COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 15 February 2018 T-PD(2018)01

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

Practical guide on the use of personal data in the police sector[1]

Directorate General of Human Rights and Rule of Law

[1] This Guide was based on the draft guidelines prepared by David Allen (UK police expert), Evelien van Beek (NL data protection expert) and John Borking (NL technical/data protection expert)

Introduction

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

Recommendation (87)15 has undergone several evaluations (in 1993, 1998 and 2002) which assessed application and relevance. In 2010, the Consultative Committee of Convention 108 decided to carry out a survey[2] on the use of personal data across Europe by the police. This evaluation highlighted that the principles of Recommendation (87)15 continued to provide a sound basis for the elaboration of regulations on this issue at a domestic level and that the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 would provide guidance on what the principles imply at an operational level.

The present Guide was therefore prepared to highlight the most important issues that may arise in the use of personal data in the police sector and to point out the key elements to be considered in that context.

This Guide does not repeat the provisions of Convention 108 nor those of Recommendation (87)15 but concentrates on practical guidance.

The overarching principles set out in Recommendation (87)15 and their practical implications aim to ensure that in the police use of personal data a balance is struck between the essential objectives of general public interest, and the respect for the rights of individuals to privacy and data protection.

It should be stressed that the Guide intends to give orientations for practical situation the police may face in its everyday operation and acknowledges that the lawful collection and use of personal data for law enforcement purposes are crucial in the interests of national security and for the prevention of crime or maintenance of public order. It emphasises with concrete examples that the prevention and suppression of crime, including through the collection and use of personal data for law enforcement purposes, can be efficiently conducted in compliance with the law.

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

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

General considerations

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

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

1. Scope

The principles explained in the present guide apply to the processing of personal data for the following police purposes: prevention, investigation and prosecution of criminal offences and the execution of criminal penalties. This includes the maintenance of public order by the police (hereafter referred to as "police purposes"). Where 'police' is used in the text, it can be taken to mean wider law enforcement authorities, notably public prosecutor services 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 police as data controller is responsible for all data processing it undertakes and is accountable for its data processing operations.

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

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

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

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

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

Prior to and during the collection of data, the question of whether the personal data collected is necessary for the investigation or for a task of the police as described in Point 1 should always be considered. One should note that once personal data are collected, a clear link between the person whose personal data are processed and the purpose of the processing (i.e. investigation or specific

task of the police) should exist. This link together with compliance to the data protection principles as described in this Guide must be demonstrable at all times. After the collection phase and at different stages of the investigation, a thorough analysis is needed to assess which data are to be retained and which are to be deleted.

According to the accountability principle the police, as other data controllers, is responsible for the data processing it undertakes. It implies that it has to be able to demonstrate at all time that its processing activities are in compliance with data protection rules. It furthermore requires that the police actively implements measures to safeguard and promote data protection in all its activities.

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

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

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

It is highly recommended to make a clear distinction in how the police processes personal data that relate to different categories of persons, e.g. suspects, persons convicted of a criminal offence, victims and third parties such as witnesses. This should also relate to the specific purpose for which the data was collected.

According to the purpose limitation principle, personal data collected for police purposes should be used for those purposes only and should not be used for any other purpose that is incompatible with the original purpose stated at the time of collection. They should furthermore be necessary and proportionate for police purposes, unless this is provided for in law.

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

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

3. Subsequent use of data

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

Notwithstanding the computerised and/or automated data processing and the large volume of personal data stored very often in different processing environments, the personal data collected and retained for police purposes should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

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

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

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

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

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

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

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

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

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

5. Providing information to data subjects

One of the most important obligations of a data controller is to provide information on data processing to data subjects. This obligation is two-fold: it requires the data controller to provide *general information* to the public on the data processing that it carries out, and to give *specific* information to data subjects if no restrictions or derogations as described in Point 7 apply to the data processing.

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

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

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

In order to comply with the second obligation of giving data subjects specific information regarding data processed, the police shall inform data subjects on the data processing envisaged before the processing or, if it is not possible for objective reasons, after it. This communication shall comprise information on the data processing, on the collection of the individuals' data and comprehensive information on their rights. The obligation to provide specific information implies that, in principle, the data subjects shall be provided with details such as the name, contact details of the data controller, data processor, recipients of the data, the set of data to be processed, the purpose of the data processing, the legal basis for it and information about their rights.

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

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

Example: For the purpose of investigation of a high risk sex offender, data processing and long-term data retention may be justified without informing the individuals under surveillance if this would potentially prejudice an on-going or planned investigation. However, once the purpose for covert monitoring has been achieved and no other restriction or derogation is applicable, the data subject should be informed about the fact that she or he was subject to such a measure.

6. Data subject's rights

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

In case an individual has her/his data collected during the course of an investigation or other tasks of the police as described in Point 1, as soon as circumstances safely permit, the police in principle should grant access to the data subject if there is such request. The communication has to contain the same information as described in point 5, unless data subjects wish otherwise.

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

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

Example: If a data subject asks the police on data it processes on them, the police, if no exception is applicable and after verification of the identity of the data subject, should provide a detailed answer with legal references containing the list of police files where the data of the data subject are processed, but should do so in a plain language, avoiding uncommon or specialised expressions.

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

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

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

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

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

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

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

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

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

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

In some cases, it may be appropriate to add additional or corrective information to the file. It is important to underline that this right can only be exercised with due respect to other individuals' rights.

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

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

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

Restrictions or derogations to the rights of data subjects should only apply to the extent necessary and be interpreted narrowly[4]. Every data subject's request should be assessed carefully on a case-by-case basis. Any decision to refuse a data subject's request should be provided in writing (including by electronic means). The response should provide clear justification of the decision making which can be verified by an independent authority or a court. It is possible that communicating the reasons for refusal could pose a risk to law enforcement or the data subject or to the rights and freedoms of others. If this is the case, it should be documented and provided to the independent authority or court to be verified, if required.

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

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

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

7. Exceptions from the application of data protection principles

Exceptions can only be used for specific purposes foreseen by article 8 of the European Convention on Human Rights and by Convention 108, if foreseen by law (the law should be public, open and transparent and, in addition, detailed enough) and if they constitute a necessary and proportionate measure in a democratic society for the purpose of the protection of national security, defence, public safety, important economic and financial interests, impartiality and independence of the judiciary, the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest (which includes purposes in connection with the fulfilment of a state's international legal commitments or obligations, most prominently deriving from the binding decisions of United Nations' bodies, and humanitarian purposes.) or the protection of the rights and fundamental freedoms of others.

The exceptions which have to be incorporated into national legislation should not be described in a general way, but should serve a well-defined purpose. Exceptions can be applicable to those principles described under Points 2, 3, 4, 5 as well as to the data subjects' rights (Point 6).

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

If the exception, as defined by national law providing specific safeguards is used by the police, it should be used for legitimate aims and only to the extent necessary and proportionate to achieve the aim for which it is being used. The aim of using exceptions by the police should be limited to cases where not using those exceptions would endanger tasks of the police described under Point 1 or would endanger actions performed for the purposes falling in the list of exceptions as described above.

Example: If specific intelligence proves that money laundering operations have been carried out to finance terrorist operations, data collected on individuals can be kept, if approved by the body ensuring the external oversight, for a longer period than it would otherwise be strictly necessary for the police investigations.

[4] ECtHR case: paragraph 42 of *Klass and Others v. Germany* (Application no. 5029/71).

8. Use of special investigation techniques

Concerning the use of special investigation techniques the police is invited to refer to Recommendation (2017)6 of the Committee of Ministers to member States on "special investigation techniques" in relation to serious crimes including acts of terrorism. Paragraphs 7-10 of the Recommendation in particular can give useful guidance on the lawful application of these investigation techniques.

This area is regulated in detail generally in national criminal procedural law, however when deciding on their use, some data protection considerations could be assessed in order to allow to the police to use the least intrusive means of data processing during its operations. If less intrusive methods can be used to achieve the desired ends, they should be preferred. The use of special investigation techniques can be considered as proportionate if the same result cannot be achieved by less intrusive methods. Regardless of the method of investigation or other operation led by the police, the police is obliged to comply with the general principles of data protection as described in General considerations, unless a law expressly exempts from it.

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

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

9. Introduction of new data processing technologies

If data 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. Considering that the introduction of new data processing technologies bears *per se* such potential risk, it is likely that the introduction of such new technology will make a DPIA advisable. It is recommended that the assessment of risk is not static, but takes into account the specific case, it is repeated at reasonable intervals, and that it touches upon relevant phases of the data processing activity and that it takes into account accountability considerations.

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

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

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

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

Appropriate details should be provided to the supervisory authority, in particular regarding the type of file, the data controller, the data processor, the legal basis and the purpose of the data processing, the

type of data being processed and by whom the data is being accessed, as well as information on retention of data, log policy and access policy, and other relevant technical aspects of implementation.

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

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

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

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

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

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

Big data analytics in the police

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

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

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

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

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

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

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

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

To observe the above mentioned considerations, especially those related to human intervention and the combination of new analytical methods with traditional ones are highly recommended when sensitive data are processed in Big Data analytics.

10. Storage of data

Personal data shall be processed until they have served the purpose for which they were collected as pointed out in "Point 2". Stored data should be adequate, up to date, necessary, relevant and not excessive in relation to the purposes for which they were collected.
Clear rules have to be established in relation to the handling of different data bases with special attention to the analysis of searches resulting in multiple results.

The principle of necessity must be applied throughout the lifecycle of the processing. Storage can be permissible if analysis shows that the personal data is strictly necessary to achieve the police purposes as described in Point 1.

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

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

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 and if all deadline for redress have passed) from the database, provided that all deadlines for the review of the case have expired. Likewise, if, after 4 years, the investigation is still on-going and their data is still relevant to it, the police should be able to retain it.

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

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

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

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

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

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

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

11. Communication of data within the police sector

A distinction should be made between domestic communication of data within the police sector (Point 11) or to other public bodies (Point 12) and international transfers (Point 14.) of data. Within these distinct operations different requirements apply, depending upon who is receiving the data, whether it is the police, another public body or a private body.

The police can only communicate personal data within the police sector if a legitimate interest exists for such communication within the framework of the legal powers of these bodies (e.g. an on-going criminal investigation or a shared law enforcement task and laws or agreements allowing the communication).

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

The communication of personal data from one police body to another should be in line with the General Considerations described above.

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

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

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

Specific rules should be followed when data are to be transmitted domestically outside of the police sector, as there is a risk that the processing of personal data, which are considered as sensitive data, could result in adverse effects for the individual.

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

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

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

13. Communication of data by the police to private bodies

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

Where the police is entitled to 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 that such publicity is allowed in the public interest. Appropriate safeguards have to be put in place to ensure the respect for the rights of the individuals involved in the case.

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

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

14. International transfer

As a general rule any transfer of police data internationally should be limited to police bodies and should be fit for purpose and in accordance with the law. This implies also to follow internal procedures set up by national criminal procedural law which may include the active participation of wider law enforcement bodies and services, such as the Ministry of interior, Ministry of justice, public prosecutor services, investigative judges, etc. For this, multilateral international legal instruments, such as Convention 108 and the Interpol Constitution and its supporting documentation in respect of data handling, regional legal frameworks such as EU and EU institutions' legislation (on Europol, Eurojust, Frontex, etc.) and subsequent agreements (operational bilateral agreements), bilateral treaties and in general, international agreements on mutual assistance, or other bilateral or multilateral agreements made regarding effective cooperation can be of use.

When sharing data, consideration should be given as to whether the receiving authority is performing a function conferred to it in law related to police purposes, and whether the sharing of the data is necessary to perform its specific task.

The sending authority should ascertain that there is an appropriate level of data protection in the receiving state and that the receiving state complies with the relevant rules of international transfers of personal data. This includes providing for appropriate safeguards regarding data protection in cases where no relevant national legal provisions or international agreements are in place. This means of transfer should be used as a last resort option. International transfers framework such as "INTERPOL's Rule on the Processing of Data" and its "Statute of the Commission for the Control of INTERPOL's files" Rules on the Control of Information and access to INTERPOL's Files", the

provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185) may be taken into account[7] so as to ensure that any transfer of data is legally justified and has appropriate safeguards in place. The request should clearly state all the necessary elements from the requesting party to enable the receiving party to make a sound decision on the request. These details would be expected to include the reason for the request as well as the purpose for the transfer of data.

It is required to ensure that proper measures are in place to protect the security of the information.

An appropriate level of data protection should be guaranteed (e.g. through ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments) if data are to be transferred to countries or organisations not participating in Convention 108.

If there are conditions applied by the sending authority in relation to the use of the data in the receiving state these should be adhered to. The sending and the receiving states should be in agreement on the use of the data throughout all processing operations and the sending authority should obtain reassurances from the recipient that agreed conditions are respected.

Example: Further transfer of data should only be allowed if it is required for the fulfilment of police tasks described in Point 1, the second recipient is also a police body ensuring an appropriate level of data protection. The police, including public prosecutor services and/or investigative judges which originally sent the data must also consent to the onward transfer. If the police from country X sends personal data to the police of country Y it is only permissible for the country Y to transfer this data if above all requirements foreseen by law (there is a valid legal basis and the transfer fits the original purpose) if country X consents to the transfer. If the data is sent to country Z which is a non-party of the Convention 108, then country Y should ascertain that this country provides an appropriate level of protection of personal data including the existence of effective means of exercise of the related data subject rights.

The international transfer of personal data to a non-police public body is only permissible exceptionally and in individual cases if it is required for the performance of the task of the transferring authority and there is no effective means of transferring the data to a competent police body. The data protection principles laid down in Convention 108 must be followed for all types of transfers especially those related to the requirement of an appropriate level of protection which takes into account the sensitive nature of police data.

Example: If tax authorities in country X requests the police in country Y about the whereabouts of a person involved in non-criminal tax evasion because they have evidence that the person is involved in criminal matters in country X, the police, if the national law permits (for instance on the basis of a bilateral tax evasion agreement between the two country) can transfer the personal data of the individual.

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

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

15. Conditions for communications

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

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

16. Safeguards for communication

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

Any data shared should not be used for anything other than the purpose for which it was sent or received. The exceptions to this are when the sending authority, based on legal provisions, gives agreement to further use, and it is necessary and vital for the recipient to fulfil their task.

Data can also be communicated if it is in the interest of the data subject, for humanitarian reasons, is necessary to prevent serious and imminent risk to public order or public security.

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

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

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

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

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

Clear legislation and guidance, which adheres to the data protection principles, should exist for cross-referencing of databases. Such cross referencing should be necessary, purpose bound and proportionate.

Example: Data held for citizenship purposes can only be used in an investigation if the national legislation allows it and to the extent to which it is necessary for the purpose of the investigation to do so. For instance, the number of children a suspect has may not be relevant in an investigation, and should therefore not be processed by police.

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. When considering data security the police should also take into account factors such as data localisation, adequate certification of service providers and insurance of the availability of data. It is also advisable to pay attention to data security considerations when distributing access rights. The controller should notify, without delay, at least, the competent supervisory authority of those data breaches which according to its assessment may seriously interfere with the rights and fundamental freedoms of data subjects. The information of data subjects of data breaches which may seriously interfere with their rights may also have to be ensured without undue delay, unless it jeopardises the task of the police.

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

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

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

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

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

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

The data controller, following an evaluation of the risks, should implement appropriate measures in respect of different elements such as:

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

Privacy-by-Design

The concept of privacy-by-design is an integral part of data security. Data protection and security may be embedded directly into information systems and processes, using technical and organisational measures, to ensure a high level of data protection and security and, in particular, to minimise the likelihood of data breaches. This approach is known as Privacy–by–Design, promoting privacy and

data protection compliance from the start. It can be achieved through software and/or hardware. It requires a threat analysis, a full life cycle approach and rigorous testing.

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

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

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

19. External control

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

Certain states may require more than one supervisory authority whilst others will prefer to have a single supervisory authority, responsible for the entirety of the supervision of data processing operations.

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

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

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

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

Glossary/Definitions

For the purposes of this Guide:

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

b. “sensitive data”: genetic data, personal data relating 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;

c. “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;

d. “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;

e. “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;

f. “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;

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

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

i. 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.

j. “special investigation techniques” means techniques applied by the competent authorities in the context of criminal investigations for the purpose of preventing, detecting, investigating, prosecuting and suppressing serious crimes, aiming at gathering information in such a way as not to alert the target persons

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