fair and transparent manner does not prevent police from carrying out activities such as covert investigations or video surveillance. (See paragraph 89 of the draft Explanatory report on the modernised Convention 108). We would also like to delete the reference to 'transparent' as there is no reference to 'transparent' in article 4.1 of Directive (EU) 2016/680.

Comment [00103]: The meaning of this is not clear. The first part of the sentence recognises that personal data can be processed for the purposes of the prevention of crinimal offences.

Comment [00104]: This paragraph is too narrow as it appears to be based on the assumption that all processing of personal data by police is linked to a specific investigation and does not take into account the role of the police in the prevention of crime and the maintenance of public order and security.

Comment [00105]: This statement appears to be too simplistic and may be confusing.

Comment [00106]: This is not an appropriate example.

3. Subsequent use of data

Every subsequent processing of data by police must meet the same 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.

As it is very easy to use personal data collected for one purpose for another purpose, personal data collected and retained of an individual for police purposes should not be kept and processed in an unstructured manner unless there is a legal basis and operational reason for this. The general rule is that all data held by police have to have a direct link to an investigation and have to be processed in relation with this specific investigation. However in exceptional cases where there is an additional criterion which can validate the legitimacy of the processing the data can be stored in a less structured manner. For example recidivists' data or data related to the members of a terrorist group can be retained longer and in a less structured manner in respect of crime they are charged or convicted of. However even in these cases any subsequent use of personal data, in particular of vulnerable individuals such as victims, minors, ~~disabled people~~, or enjoying international protection should be based on solid legal grounds and thorough analysis.

In difficult cases such as trafficking ~~in~~ of human beings, drug trafficking, sexual exploitation, where victims can often also be suspects, or where the protection of victims of a more ~~severe~~ serious crime can override the interest of prosecuting less ~~severe~~ serious 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.

Example - Biometric data taken for immigration purposes can be processed for other law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Conversely, for minor theft (such as theft of a magazine) searches into the DNA registry held for immigration purposes would not be seen as appropriate and would be unlikely to meet the proportionality principle.

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, ~~prior to the data processing,~~ 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 ~~specific~~ 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 can 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 would be the responsibility of the data controller or the processor to provide.

According to the second obligation of giving data subject specific information regarding their data, the data controller has to inform the individuals upon request on the data processing activities that it has pursued with their data. This means that if an individual requests his or her personal data, the police should ~~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. Such provision of information to

Comment [00107]: It is suggested that this paragraph needs to be clarified and redrafted.

Comment [00108]: The meaning of this should be clarified.

Comment [00109]: This is too narrow. It would appear for example to undermine the possibility of keeping a DNA database.

Comment [00110]: The relevance of this paragraph to 'subsequent use of data' is not clear.

Comment [00111]: This paragraph is too detailed and goes beyond the requirements of Directive (EU) 2016/680.

Comment [00112]: It is suggested that this text should be deleted as its meaning is not clear.

the data subject may be carried out as provided for under national law. The information should be provided in clear and plain language.

It should be noted, however, that the police do not need to advise the individual of the data processing if they believe that providing this information may prejudice ~~the investigation~~ the prevention, investigation or prosecution of a criminal offence, for example by allowing them to abscond or destroy evidence. Withholding notification of data processing 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 ~~as to the extent that the data are necessary for this purpose, and that~~ if informing the individual would potentially prejudice an on-going or planned investigation.

5. Exceptions

Exceptions can only be used if foreseen by law and constitute a necessary and proportionate measure in a democratic society. This latter means that the measure the exception is based on should be public, open and transparent and in addition detailed enough. Furthermore, the exception can only be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. Finally the measures used have to be subject to a proper external oversight.

Comment [00113]: The meaning of this sentence is not clear. Is it intended to refer to the role of the independent data protection authority?

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 19) ~~in case of some specific data processing activities~~ Such exemptions may apply in ~~. In~~ particular where necessary ~~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 or the protection of the rights and fundamental freedoms of others or ~~.~~

~~Exceptions to those rules and principles can also be applied~~ if their application would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other essential objectives of general interests.

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.

While it is a perfectly legitimate aim for a state to protect its national security, and therefore for the police to investigate individuals and groups involved in activities such as terrorism, this cannot lead to the permanent, non-controlled and unlimited wiretapping of an individual's mobile phone (*Zakharov vs. Russia case*[22]) or to the use of special investigative techniques (point 6) with only governmental oversight (*Szabó vs. Hungary case*[23]).

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 share personal data stored on identified suspects with national security agencies. However if there is no risk of terrorist attack, police should not share its data with national security agencies as the purpose limitation principle would be infringed.

6. Use of special investigative techniques

The police should always choose the most efficient and straightforward method(s) for an investigation. 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 [00114]: The meaning and implications of this text is not clear. There is a danger that this is going beyond data protection.

With increasingly sophisticated technological developments, electronic surveillance has become easier, however, it must be remembered that the use of these techniques interferes with the right to ~~privacy and~~ personal data and with other human rights. When deciding upon the method of

[22] ECHR Roman Zakharov v. Russia, 47143/06
[23] ECHR Szabó and Vissy v. Hungary, 37138/14

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. Use of new data processing technologies

It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance ~~to~~ with 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 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.~~

Comment [00115]: In our opinion, this goes beyond the requirements or Article 8bis.2 of the modernised Convention 108

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 supervisory 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.

Following consultation, the data controller should implement any necessary measures and safeguards that have been agreed prior to starting the processing operations.

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

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: National reference files containing fingerprint data should have a valid legal basis. Detailed information on the files, such as purpose, data controller etc. should be reported to or made available to the supervisory authority.

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

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

Example: In light of their potential security vulnerabilities smart glass used by police should not be directly connected to a national criminal record data base; they should gather information which is to be downloaded to a secure IT environment for further analysis.

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 way of processing data could potentially cause collateral interference, impacting on individual's fundamental rights, such as 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 Data[24] 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 limited to serious crime.
- 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.
- 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.
- Expertise should be ensured both in operating the big data analytics and in processing the results of the analysis.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals.

Comment [00116]: The reason for including this indent is not clear so we would appreciate an explanation.

8. Processing of special categories of 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

Comment [00117]: This would encompass virtually all data processed by the police so it doesn't seem logical to categorise such data as 'special categories of data'.

[24] Document T-PD(2017)1

processed only if ~~additional~~ appropriate safeguards are prescribed by law. 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.

A careful balance of interest is necessary to determine whether or not and to which extent the police would process sensitive data. A greater use of Privacy Impact Assessment (PIA) is recommended in order to ensure that the ~~additional~~ 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.

The collection of data on individuals solely on the basis of sensitive data which is not prescribed by law is prohibited.

Regarding these data, profiling should be avoided as a general rule and should only be permitted where significant additional safeguards have been put in place to tackle the potential risk of discrimination. 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 ethnical origin. There should be additional criteria such as frequent communication with the known members of the group, etc. to allow the processing of data on this ground.

Example - Processing data on purely 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

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 foreseen by law *and* is deemed relevant for a purpose which is not incompatible with the original processing purpose. Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they ~~were collected.~~are processed

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 principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is ~~strictly~~ necessary to achieve the purpose of the investigation.
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. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

Comment [00118]: This is the word used in the modernised Convention 108 text.

Comment [00119]: It would be appreciated if the implications of this sentence would be explained for example in the case of biometric data?

Comment [00120]: It is suggested that 'appropriate' would be a better word.

Comment [00121]: What does this mean in practice?

Comment [00122]: This is too narrow.

Comment [00123]: This paragraph needs to be clarified.

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 ~~judiciary~~ judicial procedure terminates completely (which means all redress have been made or all deadline for redress have been passed).

Comment [00124]: The meaning of this text is not clear.

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.

Comment [00125]: This is not practical and needs to be clarified.

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 [00126]: In our opinion, this example is not realistic.

Personal data collected by police for administrative purposes must be kept 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, firearms certificates and lost property.

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 the investigations they are pursuing. The communication of personal data in general should be subject to the principle of necessity and proportionality and has to serve the purpose of the investigation.

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.

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

Communication of data to any other public bodies is allowable if there is a legal basis to do so. Mutual assistance 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).

Communication to any other public authority is also allowed if it is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to another individual or public order or 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 domestically to private bodies. This communication has to be based in law, has to serve the purpose of prevention or investigation of a criminal offence and can only be done by the authority which is processing the data~~, for the purpose of investigation~~. Such communication ~~must~~ may be subject to additional requirements, such as authorisation of the supervisory body or a magistrate, and should only be done for the purpose of the prevention or investigation of a crime, 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.

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 and/or authorisation 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 communication 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 and communication, 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.

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 of great use 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.

Communication should always ensure an appropriate level of data protection if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

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

Example - Further onward transfer of data should only be allowed if this is necessary for the same 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 private party residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases 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, in particular because of the length of the procedure. The local police should be informed afterwards unless this is ineffective or inappropriate. 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 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 unless this is ineffective or inappropriate.

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.

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 such cross-referencing of databases.

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 strictly 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 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.

Comment [00127]: This doesn't seem to accurately reflect point 4 which acknowledges that there may be situations where it is appropriate to 'neither confirm nor deny' the fact that personal data in relation to an individual is being processed.

The right of access (as the right to information) should, in principle, be free of charge. The police can refuse to respond to manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a refusal.

It is possible to charge a reasonable administrative fee for the request, if national law permits.
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 the right of access provided for is indirect, the data subject may direct their request to the supervisory authority, which 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).

Comment [00128]: The meaning of this text is not clear.

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. 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.

Comment [00129]: It should be acknowledged that for example in the case of witness statements that the requirement of accuracy relates to the making of the statement not its contents – see recital 30 of Directive (EU) 2016/680.

In some cases, it may be appropriate to add additional or corrective information to the file.
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 which might jeopardise an investigation and should therefore be excluded for its duration.

Restrictions to the communication of data should only apply to the extent necessary and interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis.

Any 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 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 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 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 PIA 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.

Comment [00130]: Is it clear that this doesn't apply to individual cases? Perhaps, the following sentence should be added: 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 is an essential requirement to ensure safe and appropriate access to data.

Comment [00131]: This appears to go further than the first sentence.

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

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

Privacy-by-Design

Privacy 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 has to be established outside of the executive power and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

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

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

Comment [00132]: The compatibility of this definition with the definition in Directive (EU) 2016/680 should be examined

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

Comment [00133]: The compatibility of this definition with the definition in Directive (EU) 2016/680 should be examined

d. “soft data” means data acquired through testimony of person involved in the investigation;

Comment [00134]: This would appear to be too narrow.

e. “hard data “means data acquired from official documents or other certified sources;

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

g. “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;

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

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

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

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

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

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

MONACO

Faisant suite à votre mail du 19 mai écoulé, j'ai l'honneur de vous informer que le projet cité en objet n'appelle aucune observation de fond de la part de Monaco, étant précisé que les recommandations qui figurent dans ce document à l'usage des services de police correspondent pour l'essentiel aux principes de protection des données personnelles qui sont déjà observés par la Direction de la Sûreté Publique monégasque au titre de ses engagements internationaux ou de son droit interne, qu'il s'agisse de l'administration, de la gestion ou de l'utilisation des données personnelles.

Au contraire, il a été relevé avec le plus grand intérêt qu'aucune disposition de la Convention n°108 ou de la Convention européenne de sauvegarde des droits de l'homme, notamment son article 8, ne s'opposait par principe à :

- la mise en œuvre, par les services de l'Etat, d'un système de reconnaissance faciale (p.7, §1);

- ce que le demandeur d'un permis de séjour ne fasse l'objet de vérification tendant à s'assurer qu'il n'a pas été impliqué dans des activités criminelles (p11, §4) ;

- au traitement de données biométriques recueillies à des fins d'immigration pour d'autres utilisations répressives, telles le contrôle des personnes recherchées (p.4§4).

T-PD(2017)06mos

PORTUGAL

Strasbourg, 18 mai 2017 T-PD (2016)02rev5

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

Projet de guide pratique sur l'utilisation de données à caractère personnel par la police

Direction générale Droits de l'Homme et État de droit

Introduction

La Recommandation (87)15 visant à réglementer l'utilisation de données à caractère personnel par la police énonce un ensemble général de principes à appliquer dans ce secteur pour garantir le respect du droit à la protection des données et de la vie privée 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 sa mise en œuvre que de sa pertinence. En 2010, le Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) a décidé de réaliser une étude[25] sur l'utilisation de données à caractère personnel par la police dans l'ensemble de l'Europe. Cette évaluation a montré que les principes de la Recommandation (87)15 constituaient un point de départ approprié pour élaborer des réglementations s'appliquant à cette question au niveau local et que l'élaboration d'un guide pratique sur l'utilisation de données à caractère personnel par la police, sur la base des principes énoncés par la recommandation, 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 problèmes les plus importants qui peuvent découler 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 leur application pratique.

Ces principes généraux et leurs conséquences pratiques visent à ce qu'un juste équilibre soit trouvé entre différents intérêts durant le travail de la police, tels que la sûreté ou la sécurité publique, 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.

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

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 loyale, transparente et licite, et qu'il soit adéquat, pertinent et non excessif par rapport aux finalités. Enfin, les données traitées par la police devraient être exactes et actualisées pour que leur qualité soit optimale.

1. Champ d'application

Les principes énoncés dans le présent guide s'appliquent au traitement de données à caractère personnel à des fins policières, plus précisément aux fins de prévention, d'investigation et de répression des infractions pénales et d'exécution des sanctions pénales. 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

Le traitement 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 par exemple).

Le traitement des données à caractère personnel à des fins policières ~~constitue~~ tout en étant une ingérence nécessaire, parce qu'elle poursuit un but légitime, celui de combattre le crime, dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel, ~~et toute ingérence~~ doit toujours ~~par conséquent~~ être fondée 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.

Il importe que la collecte de données à caractère personnel par la police soit conforme au cadre législatif et toujours liée à des enquêtes en cours. 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, toute donnée à caractère personnel « utile » peut être traitée à condition que toutes les obligations légales la concernant soient respectées. 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 correspondent pas 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 : en cas d'écoutes téléphoniques, les services de répression ne devraient demander que le(s) numéro(s) nécessaire(s) à la période qui fait l'objet de l'enquête et uniquement pour la ou les personnes concernées. 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 strictement 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, sauf disposition contraire de la législation nationale.

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 doit respecter les mêmes obligations légales que celles qui s'appliquent au traitement de données à caractère personnel : il devrait être prévu par la loi, être nécessaire et proportionné au but légitime poursuivi.

Comme les données à caractère personnel collectées dans une finalité précise peuvent être très facilement utilisées pour une autre finalité, les données d'une personne recueillies à des fins policières ne devraient pas être conservées et traitées d'une façon non structurée, sauf s'il existe une base légale et une justification opérationnelle à cela. La règle générale est que toutes les données détenues par la police doivent avoir un lien direct avec l'enquête et doivent être traitées en cohérence avec cette enquête spécifique. Cependant, dans des cas exceptionnels dans lesquels un critère supplémentaire vient valider la légitimité du traitement, les données peuvent être conservées dans une forme structurée plus souple. Par exemple, les données de récidivistes ou les données relatives à des membres d'un groupe terroriste peuvent être conservées plus longtemps et dans une forme structurée plus souple au vu du type d'infraction pour lesquelles ils sont poursuivis ou condamnés. Toutefois, même dans ces cas, l'utilisation ultérieure des données à caractère personnel, en particulier de personnes vulnérables, telles que les victimes, les mineurs, les personnes handicapées, les personnes en difficulté ou bénéficiant d'une protection internationale, devrait être fondée sur des bases légales solides et faire l'objet d'un examen approfondi.

Dans des affaires difficiles concernant la traite des êtres humains, le trafic de drogue, l'exploitation sexuelle, etc., dans lesquelles les victimes peuvent souvent aussi être également des suspects et où 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.

Exemple : les données biométriques recueillies à des fins d'immigration peuvent être traitées, si la loi l'autorise, pour d'autres utilisations répressives (telles que les contrôles des personnes recherchées pour un crime ou un acte terroriste grave). À l'inverse, et en principe, pour les vols mineurs (tels que le vol d'une revue), les recherches dans le fichier ADN détenu à des fins d'immigration ne seront pas considérées comme appropriées et pourraient pas ailleurs ne pas satisfaire le principe de proportionnalité.

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 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 avant le traitement des données, 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 des 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 ~~peuvent jouer~~ 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 devrait être de la responsabilité du~~ C'est au responsable du traitement ou ~~du~~ au sous-traitant 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, il appartient au responsable du traitement de l'informer, sur demande, 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 ~~lui communiquer,~~ dès que la loi le permet, communiquer les informations sur les activités de traitement de ses données. ~~La communication de ces informations à la personne concernée peut être effectuée telle qu'elle est prévue dans le droit interne.~~ Les informations doivent être communiquées de manière claire et intelligible.

Il convient toutefois de souligner que la police n'a pas à faire cette démarche si elle estime que la communication de cette information à l'intéressé peut être préjudiciable à l'enquête, par exemple parce qu'elle lui permettra de prendre la fuite ou de détruire des éléments de preuve. 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 : il serait par exemple le cas de la communication d'informations pendant toute la durée d'en enquête. ~~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, dans la mesure où ces données sont nécessaires à cette fin, si l'on considère que ces informations peuvent nuire à l'enquête.~~

5. Exceptions

Les exceptions ne peuvent être utilisées que si elles sont prévues par la loi et constituent une mesure nécessaire et proportionnée dans une société démocratique. Cela signifie que la mesure sur laquelle l'exception est fondée est publique, ouverte, transparente et suffisamment détaillée. En outre, l'exception ne peut être utilisée que pour les objectifs légitimes énumérés et uniquement lorsque cela est nécessaire et proportionné pour atteindre le but poursuivi. Enfin, les mesures utilisées doivent être soumises à un contrôle externe approprié.

Les exceptions peuvent être applicables aux principes décrits aux points 2, 3, 4, 7 ainsi qu'aux droits des personnes concernées (point 19) 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 ou la protection des droits et libertés fondamentales d'autrui.

Des exceptions à ces règles et principes peuvent également se justifier si leur exécution met en danger la prévention, l'investigation et la répression des infractions pénales, l'exécution de sanctions pénales ou d'autres objectifs essentiels d'intérêt général.

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~~ doit être limité.

Il est parfaitement légitime pour un État de protéger sa sécurité nationale et donc pour la police d'enquêter sur des personnes participant à des activités terroristes, mais cet objectif ne saurait justifier la décision de procéder à des écoutes téléphoniques permanentes, non contrôlées et illimitées du téléphone portable d'un individu (*affaire Zakharov c. Russie*[26]) ou d'utiliser des techniques d'enquête spéciales (point 6) uniquement contrôlées par le gouvernement (*affaire Szabó c. Hongrie* [27]).

Exemple : des données policières peuvent être échangées avec des services de sécurité nationale s'il existe une menace réelle et imminente pour la sécurité nationale, par exemple pour déjouer un attentat terroriste. Afin d'identifier rapidement l'auteur de l'attentat, la police doit coopérer activement avec les services de sécurité nationale et échanger les données à caractère personnel recueillies sur

[26] ECHR Roman Zakharov v. Russia, 47143/06

[27] ECHR Szabó and Vissy v. Hungary, 37138/14

des suspects. ~~Mais s'il n'y a pas de risque d'attentat terroriste, la police ne devrait pas communiquer ses données aux services de sécurité nationale car cela serait contraire au principe de la limitation de la finalité~~.

6. Utilisation de techniques d'enquête spéciales

La police devrait toujours choisir la ou les méthodes les plus efficaces et les plus simples pour une enquête. Les méthodes les moins intrusives, dans le cas où elles peuvent être employées pour aboutir au but recherché, devraient être privilégiées. L'emploi de techniques spéciales d'enquête ne peut être envisagé que si le même résultat ne peut être obtenu par des méthodes moins intrusives.

Les progrès techniques ont rendu la surveillance électronique plus facile, mais il ne faut pas oublier que leur utilisation est une ingérence dans le droit au respect de la vie privée, le droit à la protection des données à caractère personnel et d'autres droits fondamentaux. 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.

7. Utilisation 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 pour les actions envisagées. Il est recommandé que l'évaluation des risques ne soit pas statique, mais continue (c'est-à-dire effectuée à des intervalles raisonnables où dans toute situation ou cette évaluation se montre nécessaire), 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 contrôle 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.

À l'issue de ces consultations, le responsable du traitement devrait mettre en œuvre les mesures et les garanties nécessaires convenues avant de procéder au traitement 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

Il convient, pendant le processus de consultation, de communiquer des renseignements appropriés à l'autorité de contrôle, 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 : les fichiers nationaux de référence qui contiennent des données sur les empreintes digitales doivent être conformes à la législation nationale. Toute information détaillée sur les fichiers, tel que leur finalité ou le responsable du traitement des données, etc., devrait être indiquée ou mise à disposition de l'autorité de contrôle.

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 exemple, au moyen d'un GPS et de caméras corporelles) par internet montrent que la technologie de l'internet des objets est déjà opérationnelle. En raison des vulnérabilités qu'elle peut présenter, 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 » 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 risque d'entraîner une ingérence collatérale qui peut avoir des répercussions sur les droits fondamentaux d'une personne, tel que le droit au respect de la vie privée et le droit 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 du big data[28] 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;

[28] Document T-PD(2017)1

- la quantité croissante de données détenues dans des bases de données peut entrainer 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 limitée à des formes graves de criminalité ;
- 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 ;
- 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 ;
- l'analyse du big data et le traitement des résultats de cette analyse devraient être effectués par des personnes expertes en la matière ;
- veiller à la loyauté du traitement des données à caractère personnel lorsque la prise de décisions qui ont des conséquences pour les intéressés repose sur l'utilisation du big data.

8. Traitement portant sur des catégories particulières de données

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 des protections supplémentaires sont prévues par la loi. 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 ».

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 est en outre recommandé d'utiliser davantage l'évaluation de l'impact sur le respect de la vie privée (EIPD) afin d'être sûr que des protections supplémentaires sont mises en place de manière adéquate. Le responsable du traitement devrait démontrer après évaluation que la finalité du traitement (p.ex. l'enquête pénale) ne peut pas être atteinte en utilisant un traitement qui affecte moins le droit au respect de la vie privée et le droit 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.

La collecte de données sur des personnes fondée seulement sur des données à caractère sensible qui ne serait pas prévue par la loi est interdite.

En ce qui concerne ces données (sensibles), le profilage devrait être évité en règle générale et ne devrait être autorisé que lorsque des garanties supplémentaires importantes sont mises en place pour contenir le risque potentiel de discrimination. 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 tels que la communication fréquente avec des membres connus du groupe, etc., pour autoriser le traitement des données pour ce motif.

Exemple : le traitement de données pour des motifs purement 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

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 est prévu par la loi *et* est considéré comme pertinent pour une fin qui n'est pas incompatible avec le but initial du traitement. 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.

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 strictement nécessaires pour atteindre l'objectif de l'enquête.

Les motifs de conservation et de traitement des données devraient être réexamines 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.

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 façon de réexaminer la période 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). De même, s'il s'avère qu'au bout de 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 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 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, aux permis de port d'arme et à la perte d'un bien.

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. 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 devraient ne communiquent 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 des enquêtes qu'ils mènent. En général, la communication de données à caractère personnel doit être soumise au principe de nécessité et de proportionnalité et servir aux fins de l'enquête.

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 en général 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 principes plus stricts devraient être respectés lorsque des données sont transmises à d'autres organismes nationaux que des services de police, car la communication pourrait servir à d'autres fins que la répression.

La communication de données à d'autres organismes publics ne devrait être autorisée que dans un cadre légal. L'entraide prévue par la loi entre services de répression et organismes publics permet à ces derniers d'avoir accès à des données policières essentielles à leurs fonctions et tâches (par exemple dans leurs enquêtes ou d'autres attributions légales conformes au droit interne).

La communication à une autre autorité publique est également autorisée si elle est effectuée dans l'intérêt certain de la personne concernée, ou si elle est nécessaire pour éviter un risque grave et imminent 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 a des tiers privés

Il peut arriver que, dans des conditions strictes, la police ait besoin, au niveau national, de communiquer des données à des organismes privés. Cette communication doit être prévue par la loi, servir aux fins de l'enquête et être effectuée uniquement par l'autorité qui traite les données à cette fin. Elle doit faire l'objet de garanties supplémentaires telles que l'autorisation de l'organe de contrôle ou d'un magistrat, et ne devrait être effectuée qu'aux fins de l'enquête, 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.

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. Cette communication devrait avoir lieu au cas par cas, être chaque fois clairement prévue par la loi ou faire l'objet d'une autorisation.

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

Toute communication internationale de données devrait être limitée à d'autres services de police, être adaptée au but poursuivi et prévue 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 et la communication.

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 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 très utiles pour veiller à ce que tout transfert de données soit légalement justifié t 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.

La communication de données devrait toujours être effectuée avec un niveau de protection suffisant des données lorsqu'elle est effectuée à destination de pays qui ne sont pas parties à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (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 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 tiers 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 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. 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 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 criminelle.

15. Garanties concernant la communication

Il est de la plus haute importance que les principes de nécessité et de limitation de la finalité soit applicable à toute communication intérieure 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 pour l'ordre public ou la sécurité publique.

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 criminelle 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.

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 strictement 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 des conditions particulières dont il est assorti (voir point 4). L'autorité de contrôle peut contribuer à la diffusion publique des informations nécessaires.

La police devrait fournir une réponse, même aux questions d'ordre général posées par les intéressés sur les activités de traitement de leurs données à caractère personnel, mais elle peut utiliser des formulaires pour faciliter la communication.

Exemple : si une personne concernée demande à la police des informations sur le traitement de ses données à caractères personnel, la police 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. La police peut refuser de répondre aux demandes manifestement infondées ou excessives, notamment lorsque leur caractère répétitif justifie un tel refus.

Il est possible de facturer des frais administratifs raisonnables pour la demande si la législation nationale le prévoit.

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 un accès aux fichiers. 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.

S'il s'agit d'un accès indirect, la personne concernée peut adresser sa demande à l'autorité de contrôle qui traitera la demande en son nom et procédera à des vérifications sur la disponibilité et la légalité 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).

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 avant toute autorisation d'accès à des données et de même s'il 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. 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.

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 de ne pas donner d'informations ou de ne pas accorder un droit d'accès qui pourrait compromettre une enquête (voir le point 5). La divulgation de ces données devrait donc être exclue pendant toute la durée de l'enquête.

Les restrictions imposées à la communication de données 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) et 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 fournir un extrait de son casier judiciaire. Or la fourniture d'une copie ou d'une communication écrite n'est peut-être pas dans son intérêt; 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 fausse, les services de police peuvent juger utile de conserver cette fausse 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 il dispose en cas de refus, comme le dépôt d'un recours auprès de l'autorité de contrôle 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 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'incidence des incidents de sécurité 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 à une évaluation de l'impact sur le respect de la vie privée de la personne concernée s'agissant 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.

Un délègue à la protection des données (DPD) au sein de police peut jouer un rôle essentiel dans la réalisation de vérifications internes et l'évaluation de la légalité du traitement. Cette fonction contribue au renforcement de la protection de la sécurité des données. En outre, ce délègue 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 '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 est essentiel pour garantir un accès sécurisé et adéquat aux données.

Le responsable du traitement des données met 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

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 des fichiers. Cette approche, appelle respect de la vie privée dès la conception, favorise dès le début la protection de la vie privée et des données. Elle peut être mise en place au moyen d'un logiciel et/ou d'un matériel informatique. Elle suppose une analyse des risques, une approche fondée sur un cycle de vie complet et une vérification rigoureuse.

Il importe que les responsables du traitement veillent à ce que la protection de la vie privée et des données soit rigoureusement prise en compte aux premiers stades d'un projet, puis tout au long de son cycle de vie. C'est tout particulièrement le cas lorsqu'on conçoit un nouveau système informatique d'enregistrement de données à caractère personnel ou d'accès à celles-ci, lorsqu'on élabore une législation, une politique ou une stratégie ayant des répercussions sur la vie privée et lorsqu'on met en place un partage des informations qui utilise des données à de nouvelles fins.

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 à l'élaboration ou la conception d'un nouveau système informatique, ou à 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 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 par 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 instituée en dehors du pouvoir exécutif et 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 :

a. « données à caractère personnel » : toute information concernant une personne physique identifiée ou identifiable (« la personne concernée ») ;

b. « données génétiques » : toutes les données concernant les caractéristiques génétiques d'une personne qui ont été héritées ou acquises durant la phase de développement prénatal, tels qu'elles résultent d'une analyse d'un échantillon biologique de la personne concernée : analyse chromosomique, analyse d'ADN ou d'ARN ou analyse de tout autre élément permettant d'obtenir des informations équivalentes ;

c. « données biométriques » : données résultant d'un traitement technique spécifique des données concernant les caractéristiques physiques, biologiques ou physiologiques d'une personne et qui permettent son identification ou son authentification ;

d. « donnés subjectives » : données acquises par le biais de témoignages de personnes impliquées dans l'enquête ;

e. « données objectives » : données acquises provenant de documents officiels ou d'autres sources certifiées ;

f. « traitement de données » : toute opération ou ensemble d'opérations effectuées sur des données à caractère personnel, telles que la collecte, l'enregistrement, la conservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction des données, ou l'application d'opérations logiques et/ou arithmétiques à ces données. Lorsqu'un traitement automatisé n'est pas utilisé, le traitement de données désigne une opération ou un ensemble d'opérations effectuées sur des données à caractère personnel présentes dans un ensemble structuré de ces données qui sont accessibles ou récupérables selon des critères spécifiques ;

g. « 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 ;

h. «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;

i. « 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;

j. «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. ;

k. « Internet des objets » (Internet stylisé des objets ou 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 ;

l. « surveillance discrète » : 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.

m. « 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.

SWEDEN / SUEDE

Sweden's comments regarding the draft practical guide on the use of personal data in the police sector

Sweden still considers it to be very important that the Draft practical guide on the use of personal data in the police sector is in compliance with the newly adopted EU reform on the protection of natural persons with regard to the processing of personal data. It can be questioned if the practical guide fully harmonises with the reform, for example regarding the purpose limitation principle. In section 2 and section 9 it is stated that collected data should not be used in a way that is incompatible with the original purpose at the time of the collection. In article 4.2 in Directive (EU) 2016/680, on the other hand, it is not stated that subsequent processing for the purposes of the Directive has to be compatible with the original processing purpose. It is also stated in the practical guide that the collection of personal data should always be in connection with on-going investigations (see section 2 and section 3). However, the police must have the ability to process personal data in relation to other tasks than investigations. Data held by the police can also be linked to tasks such as the prevention or detection of criminal offences. This should be reflected in the practical guide, for example through the following addition "…in connection with on-going investigations or other tasks relating to prevention, detection or prosecution of criminal offences or execution of criminal penalties including the safeguarding against and the prevention of threats to public security". If the practical guide does not fully harmonise with Directive (EU) 2016/680, it is going to be very difficult for the police and other law enforcement bodies to follow the guide. Instead of providing clear guidance on what the principles imply at an operational level, the guide will cause uncertainty.

UNITED KINGDOM / ROYAUME-UNI

A guide such as this must provide a pragmatic overview of the broad guidelines to be followed, as set out in the Council of Europe Recommendation (87) 15 but also take account of other relevant international public law. Whilst the EU Data Protection Directive 2016/680/EU (hereafter EU DPD) is separate, if this draft guidance is to achieve its purpose, we consider that it should take account of the DPD's requirements. We have found that this draft practical guide is in part in keeping with the EU DPD but at times does not take into account those requirements, resulting in a skewed view of what is expected of police when handling data. Our starting point is that data protection in the law enforcement area must provide a balance between the need for public protection and the protection of the data subject's personal data. Some initial suggestions are outlined below. These written comments are without prejudice to any further comments that we may make.

Paragraph 2 **- Collection of data and use of data**

(paragraph 2.1)

This phrase from Recommendation (87) 15 - that the collection of personal data for "police purposes" should be "limited to that which is necessary for the purpose of prevention, investigation and prosecution of criminal offences and the execution of criminal penalties (i.e. to a specific criminal offence)' is not sufficiently broad as to capture the broader range of tasks which the police perform, particularly in the safeguarding arena. The drafting in the EU DPD better reflects that role and it would be clearer to state that the collection of personal data for law enforcement purposes is permitted for "*the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security"* (Article 1(1), DPD) which aligns with the scope and definition explanation of "police purposes" in Recommendation (87) 15.

(paragraph 2.2)

Furthermore, it is unhelpful and inaccurate to state simply that the processing of personal data "constitutes an interference with the right to privacy". There is clearly a balance to be struck here with the need to process data in order to protect the public as well – it is not just a binary interference and should not be presented as such.

(paragraph 2.3)

The explanation that "if police collect personal data it must fit into the legislative framework and should always be in connection with ongoing investigations" is misleading. We consider that it would be more helpful to explain that personal data is to be "collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes" (Article 4(1)(b), EU DPD).

(paragraph 2.6)

The guidance notes that police do not need to advise the individual of the data processing if they believe that providing this information may prejudice the investigation. We would encourage that the practical guide clearly illustrates that it may be necessary to withhold this information for other purposes such as for the avoidance of obstructing official or legal inquiries, investigations or procedures, to protect public security, to protect national security, or to protect the rights and freedoms of others. These criteria can be found in Article 13(3) of the EU DPD.

Paragraph 6.2 – Use of special investigative techniques

As with paragraph 2.2, it is unhelpful to state simply that the use of "electronic surveillance interferes with the right to privacy and personal data and with other human rights" and we suggest that it is more balanced to state that it "potentially interferes with the right to privacy".

Paragraph 8.4 – Processing of special categories of data

The explanation should make clear that on the processing of sensitive data more widely (and not just "solely") that this is permitted not just for a particular inquiry or where proscribed by law. But that it is also permitted in order to protect the vital interests of the data subject or of another natural person or indeed where such processing relates to data which are manifestly made public by the data subject. This will align the meaning with Article 10 (b) and (c) of the DPD.

Secondly, on the issue of collecting data solely on the basis of profiling, the explanation should be expanded to state that a decision based solely on profiling which has the impact of producing an "adverse legal effect concerning the data subject or significantly affects him or her" should be prohibited. This is to take account of the EU DPD (Article 11).

Paragraph 12 – Communication of data by the police to private parties

It is clear that private bodies can be viewed as carrying out a public role, on behalf of public bodies, and in order to reflect that context the EU DPD included in its definition of a competent authority can be, in addition to a public body, it also be "any other body or entity entrusted by ~~Member State~~ law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security" (Article 3 (7) (b), EU DPD).

The sentence under paragraph 12.3, which states that "such communication should only be on a case by case basis and in each case there must be a clear legal basis and/or authorisation for any such communication to occur", does not make clear the level of authorisation required. We suggest that it should refer only to legal basis which should provide the necessary procedure to be followed.

Paragraph 13 – International transfer

(paragraph 13.1)

For international transfers, the EU DPD provides for a range of routes; by virtue of an adequacy decision, appropriate safeguards as well as a section on derogations. These all provide means of transferring internationally with a broader range of possible criteria.

In addition, the EU DPD clearly allows for the transfer of data to a private entity internationally which is not consistent with the explanation in the draft guidance which states that "any communication of data internationally should be strictly limited to another police organisation."

(paragraph 13.6)

We consider that the following wording in this paragraph is unhelpful. "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".

It would be better if this could read more permissively and we suggest the following wording: *'The transfer of personal data to a non-police body is permissible when necessary to comply with a duty required of the transferring authority and it is not possible to transfer to a policing body'*.

(paragraph 13.7)

This paragraph references transfer of police data to a 'private party'. In paragraph 12, there is a reference to 'private bodies' and we should try and be consistent with that wording here.

The wording here is unclear as the reference to "the gravity of the crime" in this paragraph will lead to debate as to 'gravity'. We would also need to ensure proper measures were in place to protect the security of the information and have reassurances as to the use to be made of it. Additionally there would need to be certainty that this did not contravene local law.

We also consider that the explanation must make even clearer that it is not just occasionally when it is necessary to transfer data to private entities in order to protect the public, and that it might be helpful to draw upon the criteria in Article 39 (1) (a) to (e) of the EU DPD.

Paragraph 17 – **Data subject's rights**

(paragraph 17.6)

Regarding the "possible exemptions" from direct access, and in the event of a refusal of that right, the explanation should make more clearly the possibility to provide a "Neither Confirm Nor Deny" in response to such requests. This is consistent with Article 13 (3) of the EU DPD.

(paragraph 17.7)

Regarding indirect access, the explanation should take note of Article 55 of the EU DPD which makes clear that any action of this kind must be clearly mandated. In addition, the ability to "Neither Confirm Nor Deny" (which is provided for in the EU DPD in Article 13(3)) must still be upheld with both direct and indirect access, and so the explanation that "the DPA will then reply to the data subject" should be amended to ensure that this reply upholds this essential NCND requirement where necessary.

Glossary/definitions

In the glossary we would prefer 'covert' to 'discreet' surveillance, as that is a term more familiar to law enforcement officials

T-PD(2017)06mos

EUROPEAN COMMISSION / COMMISSION EUROPEENNE

Strasbourg, 18 May 2017 T-PD (2016)02rev5

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

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

Directorate General of Human Rights and Rule of Law

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied for ensuring the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").

Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed implementation and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[29] 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 their practical application.

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 public safety and public security, 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.

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

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 in a fair, transparent and lawful manner and should 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, i.e. 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.

2. Collection of data and use of data

The processing 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).

The processing of personal data for law enforcement purposes constitutes an interference with the right to privacy and right to protection of personal data and as such any interference *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.

If police collect personal data it must fit into the legislative framework and should always be in connection with on-going investigations. 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, any "useful" 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 out of purpose. 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 strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for law enforcement 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 national law.

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 for law enforcement purposes must meet the same 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.

As it is very easy to use personal data collected for one purpose for another purpose, personal data collected and retained of an individual for police purposes should not be kept and processed in an unstructured manner unless there is a legal basis and operational reason for this. The general rule is that all data held by police have to have a direct link to an investigation and have to be processed in relation with this specific investigation. However in exceptional cases where there is an additional criterion which can validate the legitimacy of the processing the data can be stored in a less structured manner. For example recidivists' data or data related to the members of a terrorist group can be retained longer and in a less structured manner in respect of crime they are charged or convicted of. However even in these cases any subsequent use of personal data, in particular of vulnerable individuals such as victims, minors, disabled people, or enjoying international protection should be based on solid legal grounds and thorough analysis.

In difficult cases such as trafficking in human beings, drug trafficking, sexual exploitation, where victims can often also be 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.

Example - Biometric data taken for immigration purposes can be processed for other law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Conversely, for minor theft (such as theft of a magazine) searches into the DNA registry held for immigration purposes would not be seen as appropriate and would be unlikely to meet the proportionality principle.

Comment [00135]: This is a bad example because immigration purposes are not law enforcement purposes! For example, under EU law processing of personal data for immigration purposes will be carried out under the GDPR. Further processing for law enforcement purposes will have to be foreseen by law.

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, prior to the data processing, 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 specific 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 can 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 would be the responsibility of the data controller or the processor to provide.

According to the second obligation of giving data subject specific information regarding their data, the data controller has to inform the individuals upon request 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. Such provision of information to the data subject may be carried out as provided for under national law. The information should be provided in clear and plain language.

It should be noted, however, that the police do not need to advise the individual of the data processing if they believe that providing this information may prejudice the investigation, for example by allowing them to abscond or destroy evidence. Withholding notification of data processing 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 as to the extent that the data are necessary for this purpose, and that informing the individual would potentially prejudice an on-going or planned investigation. However, after the purposes fo covert monitoring have been achieved, the data subject should be informed about the fact that he or she was subject to such a measure.

5. Exceptions

Exceptions can only be used if foreseen by law and constitute a necessary and proportionate measure in a democratic society. This latter means that the measure the exception is based on should be public, open and transparent and in addition detailed enough. Furthermore, the exception can only be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. Finally the measures used have to be subject to a proper external oversight.

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 19) 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 or the protection of the rights and fundamental freedoms of others.

Exceptions to those rules and principles can also be applied if their application would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other essential objectives of general interests.

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.

While it is a perfectly legitimate aim for a state to protect its national security, and therefore for the police to investigate individuals and groups involved in activities such as terrorism, this cannot lead to the permanent, non-controlled and unlimited wiretapping of an individual's mobile phone (*Zakharov vs. Russia case*[30]) or to the use of special investigative techniques (point 6) with only governmental oversight (*Szabó vs. Hungary case*[31]).

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 share personal data stored on identified suspects with national security agencies. However if there is no risk of terrorist attack, police should not share its data with national security agencies as the purpose limitation principle would be infringed.

6. Use of special investigative techniques

The police should always choose the most efficient and straightforward method(s) for an investigation. 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 right to privacy and personal data and with other human rights. When deciding upon the method of

[30] ECHR Roman Zakharov v. Russia, 47143/06
[31] ECHR Szabó and Vissy v. Hungary, 37138/14

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. Use of new data processing technologies

It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance to existing privacy and data protection standards.

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 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 supervisory 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.

Following consultation, the data controller should implement any necessary measures and safeguards that have been agreed prior to starting the processing operations.

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

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: National reference files containing fingerprint data should have a valid legal basis. Detailed information on the files, such as purpose, data controller etc. should be reported to or made available to the supervisory authority.

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

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

Example: In light of their potential security vulnerabilities smart glass used by police should not be directly connected to a national criminal record data base; they should gather information which is to be downloaded to a secure IT environment for further analysis.

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 way of processing data could potentially cause collateral interference, impacting on individual's fundamental rights, such as 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 Data[32] can be of use in the context of Big Data analysis for police use too.

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

- Databases originating from one domain can be used in another domain and for another purpose, which changes the context and may lead to inaccurate conclusions 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 limited to serious crime.
- 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.
- 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.
- Expertise should be ensured both in operating the big data analytics and in processing the results of the analysis.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals.

[32] Document T-PD(2017)1

8. Processing of special categories of 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 additional safeguards are prescribed by law. 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.

A careful balance of interest is necessary to determine whether or not and to which extent the police would process sensitive data. A greater use of Privacy Impact Assessment (PIA) is recommended in order to ensure that the additional 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.

The collection of data on individuals solely on the basis of sensitive data which is not prescribed by law is prohibited.

Regarding these data, profiling should be avoided as a general rule and should only be permitted where significant additional safeguards have been put in place to tackle the potential risk of discrimination. 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 such as frequent communication with the known members of the group, etc. to allow the processing of data on this ground.

Example - Processing data on purely 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

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 foreseen by law *and* is deemed relevant for a purpose which is not incompatible with the original processing purpose. 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 strictly necessary to achieve the purpose of the investigation.
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. 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. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judiciary 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 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, firearms certificates and lost property.

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.

Comment [00136]: At EU level, no such distinction should be made.

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 the investigations they are pursuing. The communication of personal data in general should be subject to the principle of necessity and proportionality and has to serve the purpose of the investigation.

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.

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

Communication of data to any other public bodies is allowable if there is a legal basis to do so. Mutual assistance 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).

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

Comment [00137]: In EU law, this is not allowed unless provided for by law.

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 domestically to private bodies. This communication has to be based in law, has to serve the purpose of investigation and can only be done by the authority which is processing the data for the purpose of investigation. Such communication must be subject to additional requirements, such as authorisation of the supervisory body or a magistrate, and should 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.

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 and/or authorisation 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 communication 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 and communication, 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.

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 of great use 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 [00138]: Are these instruments really transfer tools?

Communication should always ensure an appropriate level of data protection if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

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

Example - Further onward transfer of data should only be allowed if this is necessary for the same 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 private party residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases 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. 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 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.

Comment [00139]: Again, this is a lower level of protection than in EU law.

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 such cross-referencing of databases.

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 strictly 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 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.

Comment [00140]: In EU it has to be direct access.

The right of access (as the right to information) should, in principle, be free of charge. The police can refuse to respond to manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a refusal.

It is possible to charge a reasonable administrative fee for the request, if national law permits.
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.

Comment [00141]: In EU it is possible to charge this fee only where requests are manifestly unfounded or excessive.

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 the right of access provided for is indirect, the data subject may direct their request to the supervisory authority, which 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).

Comment [00142]: Indirect access in EU is a fall-back option, in case the controller decided to apply limitations to data subject rights.

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. 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.
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 which might jeopardise an investigation and should therefore be excluded for its duration.

Restrictions to the communication of data should only apply to the extent necessary and interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis.

Any 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 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 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 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 PIA 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.

Comment [00143]: In EU they have to carry out DPIAs in some 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.

Comment [00144]: In EU the appointment of DPO is obligatory.

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 is an essential requirement to ensure safe and appropriate access to data.

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

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

Privacy-by-Design

Privacy 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 has to be established outside of the executive power and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

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

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

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

d. “soft data” means data acquired through testimony of person involved in the investigation;

e. “hard data “means data acquired from official documents or other certified sources;

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

g. “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;

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

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

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

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

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

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

T-PD(2017)06mos

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 18 May 2017 T-PD (2016)02rev5

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

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

Directorate General of Human Rights and Rule of Law

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector provides a general set of principles to be applied for ensuring the respect for the right to private life and data protection as provided for by Article 8 of the European Convention on Human rights and by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108").

Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed implementation and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[33] 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 their practical application.

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 public safety and public security, 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.

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

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 in a fair, transparent and lawful manner and should 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, i.e. 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.

2. Collection of data and use of data

The processing 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).

The processing of personal data for law enforcement purposes constitutes an interference with the right to privacy and right to protection of personal data and as such any interference *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.

If police collect personal data it must fit into the legislative framework and should always be in connection with on-going investigations. 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, any "useful" 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 out of purpose. 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 strictly necessary for the purpose of the investigation.

According to the purpose limitation principle, personal data collected for law enforcement 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 national law.

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 must meet the same 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.

As it is very easy to use personal data collected for one purpose for another purpose, personal data collected and retained of an individual for police purposes should not be kept and processed in an unstructured manner unless there is a legal basis and operational reason for this. The general rule is that all data held by police have to have a direct link to an investigation and have to be processed in relation with this specific investigation. However in exceptional cases where there is an additional criterion which can validate the legitimacy of the processing the data can be stored in a less structured manner. For example recidivists' data or data related to the members of a terrorist group can be retained longer and in a less structured manner in respect of crime they are charged or convicted of. However even in these cases any subsequent use of personal data, in particular of vulnerable individuals such as victims, minors, disabled people, or enjoying international protection should be based on solid legal grounds and thorough analysis.

In difficult cases such as trafficking in human beings, drug trafficking, sexual exploitation, where victims can often also be 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.

Comment [00145]: Is it really the case that victims are "often" suspects? Removing the term "often" and replacing "can" with "may" might be more nuanced. Indeed, protecting victims in those contexts is essential.

Example - Biometric data taken for immigration purposes can be processed for other law enforcement use (such as checks against persons wanted for serious crime/terrorism) if the law allows. Conversely, for minor theft (such as theft of a magazine) searches into the DNA registry held for immigration purposes would not be seen as appropriate and would be unlikely to meet the proportionality principle.

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, prior to the data processing, 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 specific 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 can 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 would be the responsibility of the data controller or the processor to provide.

According to the second obligation of giving data subject specific information regarding their data, the data controller has to inform the individuals upon request 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. Such provision of information to the data subject may be carried out as provided for under national law. The information should be provided in clear and plain language.

It should be noted, however, that the police do not need to advise the individual of the data processing if they believe that providing this information may prejudice the investigation, for example by allowing them to abscond or destroy evidence. Withholding notification of data processing 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 as to the extent that the data are necessary for this purpose, and that informing the individual would potentially prejudice an on-going or planned investigation.

5. Exceptions

Exceptions can only be used if foreseen by law and constitute a necessary and proportionate measure in a democratic society. This latter means that the measure the exception is based on should be public, open and transparent and in addition detailed enough. Furthermore, the exception can only be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. Finally the measures used have to be subject to a proper external oversight.

Exceptions can be applicable to those principles described under points 2,3,4,7 as well as to the data subjects' rights (point 19) 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 or the protection of the rights and fundamental freedoms of others.

Exceptions to those rules and principles can also be applied if their application would endanger the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties or other essential objectives of general interests.

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.

While it is a perfectly legitimate aim for a state to protect its national security, and therefore for the police to investigate individuals and groups involved in activities such as terrorism, this cannot lead to the permanent, non-controlled and unlimited wiretapping of an individual's mobile phone (*Zakharov vs. Russia case*[34]) or to the use of special investigative techniques (point 6) with only governmental oversight (*Szabó vs. Hungary case*[35]).

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 share personal data stored on identified suspects with national security agencies. However if there is no risk of terrorist attack, police should not share its data with national security agencies as the purpose limitation principle would be infringed.

6. Use of special investigative techniques

The police should always choose the most efficient and straightforward method(s) for an investigation. 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 right to privacy and personal data and with other human rights. When deciding upon the method of investigation, those considerations have to be balanced with cost-effectiveness, use of resources and efficiency of investigations.

[34] ECHR Roman Zakharov v. Russia, 47143/06
[35] ECHR Szabó and Vissy v. Hungary, 37138/14

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. Use of new data processing technologies

It is advisable when new technical means for data processing are introduced, that a Regulatory Impact Analysis be carried out which should take into account the new measures' compliance to existing privacy and data protection standards.

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 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 supervisory 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.

Following consultation, the data controller should implement any necessary measures and safeguards that have been agreed prior to starting the processing operations.

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

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: National reference files containing fingerprint data should have a valid legal basis. Detailed information on the files, such as purpose, data controller etc. should be reported to or made available to the supervisory authority.

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

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

Example: In light of their potential security vulnerabilities smart glass used by police should not be directly connected to a national criminal record data base; they should gather information which is to be downloaded to a secure IT environment for further analysis.

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 way of processing data could potentially cause collateral interference, impacting on individual's fundamental rights, such as 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 Data[36] 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 limited to serious crime.
- 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.
- 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.
- Expertise should be ensured both in operating the big data analytics and in processing the results of the analysis.
- Data controllers should ensure that processing of personal data is fair where big data is being used to make decisions affecting individuals.

8. Processing of special categories of 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

[36] Document T-PD(2017)1

processed if additional safeguards are prescribed by law. 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.

A careful balance of interest is necessary to determine whether or not and to which extent the police would process sensitive data. A greater use of Privacy Impact Assessment (PIA) is recommended in order to ensure that the additional 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.

The collection of data on individuals solely on the basis of sensitive data which is not prescribed by law is prohibited.

Regarding these data, profiling should be avoided as a general rule and should only be permitted where significant additional safeguards have been put in place to tackle the potential risk of discrimination. 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 such as frequent communication with the known members of the group, etc. to allow the processing of data on this ground.

Example - Processing data on purely 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

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 foreseen by law *and* is deemed relevant for a purpose which is not incompatible with the original processing purpose. 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 strictly necessary to achieve the purpose of the investigation.
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. 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. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

In the latter case it is important to design the data retention policy so that the data used in criminal cases remains within the oversight of the data controller until the judiciary 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 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, firearms certificates and lost property.

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 the investigations they are pursuing. The communication of personal data in general should be subject to the principle of necessity and proportionality and has to serve the purpose of the investigation.

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.

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

Communication of data to any other public bodies is allowable if there is a legal basis to do so. Mutual assistance 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).

Communication to any other public authority is also allowed if it is undoubtedly in the interest of the data subject, or the communication is required to prevent serious and imminent risk to public order or 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 domestically to private bodies. This communication has to be based in law, has to serve the purpose of investigation or other compatible purposes and can only be done by the authority which is processing the data for the purpose of investigation. Such communication must be subject to additional requirements, such as authorisation of the supervisory body or a magistrate, and should only be done for the purpose of the investigation, or 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, t~~T~~here might also be instances where data may be communicated by the police to humanitarian organisations in the interest of the data subject or for reasons of public interest, such as humanitarian reasons.

Comment [00146]: Not necessarily. The sentence below refers to various reasons for such communication, besides the purpose of investigation. Therefore we have added “other compatible purposes” to refer to those other reasons for communication.

Comment [00147]: This is already the case for the ICRC which, in a number of countries, receives information from the national authorities on persons detained so that the ICRC can visit them and assess their conditions of detention.

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 and/or authorisation 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 communication 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 and communication, 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.

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 of great use 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.

Communication should always ensure an appropriate level of data protection if data are to be transferred to countries not participating in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

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

Example - Further onward transfer of data should only be allowed if this is necessary for the same 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 private party residing in a different jurisdiction should be avoided as a general rule. It can only be done in very exceptional cases 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. 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 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.

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 such cross-referencing of databases.

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 strictly 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 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. The police can refuse to respond to manifestly unfounded or excessive requests, in particular where their repetitive character justifies such a refusal.

It is possible to charge a reasonable administrative fee for the request, if national law permits.
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 the right of access provided for is indirect, the data subject may direct their request to the supervisory authority, which 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).

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. 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.
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 which might jeopardise an investigation and should therefore be excluded for its duration.

Besides, restrictions concerning specific principles and data subjects' rights, including the rights of information, access to and rectification or erasure of personal data as well as the communication of a personal data breach to a data subject and certain related obligations of the controllers may be imposed by national law for important objectives of general public interest including humanitarian purposes.

Comment [00148]: This is in line with recital 73 of the GDPR.

Restrictions to the communication of data should only apply to the extent necessary and interpreted narrowly. Every data subject's request should be assessed carefully on a case-by-case basis.

Any 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 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 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 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 PIA 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.

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 is an essential requirement to ensure safe and appropriate access to data.

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

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

Privacy-by-Design

Privacy 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 has to be established outside of the executive power and has to have all necessary powers to perform its task. The supervisory authority set up within a ministry or the police itself does not fulfil this obligation.

Glossary/Definitions

For the purposes of this Guide:

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

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

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

d. “soft data” means data acquired through testimony of person involved in the investigation;

e. “hard data “means data acquired from official documents or other certified sources;

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

g. “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;

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

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

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

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

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

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