COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 28 June / juin 2016 T-PD(2016)08MosADD

THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA (T-PD)

Compilation of comments received
Draft practical guide on the use of personal data in the police sector /

*****

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL (T-PD)

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

Directorate General / Direction Générale
Human Rights and Rule of Law / Droits de l'Homme et Etat de droit

TABLE / INDEX

GERMANY / ALLEMAGNE

Introduction

Recommendation (87)15 regulating the use of personal data in the police sector succeeded in affirming clearly that data controllers in the police sector should process data according to legitimate, specified and explicit purposes announced at the time of collection, and only use these data for purposes compatible with the original purposes of the collection.

Recommendation (87)15 has undergone since its adoption several evaluations (in 1993, 1998 and 2002) assessing its implementation as well as its relevance. In 2010, the Consultative Committee (T-PD) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data decided to carry out a survey[1] on the use of personal data across Europe by the police. The latest evaluation highlighted that the principles of Recommendation (87)15 are still relevant and continue to provide a sound and up to date basis for the elaboration of regulations on this issue at domestic level.

During its 31st Plenary meeting in 2014, the Consultative Committee confirmed that Recommendation (87)5 would not be revised and instructed its Bureau to analyse the needs in this area and the foreseeable standard-setting solutions, taking account of the work in progress in the Cybercrime Convention Committee (T-CY) and the Committee of Experts on Terrorism (CODEXTER).

Following the mandate given by the Consultative Committee, the Bureau discussed the needs and possible options regarding the work on the use of personal data in the police sector and decided to propose the preparation of a practical guide on the use of personal data by the police, based on the principles of Recommendation (87)15 and providing clear and concrete guidance on what such principles imply at operational level.

A group of experts was commissioned to prepare the draft practical guide. It was presented at the 38th Bureau meeting (22-24 March 2016) and subsequently revised. It is submitted to the delegations and observers of the Consultative Committee, as well as to other interested stakeholders, in view of its adoption at the 33rd Plenary meeting of the Consultative Committee (29 June to 1 July 2016).

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

Principle 1 – Control and notification

1.1. Each member state should have an independent supervisory authority outside the police sector which should be responsible for ensuring respect for the data protection principles.

It is important to note that processing of personal data should only be done when subject to law establishing these processes and requirements.

Each member state must have an independent supervisory authority whose role it is to supervise the processing of personal data in the police sector. Certain member states may require more than one supervisory authority for instance a national or federal authority and a number of decentralised or regional authorities.

The supervisory authority or Data Protection Authority (DPA) must be able to act ~~totally~~ independently from any other public or private authority. In order to be effective the DPA should have sufficient resources – budget and staff – to perform its tasks in true independence. Case-law of the European Court of Human Rights and of the Court of Justice of the European Union demonstrates the importance of this issue.

Comment [PG1]: We would like to clarify that "total" independence does not imply that it is impossible to lodge an appeal against decisions made by the DPA. Furthermore, it is not necessary to add the word "totally".

The DPA should have sufficient powers to enable it to effectively supervise in an independent way. National law should provide for both investigative and enforcement powers to enable it to investigate complaints and to stop unlawful processing of personal data or impose sanctions where needed. ~~It is recommended to provide the DPA with powers to sanction unlawful data processing.~~

Comment [PG2]: This sentence provides the same information as the previous sentence. It should therefore be deleted. The fact that the DPA is allowed to impose sanctions on authorities is a rather sensitive issue and should therefore not be unnecessarily emphasized in this part of the text.

1.2. New technical means for data processing may only be introduced if all reasonable measures have been taken to ensure that their use complies with the spirit of existing data protection legislation.

Where new technical means – computerised or otherwise – are available to the police sector for use in the processing of personal data, the data controller should assess its compliance with data protection law. 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 protection of personal data.

Example:
New datamining techniques may offer extended possibilities for selection of possible suspects and should be assessed carefully for their compliance with existing data protection law.

1.3. The responsible body should consult the supervisory authority in advance in any case where the introduction of automatic processing methods raises profound data protection questions.

Comment [PG3]: The word "profound" makes it clear that it is not necessary to hold consultations prior to any processing operation - even though the following paragraph seems to imply this.

The DPA has an important role in advising which risks are involved for data protection and which safeguards should be provided to ensure any technical means comply with data protection law. Prior to processing in a new system, in particular where new technologies are involved, the data controller should consult the DPA whenever the risk assessment or DPIA demonstrates a high risk to the individual's rights.

The methodology of the consultation between the DPA and the data controller should be defined in a way that provides the DPA 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 the necessary measures and safeguards 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 imminent risks to individual's rights. Where needed specific safeguards should be added to guarantee compliance, fair processing and information security.

1.4. Information about ~~P~~ppermanent automated files should be made available ~~notified~~ to the supervisory authority. The ~~notification~~ information provided should specify the nature of each file declared, the body responsible for its processing, its purposes, the type of data contained in the file and the persons to whom the data are communicated.

AA~~d~~d hoc files which have been set up at the time of particular inquiries should also be subject to the aforementioned information made available ~~notified~~ to the supervisory authority either in accordance with conditions settled with the latter, taking account of the specific nature of these files, or in accordance with national legislation.

Permanent files can be created for different categories of data processing according to police needs and requirements. Information about ~~T~~these files should be ~~notified~~made available to the DPA if there is not already specific legislation in place regarding the type of file concerned. Each notification should provide detail about the type of file, the data controller, the purpose of the data, the type of data contained and who the data is being sent to as well as information on retention of data, log policy and access policy.

Example:
National reference files containing fingerprinting data should be based on national law. All detailed information on the files, like purpose, data controller etc. should be made available ~~reported~~ to the DPA.

Ad hoc or temporary files created for a particular event or a specific investigation should be established in a way that complies with data protection law. The existence of these files should be notified in accordance with national law, or either to the DPA or an internal Data Protection Officer (DPO) if there is one who will be responsible for monitoring compliance with national law. In case of ad hoc files, notification should include reference to data processing body, the purpose of the file, the categories of data that may be processed including whether this is sensitive data and/or there are time-limits for storage of the data or conditions for whom the data can be sent to.

National legislation may provide that no notification is needed at all or that only the type of file needs notification, without the need to notify every single investigation or operation whenever it is commenced.

Example:
An investigation of a specific crime or criminal group. Details on purpose, data controller,

Comment [PG4]: The proposed amendments are intended to move the initially requested "notification" closer towards a record of processing operations as provided for in Directive 2016/680. However, this record will only be made available to the DPA. No information is actively provided about each file.

categories of data processed etcetera could be notified to the DPO of the law enforcement agency, so as to keep the relevant data documented.

Principle 2 - Collection of data

2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

The processing of personal data for law enforcement purposes constitutes an interference with the right to privacy and right to protection of personal data. Therefore this interference must be based on clear and publicly available rules and has to be limited to what is necessary in a democratic society.

There must be a clear benefit to any investigation when obtaining personal data. Only the minimum data to achieve what is needed should be collected.

Comment [PG5]: The "clear benefit" of data collection is a category that is not part of data protection law. It should therefore be deleted.

Example:
In case of Telephone Billing only the number(s) required for the time periods being investigated should be sought.

Personal data collected should only fit one of the purposes of prevention, detection or investigation of a criminal offence. The definition of real danger/specific criminal offence has been widened and relates to the suspicion of criminal activity which has either taken place or is expected to take place in the future.

Comment [PG6]: What is the reason behind this restriction according to which the collection of data should only fit ONE of the purposes mentioned? This is not in line with the vast range of purposes referred to in Directive 2016/680.

Comment [PG7]: The word "real" should be deleted because the authors do not explain when a danger/specific criminal offence is considered real.

Example:
There may be intelligence that a specific Money Transfer Office was being used to launder money. This would justify the collection of data in relation to the owners and customers of the specific business. It would not justify the collection of data in relation to the owners and customers of all Money Transfer Offices in the city.

Any exceptions to this must be underpinned by domestic legislation.

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

2.2. Where data concerning an individual have been collected and stored without her or his knowledge, and unless the data are deleted, that person should be informed, where

practicable, that information is held about her or him as soon as the object of the police activities is no longer likely to be prejudiced.

This relates to individuals subjected to covert, targeted surveillance and/or investigation and not those persons captured by mass surveillance techniques such as CCTV.

If an individual has their data collected during the course of an investigation where they are the suspect, as soon as circumstances permit the police should advise the individual of the data processing.

The police do not need to do so if they believe that providing this information to the individual may prejudice the investigation, allowing them to abscond or destroy evidence.

If the data is not used it should be deleted immediately.

Comment [PG8]: To be deleted. Sophisticated deletion rules contained in the EU acquis and domestic law are not adequately reflected in such a brief statement.

Occasionally long term data retention is justified and disclosure to a data subject is prejudicial. There must be valid justified reasons for the long-term retention of such data. The grounds for retention and processing should be periodically reviewed.

Example:
For the purpose of covert monitoring of a high risk sex offender long-term data processing might be justified and long-term data retention to the extent those data are necessary for this purpose.

2.3. The collection of data by technical surveillance or other automated means should be provided for in specific provisions.

Collection of personal data by technical surveillance or other automated means should only be done if legislation allows. The Police and other law enforcement agencies must work within the law which must be based as a minimum on the provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

Article 8 of the ECHR provides for a general right to respect for private and family life, as well as a privacy-based framework for the regulation of surveillance and data use. This right should only be interfered with if in accordance with domestic law and if it is necessary in the interests of national security, public safety, the prevention of disorder or crime or morals, or for the protection of the rights and freedoms of others.

Case-law of the European Court of Human Rights should be regularly reviewed in relation to the collection of data by technical surveillance. Previous judgments have stated that such forms of technical surveillance must be authorised and guaranteed against abuse. Case-law should also be reviewed in relation to the arrest or detention for questioning, search and seizure, methods of interrogation, taking of body samples/biometrics as these too must conform to relevant domestic legislation and the provisions of the Convention as interpreted by the European Court of Human Rights.

Individuals should not be subject to measures or decisions having a significant legal effect on them based on automatic processing, unless authorised by national law and subject to suitable safeguards to protect the individual's rights and legitimate interests. They should be duly informed about the type of processing used and the information should be provided in clear and plain language, allowing individuals to make sense of the logic of the processing.

Internet of Things (IoT) is formed by the networked connection of physical objects such as devices, vehicles, buildings and other items embedded with electronics, software that enables these objects to collect and exchange data. Data sent to and from the police and its employees during operational activity (e.g. GPS and bodycams) via the Internet can create vulnerabilities. IoT requires measures such as data authentication, integrity, access control and data protection to ensure resilience to (cyber) attacks.

Big data and profiling in the law enforcement sector
As life is becoming increasingly digital the amount of personal data that is generated, collected and shared through the internet is increasing. Technological advances in processing and analysing large and complex data sets leading to big data and big data analytics pose opportunities and challenges to law enforcement agencies 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 intrusion, impacting on individual's fundamental rights, such as the right to privacy and data protection.

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

- Databases originating from one domain is used in another domain, which changes the context and may lead to inaccurate conclusions.
- Inaccurate conclusions may have grave consequences for the individuals involved especially in the law enforcement domain when a lack of transparency by the data controller exists and confidentiality of information is observed.
- Profiling may lead to drawing discriminatory or unfair conclusions, which may result in reinforcement of stereotypes, stigmatisation and subsequent discrimination.
- The increasing amount of sensitive and confidential personal data held by law enforcement agencies may lead to severe vulnerabilities of their databases and subsequent risk of data breaches if information security is not guaranteed.

Where personal data is being used data controllers must ensure they are complying with their obligations under the data protection principles and should take due account of the following requirements.

- Quality of data used in big data processes is an essential prerequisite, verification of data accuracy, context and relevance of the data is required.
- Transparency should be provided by the data controller by explaining how the data are processed in accordance with data protection principles. If data collected for one purpose is used for another compatible purpose the data controller should make its users 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 is needed 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.

2.4. The collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of a particular inquiry.

The collection of personal data solely on the basis of:

- Racial or ethnic origin,
- Religious beliefs and convictions,
- Sexual life or orientation,
- Political opinions, or
- Belonging to a particular movement or organisation such as trade-union membership,

should be prohibited, unless such collection is strictly necessary for the purposes of a particular enquiry. The same applies for personal data concerning health and genetic or biometric data.

This must comply with national legislation and Article 8 ECHR. The reference to sexual behaviour does not apply where an offence has been committed.

Comment [PG9]: An approach other than the one pursued in Directive 2016/680 (which does not contain a general prohibition) is adopted here and should therefore be rejected. Furthermore, it is not clear what is meant by "collection of personal data solely on the basis of …".

Example:
Processing data on purely religious beliefs would not be allowed. However, in an investigation of a group of persons engaging in possible terrorist activities based on Islamic jihadi convictions it would be of essential importance to process this data.

Principle 3 - Storage of data

3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law.

In order to allow police to perform their tasks in an effective way, personal data collected for police purposes needs to be stored according to specific criteria and depending on their nature (e.g. soft or hard data) and classification.

Any stored data should be adequate, relevant and not excessive in relation to the purposes for which they are collected. Data accuracy and reliability is essential for the police to be able to perform their duties.

Police should provide systems and mechanisms to ensure the data that is stored is as accurate as possible and that integrity of data is maintained. Privacy-by-Design can assist in achieving this. At the same time the rights and freedoms of individuals need to be taken fully into account.

The structure of the files and quality of the data stored in them should comply with all legal obligations, national and international. International obligations include providing data to international bodies such as Europol, Eurojust and INTERPOL, bilateral agreements and mutual legal assistance between member states.

3.2. As far as possible, the different categories of data stored should be distinguished in accordance with their degree of accuracy or reliability and, in particular, data based on facts should be distinguished from data based on opinions or personal assessments.

Data should be categorised according to the degree of accuracy and reliability in order to assist 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.

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.

Classification of data is also important when it is to be communicated to other law enforcement agencies or states.

There should be a clear distinction in how police store personal data that relates to different categories of persons, such as 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.

3.3. Where data which have been collected for administrative purposes are to be stored permanently, they should be stored in a separate file. In any case, measures should be taken so that administrative data are not subject to rules applicable to police data.

Any administrative police data, data not used for the purposes of preventing, detecting or investigating crime, should be stored independently as this may not be subject to the same rules as data collected for police purposes.

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

Principle 4 – Use of data by the police

4. Subject to Principle 5, personal data collected and stored by the police for police purposes should be used exclusively for those purposes.

According to the purpose limitation principle, personal data collected for law enforcement purposes should be used exclusively for those purposes and not be used in any way that is incompatible unless this is provided for in national law.

The processing of personal data in a way incompatible with the purposes specified at collection is unlawful and not permitted.

Comment [PG10]: To be deleted; incompatible with the EU data protection acquis (Directive 2016/680 contains a vast range of purposes, and Regulation 2016/679 contains a sophisticated regime for amending purposes).

Principle 5 - Communication of data

5.1. Communication within the police sector

The communication of data between police bodies to be used for police purposes should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of these bodies.

Police authorities should only share information when there is a legal basis for the request, e.g. an ongoing criminal investigation or a shared law enforcement task.

5.2.i. Communication to other public bodies

Communication of data to other public bodies should only be permissible if, in a particular case:
a. there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority, or if
b. these data are indispensable to the recipient to enable the fulfilment of her or his own lawful task and provided that the aim of the collection or processing to be carried out by the recipient is not incompatible with the original processing, and the legal obligations of the communicating body are not contrary to this.

5.2.ii. Furthermore, communication to other public bodies is exceptionally permissible if, in a particular case:
a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if
b. the communication is necessary so as to prevent a serious and imminent danger.

There are stricter principles when data is to be transmitted outside of the police sector as the communication could be used for non-police purposes.

Communication of data to any other of these public bodies is only allowed if there is a legal basis for the transmission, such as authorisation from a court or specific legislation to permit the transmission or if there is permission from the supervisory authority (see principle 1).

Mutual assistance between the police and public bodies allows the public bodies to have access to police data which would be essential to their investigations or other legal duties.

Example:
Customs authority investigating a Tax Fraud or an Immigration authority investigating an Asylum claim.

The communicated data may only be used by the receiving body for the purposes for which the data was transferred. Communication to any other public authority is also allowed if it is in the data subject's interest without doubt and they have consented for the transfer.

Example:
A claim for social security made by a migrant. Police data may be required to verify the legal status. It would be in the interest of the Social Security office and the claimant for this transfer of

data to take place.

It is also permitted to communicate any data if it is in the public interest and or the communication is required to prevent serious danger.

5.3.i. Communication to private parties

The communication of data to private parties should only be permissible if, in a particular case, there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority.

5.3.ii. Communication to private parties is exceptionally permissible if, in a particular case:
a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented
or circumstances are such as to allow a clear presumption of such consent, or if
b. the communication is necessary so as to prevent a serious and imminent danger.

There may be occasions when it is necessary for the police to communicate data to private bodies.

Example:
When police communicate with the financial sector in relation to known Fraud or Theft offenders or when they communicate with an airline about stolen or lost travel documents.

These transfers should be thought of as the exceptional and there must be a clear legal basis and or authorisation for any communication to occur.

Principle 5.3 repeats the same conditions set out in Principle 5.2.ii.

5.4. International communication

Communication of data to foreign authorities should be restricted to police bodies. It should only be permissible:
a. if there exists a clear legal provision under national or international law,
b. in the absence of such a provision, if the communication is necessary for the prevention of a serious and imminent danger or is necessary for the suppression of a serious criminal offence under ordinary law, and provided that domestic regulations for the protection of the person are not prejudiced.

Comment [PG11]: Article 39 of Directive 2016/680, which - under certain circumstances - also allows for communication of data to private parties in third countries, is not taken into account here.

Any international communication of personal data should only take place if there is a clear legal basis. The application of 5.4b will only exist if the recipient state is not a member of Interpol and or any authorising treaty to allow the communication.

Any communication of data internationally should be strictly limited to another police organisation and should be in accordance with international agreements on mutual assistance, co-operation within the framework of Interpol, Europol, Eurojust or any other bilateral agreements made regarding effective cooperation and communication.

It is recognised that in certain member states pieces of police work are carried out by non-police authorities. The term "police bodies" should be understood in a broad sense, it can include other public authorities that investigate crime.

When considering sharing any data always consider whether the receiving authority is performing a function related to the prevention, detection or investigation of crime.

The sending authority should ensure there is an adequate level of data protection in the receiving state and that the receiving state complies with the relevant rules in respect of international dissemination of data. This includes providing for appropriate safeguards regarding data protection in cases no relevant national legal provisions or international agreements are in place and a serious danger requires the transfer.

Communications should always comply with adequacy requirements 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 conditions are to be adhered to.

Example: The receiving state requires the permission of the sending state before forwarding the data elsewhere.

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. Further onward transfer of data should not be allowed for general law enforcement purposes.

5.5.i. Requests for communication

Subject to specific provisions contained in national legislation or in international agreements, requests for communication of data should provide indications as to the body or person requesting them as well as the reason for the request and its objective.

Principle 5.5 outlines the rules which govern the different forms of communication previously mentioned. These rules are such as Interpol's "Rules on Processing Data", the provisions of the European Convention on Mutual Assistance in Criminal Matters of 20 April 1959 and the Cybercrime Convention (CETS No. 185).

The aim of this principle is to ensure that any transfer of data is justified. This relates to exchanges within a country or to an international partner. The request should clearly state details of the requesting party and specify the reason for the request as well as the purpose for the transfer of data.

5.5.ii. Conditions for communication

As far as possible, the quality of data should be verified at the latest at the time of their communication. As far as possible, in all communications of data, judicial decisions, as

well as decisions not to prosecute, should be indicated and data based on opinions or personal assessments checked at source before being communicated and their degree of accuracy or reliability indicated.

If it is discovered that the data are no longer accurate and up to date, they should not be communicated. If data which are no longer accurate or up to date have been communicated, the communicating body should inform as far as possible all the recipients of the data of their non-conformity.

The use of the phrase "as far as possible" means that the conditions set out in this part of the principle should be applied when it is feasible to do so. It is acknowledged that police are not always informed of judicial decisions.

There is flexibility in this element of the principle as it is recognised that different member states have different periods of monitoring. Therefore the quality of data can be assessed up to the moment of communication.

5.5.iii. Safeguards for communication

The data communicated to other public bodies, private parties and foreign authorities should not be used for purposes other than those specified in the request for communication.

Use of the data for other purposes should, without prejudice to paragraphs 5.2 to 5.4 of this principle, be made subject to the agreement of the communicating body.

Any data communicated outside of the domestic police setting 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 gives agreement to any further use and if the different purpose is one or more of the factors outlined in Principles 5.2 to 5.4.

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

The interconnection of files with files held for different purposes is subject to either of the following conditions:
a. the grant of an authorisation by the supervisory body for the purposes of an inquiry into a particular offence, or
b. in compliance with a clear legal provision.

Direct access/on-line access to a file should only be allowed if it is in accordance with domestic legislation which should take account of Principles 3 to 6.

This relates to the specific circumstances where police may seek to collect data by coordinating its information with other data owners.

Example:
The police might be linking up its files with files held for different purposes, such as those held

by other public bodies and or private organisations. This may be in relation to an ongoing criminal investigation or to identify thematic trends in a certain crime type.

In order for any of these actions to be legitimate they must be authorised and be underpinned by a legal framework.

If the police have direct access to files of other law enforcement bodies or non-law enforcement bodies they must only access and use the data in accordance with domestic legislation which should reflect the key data protection principles.

Principle 6 – Publicity, right of access to police files, right of rectification and right of appeal

6.1. The supervisory authority should take measures so as to satisfy itself that the public is informed of the existence of files which are the subject of notification as well as of its rights in regard to these files. Implementation of this principle should take account of the specific nature of ad hoc files, in particular the need to avoid serious prejudice to the performance of a legal task of the police bodies.

The data controller should ensure that any relevant files are notified to the public along with any specific conditions related to the files such as categorisation of data, storage and handling conditions. Due account has to be taken of the particularities of police work when implementing this principle, in particular the need to avoid prejudice to the performance of a legal task of the police bodies. The DPA may inspect the policy in place and recommend that the necessary information is made public.

Formatted: Font: Not Bold

Comment [PG12]: The objective of this proposal is to stress the technical requirement of having the chance to limit the public information on data processed by the police.

The information provided should strike the right balance between all interests concerned and take account of the specific nature of ad hoc or temporary files and other particularly sensitive files, such as criminal intelligence files, in order to avoid serious prejudice to police in performing their functions.

The information to the public should promote awareness, inform them of their rights and provide clear guidance on exercising their rights regarding these files. Information provided should also include detail 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 can perform a role in informing the public, but the publicity does not need to be restricted to website information, it may be provided by other media. It is recommended as good practice to have in place letter templates to help the data subject in exercising her or his rights. Template letters could be provided by the same website used for the publicity and information.

The data controller should provide sufficient information to the public on its website or by any other suitable means.

In respect of any publicity campaign highlighting data protection and data subject's rights, this would be the responsibility of a Government Ministry to provide.

6.2. The data subject should be able to obtain access to a police file at reasonable intervals and without excessive delay in accordance with the arrangements provided for by domestic law.

Accessing data is a fundamental right for the data subject in relation to their personal data. Domestic law can provide for a direct or indirect right of access.

Regarding direct access the data subject can request access to the controller of the files. The data controller will assess the request and any possible exemptions and reply directly to the data subject. If the right of access provided for is indirect the data subject may direct her or his request to the DPA, 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 DPA will then reply to the data subject.

The data subject should be able to make requests for access free of charge at reasonable intervals. The data controller should assess the request and reply to the data subject within a reasonable time-limit as provided for by domestic law.

There should be arrangements in place to confirm the identity of the data subject before access to any data is granted as well as if the data subject delegates authority to someone else to exercise their rights.

6.3. The data subject should be able to obtain, where appropriate, rectification of her or his data which are contained in a file.

Personal data which the exercise of the right of access reveals to be inaccurate or which are found to be excessive, inaccurate or irrelevant in application of any of the other principles contained in this Recommendation should be erased or corrected or else be the subject of a corrective statement added to the file.

Such erasure or corrective measures should extend as far as possible to all documents accompanying the police file and, if not done immediately, should be carried out, at the latest, at the time of subsequent processing of the data or of their next communication.

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 is incorrect, excessive or irrelevant the data subject should have the right to challenge it and ensure it is amended or deleted.

In some cases it may be appropriate to add additional or corrective information to the file.

Example:
If person A submitted a declaration against person B accusing him of committing a serious offence and later it emerges that the accusation was false, it might be relevant for police to keep the false statement. Although the statement was proven to be false, adding a clear corrective statement to the file instead of removing the false statement might be necessary.

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

6.4. Exercise of the rights of access, rectification and erasure should only be restricted insofar as a restriction is indispensable for the performance of a legal task of the police or is necessary for the protection of the data subject or the rights and freedoms of others.

Data subjects should only be restricted from accessing or amending any data held on them if by doing so it will have a negative impact on the police's legal task, the protection of the data subject or the rights and freedoms of others, or the protection of national security.

It may be necessary for police not to disclose information on the processing of personal data if for example it relates to an ongoing investigation. Disclosure of data might jeopardise an investigation and should therefore be excluded for its duration.

Example:
If disclosure of information may seriously endanger the safety of a witness or an informant it should be excluded for that reason.

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.

In the interests of the data subject, a written statement can be excluded by law for specific cases.

A data subject may be required to obtain a copy of her or his police file for a prospective employer. To obtain a written copy or statement may not be in their interest and therefore in such cases domestic law may authorise oral communication of the contents.

6.5. A refusal or a restriction of those rights should be reasoned in writing. It should only be possible to refuse to communicate the reasons insofar as this is indispensable for the performance of a legal task of the police or is necessary for the protection of the rights and freedoms of others.

Any refusals provided to a data subject's request should be provided in writing providing clear justification to the decision-making which can be verified by an independent authority or court. It is possible that communicating the reasons for refusal poses risks to the police or the data subject or the rights and freedoms of others. If this is the case it should be well documented and provided to the independent authority or court to be verified if required.

6.6. Where access is refused, the data subject should be able to appeal to the supervisory authority or to another independent body which shall satisfy itself that the refusal is well founded.

The data subject should be informed of all available options following a refusal decision such as an appeal either to the DPA or to another independent authority.

The data subject should have access to a court or tribunal in order to submit an appeal and have the reasons for refusal checked whenever he or she is not satisfied with the reply given. The inspecting authority should have sufficient powers to examine the police file concerned and have the assessment communicated.

Depending on the domestic 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 may be 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, and that the file is in order. Alternatively, the inspecting body may decide to release the data contained in the file to the data subject. Furthermore the court or tribunal may have powers to enforce the access, correction or deletion of data from the file.

Principle 7 - Length of storage and updating of data

7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored. For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject; particular categories of data.

7.2. Rules aimed at fixing storage periods for the different categories of personal data as well as regular checks on their quality should be established in agreement with the supervisory authority or in accordance with domestic law.

Rules should exist in relation to the storage and retention of data. Police files should be periodically reviewed to ensure data no longer required is deleted.

The quality of the data should be regularly checked according to these rules. These rules may be laid down in domestic law or provided in agreement with the DPA.

If the police are to create the rules, they should consider consulting with the supervisory authority to ensure they are fit for purpose.

Comment [PG13]: The objective of this proposal is to refrain from extending the consultation recommendations mentioned above.

The listed considerations should be kept in mind when deciding whether or not the data is still required for the prevention, detection or investigation of crime. As should keeping data for the purposes of auditing.

An automated mechanism, providing for deletion of files in compliance with the time limits for storage and an automated warning timed well in advance of the time limit is recommended.

Audit logs related to data processing should be available for inspection and auditing purposes.

Principle 8 - Data security

The responsible body should take all the necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration. The different characteristics and contents of files should, for this purpose, be taken into account.

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 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 is the greater protection will be required.

Authorisation and authentication mechanisms are essential to protect the data and sensitive information should always be encrypted. An audit regime could be implemented to check the level of security is appropriate.

Police are advised to execute a Privacy (Data Protection) Impact Assessment (PIA) to assess the privacy risks to individuals in respect of the collection, use and any disclosure of information. This will help to identify risks and develop solutions to ensure that concerns are addressed appropriately.

Comment [PG14]: The PIA aspect and the data security aspect should be considered independently. Furthermore, the requirement to conduct a PIA should apply only in cases justifying the related efforts (similarly to 1.3 on consulting the DPA, if possible).

An Identity & Access Management System (IAM) should be used 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 implement measures designed to ensure:

- equipment access control,
- data media control,
- storage control,
- user control,
- data access control,
- communication control,
- input control,
- transport control,
- recovery and system 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 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. Privacy-by-Design requires the implementation of Privacy Enhancing Technologies (PETs) to enable users to better protect their personal data.

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. 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:

FIU.NET - EU Financial Intelligence Units ('FIUs') started, in 2013, to use the PETs technology as additional feature to the existing exchange of information via the FIU.NET decentralised computer network.

FIU.NET is used for fighting money laundering and terrorism financing. The data processing in FIU.NET excludes unnecessary requests, improves timeliness and enhances privacy by ways of autonomous and anonymous data analysis.
The used PETs technology allows connected FIUs to 'match' their data with other FIUs in order to check whether other FIUs have information on a particular individual in their databases, to conduct joint analysis for detection of relations and networks and to identify trends and threats between distributed data sources.
Core principles of the PETs technology used are autonomy and decentralisation. These principles guarantee that only information owners have full control and data governance on information sources they connect.

Cloud Computing

Clouds use networks to connect users' end point devices, like computers or smart phones, to resources that are centralised in a data center. Clouds can be accessed from any location, allowing mobile workers to access their business systems on demand.

Cloud Computing is transforming the way Information and Communication Technology (ICT) is deployed and used. Data protection and security in the Cloud is difficult to define and use in the same way across different cloud systems. This is because globally they are underpinned by different legal systems and levels of data protection. As a result organisations often do not understand the risks and should encrypt data before using cloud services.

It is essential to draft effective contracts with regular review of contractual terms to provide the correct level of protection to the organisation.

Comment [PG15]: This paragraph pays too little attention to the fact that, in addition to promoting data security, Privacy by Design can also contribute to the development of privacy-friendly processing operations in the police sector (e.g. by developing and applying pseudonymization techniques and using pseudonymized data, for instance to compare large data volumes and to ensure that subsequent data exchanges are more targeted and economic).