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[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).

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*[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.

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

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

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.

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[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.

[4] 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.

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.