15 Principles on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Principle 1

(Protection of rights and freedoms)

1. Personal data must be processed by ensuring a high level of protection of data subjects' rights, fundamental freedoms and dignity, including the right to personal data protection.

Principle 2

(Minimization)

1. The use of personal data shall be configured by minimizing their processing if the purposes sought can be achieved by using anonymous or non identifying information.

Principle 3

(Transparency)

1. The processing of personal data must be transparent under the terms set out in the law.

2. The type of data and processing operations, the relevant retention period, and the identity of the controller and processor(s) must be specified and made available.

3. The results achieved by means of the various categories of processing performed should be publicized regularly in order to assess whether the processing is further helpful in concrete.

Principle 4

(Legitimacy of processing)

1. Personal data may only be processed if this is provided for by a law setting out that processing by the competent authorities is necessary in order for the said authorities to fulfil their legitimate obligations.

Principle n. 5

(Data quality)

1. Personal data must be:

-processed fairly and lawfully;

-collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

-adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

-accurate and, where necessary, kept up to date;

-kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and/or further processed, in particular where the data are available on line.

2. Personal data must be evaluated taking into account their degree of accuracy or reliability, their source, the categories of data subjects, the purposes for which they are processed and the phase in which they are used. Every reasonable step should be taken to ensure that data which are inaccurate or incomplete are erased or rectified.

3. Data mining and any form of large-scale processing of massive quantities of personal data, in particular where related to non-suspects, including the transfer of such data to a different controller, shall only be permitted if carried out in compliance with the results of an examination performed by a supervisory authority either prior to the start thereof or in the context of preparation of a legislative measure.

4. Personal data must be processed by separating facts and objective evaluations from opinions or personal assessments, and the data related to prevention and prosecution of offences from data lawfully held for administrative purposes.

5. Appropriate checks prior and after an exchange of data must be established.

6. The controller shall take suitable measures in order to facilitate respect for the principles laid down herein, including by means of ad hoc software, as also related to the possible notification of rectification, erasure or blocking to third party recipients.

Principle 6

(Special categories of data)

1. The processing of personal data solely on the basis that they reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, and the processing of personal data concerning health or sex life shall be prohibited. The processing of these data may only be carried out if absolutely necessary for the purpose of a particular inquiry.

2. Appropriate safeguards shall be provided for by specific provisions, or on the basis of prior checking, in respect of processing operations that are likely to present specific risks to the rights and freedoms of data subjects, such as in particular the processing of Dna profiles, biometric data, data of non-suspects and the use of particular surveillance techniques or new technologies.

Principle 7

(Information to be given to the data subject)

1. The data subject shall be informed of the fact that personal data concerning him are being processed, the categories of data concerned, the identity of the controller and/or his representative, if any, the legal basis and the purposes of the processing, the existence of the right to access and rectify the data concerning him, unless the provision of such information proves impossible or incompatible with the purposes of the processing, or involves a disproportionate effort compared to data subject's interests, or where the data subject already has this information.

2. The provision of information to the data subject may be delayed to the extent this is necessary in order not to jeopardize the purposes for which the data were collected and/or further processed.

Principle 8

(Right of access to data and rectification)

1. The data subject shall have the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay:

a. confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom data are disclosed,

b. communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

c. knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in principle 9;

2. The data subject shall have the right:

a. to rectification or, if appropriate, erasure of data that are processed in breach of these principles, in particular because of the incomplete or inaccurate nature of the data,

b. to have third parties to whom the data have been disclosed notified of any rectification or erasure carried out in compliance with (a), unless this proves impossible or involves a disproportionate effort.

3. The communication referred to in paragraph 1 may be refused or delayed if such a refusal or delay is necessary to:

a. protect security and public order or to prevent crime; or

b. the investigation, detection and prosecution of criminal offences; or

c. protect the rights and freedoms of third parties.

Principle 9

(Automated individual decisions)

1. Everyone has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him.

2. Subject to other principles, a person may be subjected to a decision of the kind referred to herein if that decision is authorised by a law which also lays down appropriate measures to safeguard the data subject's legitimate interests.

Principle 10

(Confidentiality and security of processing)

1. The controller and any person acting under the authority of the latter should not disclose or anyhow make available any personal data to which access is necessitated by virtue of their function, unless authorised or required to do so by law.

2. The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss or unauthorised disclosure, alteration and access or all other unlawful forms of processing. These measures should be of a level appropriate to the risks arising from the processing and the nature of the data to be protected, by also considering the reliability and confidentiality of the data, and must be reviewed periodically.

Principle 11

(Communication of personal data)

1. The communication of data should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of the competent authorities.

2. Data communicated in accordance with the principles set forth herein should only be used for the purposes for which they have been disclosed or, if provided for by the law or agreed upon by the competent authorities, where a concrete link exists with an ongoing investigation.

3. Communication to other public bodies or private parties 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 him to fulfil 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.

4. 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.

5. Communication of data to third countries or international bodies should be subject to the existence of an appropriate legal framework resulting from an examination performed prior to the start thereof by a supervisory authority or in the context of a legislative measure, providing in particular, that the request for such communication contains clear indications as to the body or person requesting them, the purpose, the proportionality and the security measures of the processing, and the adequate guarantees to ensure a mandatory framework about the use of data. Such guarantees should be assessed in general on the basis of a standard procedure by taking into account all the principles set out in this Annex.

Principle 12

(Notification and prior checking)

1. Member States shall identify the categories of permanent or ad hoc files likely to present specific risks to the rights and freedoms of data subjects, to be notified to a supervisory authority or subject to a prior checking under the conditions and procedures to be specified by domestic law.

Principle 13

(Responsibility)

1. The controller is responsible for ensuring that the provisions set out in the principles of this Annex are respected, in particular as for any activities performed by and/or committed to processors acting under his instructions.

Principle 14

(Judicial remedies and liability)

1. Every person has the right to a judicial legal remedy for any breach of the rights guaranteed to him by these principles.

2. The data subject has the right to compensation for any damage suffered by him because of the unlawful processing of personal data concerning him.

3. The controller may be exempted from his liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Principle 15

(Supervision)

1. Observance of the principles of personal data protection should be monitored and enforced by one or more public supervisory authorities. The supervisory authorities should in particular be endowed with powers of investigation and intervention allowing them in particular to instigate, as appropriate, the rectification or erasure of personal data whose processing does not comply with the principles established in this Annex. These authorities shall act in complete independence in exercising the functions entrusted to them.

2. The supervisory authorities shall be consulted when drawing up legislative and administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data or otherwise having an impact on them.

3. The supervisory authorities shall be endowed with:

a. investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of their supervisory duties,

b. effective powers of intervention, such as, for example that of delivering opinions before processing operations are carried out, in accordance with principle 12, and of ordering erasure or destruction of data, of imposing a definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to the parliament or other political institutions,

c. the power to engage in legal proceedings where the principles have been violated or to bring these violations to the attention of judicial authorities.

Decisions by the supervisory authorities which give rise to complaints may be appealed against through the courts.

4. Supervisory authorities shall hear and decide on claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in respect of the processing of personal data. The person concerned shall be informed of the outcome of the claim.

The supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the principle 8.3 is applied. The person shall at any rate be informed that a check has taken place.

5. Supervisory authorities shall draw up a report on their activities at regular intervals. The report shall be made public.