D3.1 – [Legal State of the Art on data protection]

February 25th, 2016

Author/s: Van Gyseghem Jean-Marc (University of Namur - Crids), Hallemans Sandrine (University of Namur - Crids)

Contributor/s: Name Surname (organization)

Deliverable Lead Beneficiary: University of Namur - Crids

This project has been co-funded by the HORIZON 2020 Programme of the European Union. This publication reflects the views only of the author, and the Commission cannot be held responsible for any use, which may be made of the information contained therein.

Deliverable number or supporting document title	D3.1 Legal State of the Art on data protection
Type	Report
Dissemination level	Public
Nature	Report
Publication date	29- February-2016
Author(s)	Van Gyseghem Jean-Marc (University of Namur - Crids), Hallemans Sandrine (University of Namur - Crids)
Contributor(s)	Name Surname (organization)
Reviewer(s)	Name Surname (organization)
Keywords	Privacy, data protection, panorama, legislation
Website	www.tesla-project.eu

CHANGE LOG

Version	Date	Description of change	Responsible
V1.0	02/16/2016	Initial document	Jean-Marc Van Gyseghem
V2.0	02/18/2016	Division of work	Jean-Marc Van Gyseghem
V3.0	02/20/2016	Panorama of legislation	Jean-Marc Van Gyseghem/Sandrine Hallemans
V4.0	02/28/2016	Version submitted to reviewer	Jean-Marc Van Gyseghem

Neither the TeSLA consortium as a whole, nor a certain party of the TeSLA consortium warrants that the information contained in this document is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

The commercial use of any information contained in this document may require a license from the proprietor of that information

Table of Contents

1 Introduction 6
2 Glossary 7
2.1 Personal data 7
2.2 Anonymous data 7
2.3 Coded (encrypted) data 7
2.4 Data controller 7
2.5 Data processor 7
2.6 Data Subject 7
2.7 Necessary processing 8
2.8 Necessity 8
2.9 Proportionality 8
2.10 Transparency 8
3 Main principles on data protection 9
3.1 Definition 9
3.2 Specified and limited purpose 9
3.3 Necessity/proportionality 9
3.3.1 Processing 9
3.3.2 Data 10
3.4 Quality of the data 10
3.5 Specific categories of data 11
3.6 Confidentiality/security 11
3.7 Accountability 11
3.8 Data subject rights 11
3.9 Sanction and data protection authority 12
3.10 Transborder flows 12
4 International Data Protection Frameworks 13
4.1 United Nations (UN) 13
4.1.1 Determinate purpose 13
4.1.2 Necessity/proportionality 13
4.1.3 Data quality/categories of data 14
4.1.4 Security 14
4.1.5 Transparency 14
4.1.6 Data subject rights 15

4.1.7 Sanction 15
4.1.8 Data protection authority 15
4.1.9 Transborder flows 15
4.2 OECD 16
4.2.1 Definitions 16
4.2.2 Determinate purpose 18
4.2.3 Necessity/proportionality 18
4.2.4 Data quality 18
4.2.5 Security 19
4.2.6 Transparency 19
4.2.7 Accountability 19
4.2.8 Data subject rights 20
4.2.9 Sanction 21
4.2.10 Data protection authority 21
4.2.11 Transborder flows 21
4.3 Council of Europe (CoE) 21
4.3.1 Definitions 22
4.3.2 Determinate purpose 23
4.3.3 Necessity/proportionality 23
4.3.4 Data quality 23
4.3.5 Security 24
4.3.6 Transparency 24
4.3.7 Accountability 25
4.3.8 Data subject rights 25
4.3.9 Sanction 25
4.3.10 Data protection authority 26
4.3.11 Transborder flows 26
4.4 European Union (EU) 27
4.4.1 Definitions 28
4.4.2 Determinate purpose 28
4.4.3 Necessity/proportionality 30
4.4.4 Data quality/special categories 32
4.4.5 Security 34
4.4.6 Transparency 36
4.4.7 Accountability 40

4.4.8 Data subject rights 40
4.4.9 Sanction 43
4.4.10 Data protection authority 44
4.4.11 Transborder flows 45
4.5 Madrid resolution 47
4.5.1 Definitions 48
4.5.2 Determinate purpose 48
4.5.3 Necessity/proportionality 49
4.5.4 Data quality/categories of data 51
4.5.5 Security 52
4.5.6 Transparency 52
4.5.7 Accountability 53
4.5.8 Data subject rights 54
4.5.9 Sanction 55
4.5.10 Data protection authority 55
4.5.11 Transborder flows 56
4.6 Asia-Pacific Economic Cooperation (APEC) 57
4.6.1 Definitions 57
4.6.2 Determinate purpose 57
4.6.3 Necessity/proportionality 58
4.6.4 Data quality/categories of data 58
4.6.5 Security 58
4.6.6 Transparency 59
4.6.7 Accountability 60
4.6.8 Data subject rights 60
4.6.9 Sanction 61
4.6.10 Data protection authority 61
4.6.11 Transborder flows 61
5 Panorama of the legislations 63

1 Introduction

TeSLA project provides to educational institutions, an adaptive trust e-assessment system for assuring e-assessment processes in online and blended environments. It will support both continuous and final assessment to improve the trust level across students, teachers and institutions.

The system will be developed taking into account privacy issues in order to provide a secured platform insuring the identity of both teachers and students. This is leading to personal data being processed by this platform which will collect those data to identify the users (students, teacher, etc) and process the information to guarantee the identity of these users and reduce as much as possible any cheating during the examination.

As the personal data processing is an issue, TeSLA must deal with it from the beginning in a process of privacy by design.

The authors took the option to list, in the first part, the principles while explaining them and to draw up, in a second part, a panorama of the international legislation.

2 Glossary

2.1 Personal data

Personal data means any information relating to an identified or identifiable natural person (see above).

2.2 Anonymous data

Rendering anonymous means that the data cannot be related to an identified or identifiable individual anymore. In consequence, it is not considered as personal data in the sense of Directive 95/46 on data protection.

2.3 Coded (encrypted) data

Coded data means any personal data which can be related to an individual by means of a code.

2.4 Data controller

The controller is, usually, the natural or legal person who alone, or jointly with others, determines the purposes and means of the processing of personal data. It's the one who will responsible of the all processing of the personal data.

2.5 Data processor

Data processor is, usually, any natural person, legal person, un-associated organization or public authority which processes personal data on behalf of the controller, except for the persons who, under the direct authority of the controller, are authorized to process the data.

2.6 Data Subject

The data subject is an identified or identifiable person whom the personal data refers to. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

2.7 Necessary processing

The data controller must limit both processing and data to the extent strictly necessary to achieve the purpose of processing. Furthermore, only the necessary data to the purpose of the processing will be processed.

2.8 Necessity

This concept means that the actions implemented must be limited to what is strictly necessary to achieve a legitimate aim.

2.9 Proportionality

This concept means that one may collect only personal data that are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

2.10 Transparency

The data must be processed fairly and lawfully. The person concerned has the right to know who processes his personal data and for what purpose.

3 Main principles on data protection

As we collaborate with computer scientists and the whole consortium in creating an adaptive trust e-assessment system, we have to mention the main principles on data protection in order to analyse the international frameworks while having them in mind. These main principles are common to most of the regional and international frameworks.

3.1 Definition

If all of the terms used are not the same, we obviously have to highlight that the definitions are alike.

Also, some definitions changed with time to stay in connection with the technology evolution and the apprehension of the concepts.

TeSLA will have to take into account the applicable definition in order to be as close as possible to the applicable legislation, which can differ from one country to another and from a partner to another.

3.2 Specified and limited purpose[1]

In the various texts we have analysed, this main principle is omnipresent. The concept of specified purpose is one expression of the concept of transparency. It allows the data subject to understand to which purpose his/her data will be processed. This will give the opportunity to control the processing made by the data controller.

Each processing can either have a different or a multiple purpose.

We also have to pay attention to the concept of further processing which implies that the first processing is used for a second purpose which was not considered at the beginning.

3.3 Necessity/proportionality[2]

This principle has to be seen at two different levels.

3.3.1 Processing

The less invasive processing must be chosen, it's a question of balance. The article 8 of the (European) Convention for Human Rights is very clear regarding this by using the words *"necessary in a democratic society"*[3].

[1] See working Group 29, Opinion 03/2013 on purpose limitation, 3.04.2013.
[2] See Group 29, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 27.02.2014,
[3] www.hri.org/docs/ECHR50.html#Convention

Funded by the European Commission

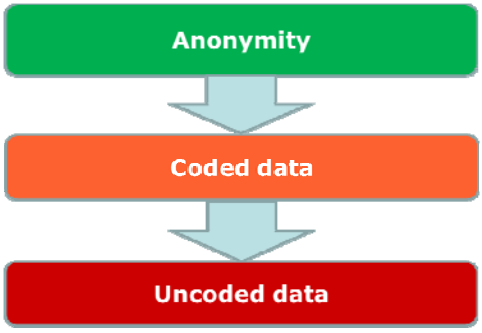
In the context of TesLA, the project will take into account all the processing that can be needed to reach its purpose and choose the one which is less invasive in the data subject privacy.

3.3.2 Data

Only the data necessary for the specified purpose can be processed[4]. Therefore, only the needed data can be collected and used, all others being excluded.

TeSLA would have to determine the kind of data needed for the purpose of the processing. This will be a major step as it will determine the kind of techniques the project will develop.

This concept of proportionality/necessity leads to the concept of "privacy stream" which can be summarized as such:



This means that

- Use of anonymous data as long as possible;
- If using anonymous data doesn't allow to reach the purpose of the processing, coded data can be processed;
- If using such a data won't allow to reach the purpose of the processing, uncoded data can be processed.

:

3.4 Quality of the data[5]

It is crucial to process data which are adequate, up to date and correct if we want to have a relevant processing.

Thanks to his/her right of access, the data subject has a look on the quality of his/her data and has the opportunity to ask for an eventual modification.

TeSLA will have to take care about keeping the data up-to-date but also adequate.

[4] Processing includes collect to destruction of the data.
[5] See working Group 29, Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones, 16.06.2015.

3.5 Specific categories of data

Some frameworks, but not all of them, make differences between categories of data: non-sensitive and sensitive data. Consequently, the regime of processing goes from authorisation to prohibition.

The concept of sensitivity varies from a region to another and we have to be aware about this.

In the TeSLA project, we will have to check if we are dealing with specific categories such as health related data.

3.6 Confidentiality/security

The data controller must insure the security of the processing against various events such as unauthorized intrusion, malware, accidental deletion, etc.

The security concerns two levels. The first one is technical and the second one is organisational.

When the concept of data processor is used, it is usually included in this concept of security.

Some regulations set the obligation of confidentiality.

3.7 Accountability[6]

The concept of accountability is growing and is becoming very important in many legislations and we have to take that in consideration.

The data controller or the person responsible of the processing has to ensure that each level of the hierarchy, even the subcontractor, observe the principles of data protection.

The article 29 working group wrote a very interesting document regarding this[7].

3.8 Data subject rights

Following the principle of auto determination, the data subject has some rights: the right of access, rectification, opposition, etc. However, some of those rights might be limited in certain circumstances.

TeSLA will have to set a procedure to allow the user/data subject to exercise her/his rights.

[6] See working Group 29, Opinion 3/2010 on the principle of accountability, 13.07.2010.
[7] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

3.9 Sanction and data protection authority

A law without sanction has no chance to be respected. Indeed, a law can be dissuasive only if it sets sanctions which have to be dissuasive themselves. On another hand, the sanction must be adequate and reach the core business of the person violating the law.

Besides the sanction, a data protection authority must be set with various competences amongst which the one to give penalties.

TeSLA will have to check which data protection authority will be competent for the notification duty.

3.10 Transborder flows

It would be a total non-sense to believe that the personal data will be confined to the national border as the objective of any data processing is the free movement between countries. We therefore necessarily have to regulate such movement in order to give an adequate protection of personal data.

As an example, European Union has set a specific regime of transborder flows in the Directive 95/46. In addition, a specific regime felt into agreement between United States of America and European Union the "Safe Harbor" agreement, which is a intermediary period due to the Schrems case[8] of the European Court of Justice. It is a kind of hybrid regime between an appropriateness regime and a contractual one.

This will be one of the issues to be solved by the project as the personal data will be processed by institutions outside Europe (third country). This implies that some specific rules will be applicable to these institutions.

[8] European Court of Justice, Maximillian Schrems v Data Protection Commissioner, 06.10.2015, http://curia.europa.eu/juris/documents.jsf?num=c-362/14.

4 International Data Protection Frameworks

4.1 United Nations (UN)

The UN adopted a regulation on data protection which is the "Guidelines for the Regulation of Computerized Personal Data Files" in 1990

4.1.1 Determinate purpose

The article 3 specifies that the purpose must be legitimate and determinate. The consequences of such settings are the duty of updating the data, adequacy and prohibition of use of the data for another purpose which is not compatible with the initial one without any authorization of the data subject, etc.

> *The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:*
>
> *(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;*
>
> *(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;*
>
> *(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.*

4.1.2 Necessity/proportionality

The article 2 specifies this concept indirectly but clearly. Indeed, the UN regulation sets a duty of relevance of the data and then of necessity to the determinate purpose.

> *Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.*

4.1.3 Data quality/categories of data

The article 2 implies that the data must be updated.

In addition, the data cannot be stored after the purpose is accomplished.

> *Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.*

The article 5 sets a prohibition of processing sensitive data.

> *Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.*

4.1.4 Security

UN imposes security measures against accidental loss, unauthorized access, etc (article 7).

> *Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.*

4.1.5 Transparency

The transparency is aimed by the article 4 which sets a right of access to the data subject.

> *Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if needs be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.*

4.1.6 Data subject rights

The article 4 gives a right of access to the data subject.

> *Everyone who offers proof of identity has the right to know whether information concerning them is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.*

4.1.7 Sanction

The article 8 sets that sanctions must be envisaged by the states.

> *In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.*

4.1.8 Data protection authority

The first part of the same article 8 mentions the need to create a supervisory authority in order to supervise the respect of the guidelines.

> *The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-a-vis persons or agencies responsible for processing and establishing data, and technical competence.*

4.1.9 Transborder flows

The transborder flow to a country is allowed only if this country insures similar data protection.

> *When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.*

4.2 OECD

The OECD adopted a recommendation on data protection which is the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" in 1980 modified in 2013.

The parties are:

- Australia
- Austria
- Belgium
- Canada
- Chile
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Israël
- Italy
- Japan
- Korea
- Luxembourg
- Mexico
- Netherlands
- New Zealand
- Norway
- Poland
- Portugal
- Slovak Republic
- Slovenia
- Spain
- Sweden
- Switzerland
- Turkey
- United Kingdom
- United States

4.2.1 Definitions

The OECD gives five definitions which are the "data controller", "personal data", laws protecting privacy, privacy enforcement authority and "transborder flow of personal data".

4.2.2 Determinate purpose

The paragraph 9 specifies that the purpose must be determinate. The consequences of such settings are the prohibition of use of the data for another purpose which is not compatible with the initial one without any authorization of the data subject.

> *The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*

4.2.3 Necessity/proportionality

The paragraph 8 specifies that the data must be relevant to the purpose which implies that they have to be necessary to the purpose.

> *Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*

The paragraph 7 also specifies a limitation to the collection setting that the data must be collected in a lawful and fair manner.

> *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

4.2.4 Data quality

The paragraph 8 specifies that the data must be accurate which implies that it must be updated.

> *Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*

There is no differentiation between categories of data and it's clearly set by the recommendation.

> *"Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited. There are precedents in European legislation to this effect (race, religious beliefs, criminal records, for instance). On the other hand, it may be held that no data are intrinsically "private" or "sensitive" but may become so in view of their context and use. This view is reflected, for example, in the privacy legislation of the United States.*

The Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive.
(…)"[9]

4.2.5 Security

The paragraph 11 specifies that the data must be protected thanks to reasonable warranties against unauthorized loss, access, use or disclosure.

> *Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*

This article must be red from both technical and organizational aspects. Indeed, it implies that the data controller takes the needed measure to ensure that the organization won't be a source of insecurity.

4.2.6 Transparency

The paragraph 12 specifies that the transparency must be ensured.

> *There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*

The transparency is also aimed by the paragraph 7 which sets the limitation of collection and the information of the data subject.

> *There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

4.2.7 Accountability

The paragraph 14 is totally explicit about the obligation of accountability:

> *A data controller should be accountable for complying with measures which give effect to the principles stated above.*

The text contains a part three concerning the implementation of accountability:

> *A data controller should:*
>
> *a) Have in place a privacy management programme that:*
>
> *i. gives effect to these Guidelines for all personal data under its control;*

[9] OECD privacy framework, p. 55.

Funded by the European Commission

ii. is tailored to the structure, scale, volume and sensitivity of its operations;

iii. provides for appropriate safeguards based on privacy risk assessment;

iv. is integrated into its governance structure and establishes internal oversight mechanisms;

v. includes plans for responding to inquiries and incidents;

vi. is updated in light of ongoing monitoring and periodic assessment;

b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and

c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

This part is completed by paragraph 16:

A data controller remains accountable for personal data under its control without regard to the location of the data.

4.2.8 Data subject rights

The paragraph 13 specifies the data subject rights which are the rights of access, modification, deletion, etc.

Individuals should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

b) to have communicated to them, data relating to them

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner; and

iv. in a form that is readily intelligible to them;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

Funded by the European Commission

d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

4.2.9 Sanction

Paragraph 19 introduced, in 2013, the obligation in charge of the Member countries to:

provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;

4.2.10 Data protection authority

The concept of data protection authority appears at the paragraph 15(b) but also in several part of the text. Its function is highlighted in the international Co-operation and in the recommendation on cross-border co-operation in the enforcement of laws protecting privacy.

4.2.11 Transborder flows

The OECD adopted a declaration in 2007 related to the transborder flows.

4.3 Council of Europe (CoE)

The CoE adopted the Convention 108 on data protection (1981) and the convention 181 (2001).

We'll mainly speak over Convention 108 and we'll mention the Convention 181 if needed.

47 Members:

- Albania
- Andorra
- Armenia
- Austria
- Azerbaijan
- Belgium
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia

- Finland
- France
- Georgia
- Germany
- Greece
- Hungary
- Iceland
- Ireland
- Italy
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Republic of Moldova
- Monaco
- Montenegro
- Netherlands
- Norway
- Poland
- Portugal
- Romania
- Russian Federation
- San Marino
- Serbia
- Slovak Republic
- Slovenia
- Spain
- Sweden
- Switzerland
- “The former Yugoslav Republic of Macedonia”
- Turkey
- Ukraine
- United Kingdom

6 Observer States:

- Canada
- Holy See
- Israel
- (Observer to the Parliamentary Assembly)
- Japan
- Mexico
- United States

4.3.1 Definitions

The CoE gives definitions.

4.3.2 Determinate purpose

The article 5 litera b specifies that the purpose must be determinate and legitimate.

> *Personal data undergoing automatic processing shall be:*
>
> *(…)*
>
> *b stored for specified and legitimate purposes and not used in a way incompatible with those purposes;*
>
> *(…)*

4.3.3 Necessity/proportionality

The article 5 specifies that the data must be appropriate, relevant and not excessive to the purpose which implies that they have to be necessary to the purpose.

> *Personal data undergoing automatic processing shall be:*
>
> *(…)*
>
> *c adequate, relevant and not excessive in relation to the purposes for which they are stored;*
>
> *d accurate and, where necessary, kept up to date;*
>
> *(…)*

4.3.4 Data quality

The articles 5 specifies that the data must be appropriate, relevant and not excessive to the purpose and updated.

> *Personal data undergoing automatic processing shall be:*
>
> *a obtained and processed fairly and lawfully;*
>
> *b stored for specified and legitimate purposes and not used in a way incompatible with those purposes;*
>
> *c adequate, relevant and not excessive in relation to the purposes for which they are stored;*
>
> *d accurate and, where necessary, kept up to date;*

> *e preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.*

The article 6 specifies that some data are sensitive and must be processed as such.

> *Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.*

4.3.5 Security

The article 7 specifies that the data must be protected against unauthorized loss, access, use or disclosure.

> *Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.*

The security must be technical and organizational.

The data processor is not specifically established but can be deduced from the article 7 but this is subject to debate.

4.3.6 Transparency

The transparency can be deduced from article 8 which specifies some rights to the data subject.

> *Any person shall be enabled:*
>
> *a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;*
>
> *b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;*
>
> *c to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;*
>
> *d to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.*

4.3.7 Accountability

There is no accountability clearly set in the Convention 108.

4.3.8 Data subject rights

The article 8 specifies the data subject rights which are the rights of access, modification, deletion, etc.

> *Any person shall be enabled:*
>
> *a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;*
>
> *b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;*
>
> *c to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;*
>
> *d to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.*

The article 9 specifies some limitations.

> *1 No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.*
>
> *2 Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:*
>
> *a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;*
>
> *b protecting the data subject or the rights and freedoms of others.*
>
> *3 Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.*

4.3.9 Sanction

The article 10 specifies that the states must set appropriate sanctions and recourses in case of violation of the national regulation on data protection.

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

4.3.10 Data protection authority

The Convention 181 introduces the establishment of national data protection authorities which have a role of control of the respect of the data protection regulation.

1 Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2 a To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3 The supervisory authorities shall exercise their functions in complete independence.

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

5 In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

4.3.11 Transborder flows

The Convention 181 is related to the transborder flows.

1 Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2 By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data :

a if domestic law provides for it because of :

– specific interests of the data subject, or

> *– legitimate prevailing interests, especially important public interests, or*
>
> *b if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.*

4.4 European Union (EU)

The EU adopted the Directive 95/46 on data protection (1995) and the Directive 2002/58 on electronic communications (2002).

We'll mainly speak over Directive 95/46 and we'll mention the Directive 2002/58 if needed.

About the European situation, we have to highlight that the directive 95/46 should be replaced by a new regulation which is on the way to be adopted next June 2016. This regulation will be analysed in depth in a following report but the main principles contained in this directive 95/46 will be maintained.

28 Member states:

- Austria (1995)
- Belgium (1958)
- Bulgaria (2007)
- Croatia (2013)
- Cyprus (2004)
- Czech Republic (2004)
- Denmark (1973)
- Estonia (2004)
- Finland (1995)
- France (1958)
- Germany (1958)
- Greece (1981)
- Hungary (2004)
- Ireland (1973)
- Italy (1958)
- Latvia (2004)
- Lithuania (2004)
- Luxembourg (1958)
- Malta (2004)
- Netherlands (1958)
- Poland (2004)
- Portugal (1986)
- Romania (2007)
- Slovakia (2004)
- Slovenia (2004)
- Spain (1986)

- Sweden (1995)
- United Kingdom (1973)

4.4.1 Definitions

The EU gives definitions.

4.4.2 Determinate purpose

The article 6 specifies that the purpose must be determinate and legitimate.

> *1. Member States shall provide that personal data must be:*
>
> *(a) (…);*
>
> *(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;*
>
> *(…)*

The legitimation principles are sets by the articles 7 and following.

> *Article 7*
>
> *Member States shall provide that personal data may be processed only if:*
>
> *(a) the data subject has unambiguously given his consent; or*
>
> *(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or*
>
> *(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or*
>
> *(d) processing is necessary in order to protect the vital interests of the data subject; or*
>
> *(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or*
>
> *(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).*

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

4.4.3 Necessity/proportionality

The article 6 specifies that the data must be appropriate, relevant and not excessive to the purpose which implies that they have to be necessary to the purpose.

1. Member States shall provide that personal data must be:

(…)

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

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) 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 or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

The necessity is also present at the level of the processing itself which imposes a necessity (article 7, 8 and 9).

Article 7

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

4.4.4 Data quality/special categories

The article 6 specifies the data must be appropriate, relevant and not excessive to the purpose and updated.

1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

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

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) 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 or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

The articles 8 and 9 specify that some data are sensitive and must be processed as such.

Article 8

The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

3. Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are

processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.

5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.

Member States may provide that data relating to administrative sanctions or judgements in civil cases shall also be processed under the control of official authority.

6. Derogations from paragraph 1 provided for in paragraphs 4 and 5 shall be notified to the Commission.

7. Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed.

Article 9

Processing of personal data and freedom of expression

Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.

4.4.5 Security

The article 17 specifies that the data must be protected (technically and organizationally) against unauthorized loss, access, use or disclosure, etc.

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Funded by the European Commission

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

The article 16 is related the confidentiality.

> *Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he is required to do so by law.*

The data processing is specifically established in the article 17.

> *2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.*
>
> *3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:*
>
> *- the processor shall act only on instructions from the controller,*
>
> *- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.*
>
> *4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.*

4.4.6 Transparency

The transparency is omnipresent in the Directive 95/46 and, therefore, is disseminated in several articles related to the information

> *Article 10*
>
> *Information in cases of collection of data from the data subject*
>
> *Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:*
>
> *(a) the identity of the controller and of his representative, if any;*
>
> *(b) the purposes of the processing for which the data are intended;*
>
> *(c) any further information such as*
>
> *- the recipients or categories of recipients of the data,*
>
> *- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,*

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

and notification

Article 18

Obligation to notify the supervisory authority

1. Member States shall provide that the controller or his representative, if any, must notify the supervisory authority referred to in Article 28 before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes.

2. Member States may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:

- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or

- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:

- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive

- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),

thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.

3. Member States may provide that paragraph 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Article 8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification.

Article 19

Contents of notification

1. Member States shall specify the information to be given in the notification. It shall include at least:

(a) the name and address of the controller and of his representative, if any;

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject and of the data or categories of data relating to them;

(d) the recipients or categories of recipient to whom the data might be disclosed;

(e) proposed transfers of data to third countries;

(f) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

2. Member States shall specify the procedures under which any change affecting the information referred to in paragraph 1 must be notified to the supervisory authority.

Article 20

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

Article 21

Publicizing of processing operations

1. Member States shall take measures to ensure that processing operations are publicized.

2. Member States shall provide that a register of processing operations notified in accordance with Article 18 shall be kept by the supervisory authority.

The register shall contain at least the information listed in Article 19 (1) (a) to (e).

The register may be inspected by any person.

3. Member States shall provide, in relation to processing operations not subject to notification, that controllers or another body appointed by the Member States make available at least the information referred to in Article 19 (1) (a) to (e) in an appropriate form to any person on request.

Member States may provide that this provision does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to

consultation either by the public in general or by any person who can provide proof of a legitimate interest.

The right of access is also an extension of the principle of transparency.

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- 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 the data are disclosed,

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

- 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 Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

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

4.4.7 Accountability

No accountability principle clearly defined but the Goup Article 29 has written a statement on it[10].

4.4.8 Data subject rights

The articles 10 and following specify the data subject rights which are the ones of information (also duty of the data controller) access, modification, deletion, etc.

Article 10

Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf

Funded by the European Commission

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Article 11

Information where the data have not been obtained from the data subject

1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

- the categories of data concerned,

- the recipients or categories of recipients,

- the existence of the right of access to and the right to rectify the data concerning him

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards.

Article 12

Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- 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 the data are disclosed,

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

- 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 Article 15 (1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

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

Article 14

The data subject's right to object

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

The article 13 specifies some limitations.

Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.

2. Subject to adequate legal safeguards, in particular that the data are not used for taking measures or decisions regarding any particular individual, Member States may, where there is clearly no risk of breaching the privacy of the data subject, restrict by a legislative measure the rights provided for in Article 12 when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.

4.4.9 Sanction

The article 24 specifies that the states must set appropriate sanctions in case of violation of the national regulation on data protection.

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.

4.4.10 Data protection authority

The article 28 introduces the establishment of national data protection authorities which have a role of control of the respect of the data protection regulation.

Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- 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 its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

- the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.

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

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

4.4.11 Transborder flows

The articles 25 and following specify criteria of transborder flows.

Article 25

Principles

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

Article 26

Derogations

1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that:

(a) the data subject has given his consent unambiguously to the proposed transfer; or

(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or

(e) the transfer is necessary in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

2. Without prejudice to paragraph 1, a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

3. The Member State shall inform the Commission and the other Member States of the authorizations it grants pursuant to paragraph 2.

If a Member State or the Commission objects on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2).

Member States shall take the necessary measures to comply with the Commission's decision.

4. Where the Commission decides, in accordance with the procedure referred to in Article 31 (2), that certain standard contractual clauses offer sufficient safeguards as required by paragraph 2, Member States shall take the necessary measures to comply with the Commission's decision.

4.5 Madrid resolution

The resolution of Madrid was adopted in November 2009.

Members of the working Group (National data protection Authorities):

- Cdata protection commission (Austria),
- Privacy protection commission (Belgium),
- Commission on computers and liberties (Burkina-Fasso),
- Office of the privacy commissioner of Canada,
- Information access commission of Quebec (Canada),
- Office for personal data protection (Czech Republic),
- European data protection supervisor,
- National commission on computers and liberties (France),
- Federal data protection commissioner (Germany),
- Data protection and freedom of information commissioner of berlin (Germany),
- Data protection commissioner of Schleswig-Holstein (Germany),
- Privacy commissioner for personal data (Hong Kong),
- Irish data protection commissioner,
- Italian data protection authority,
- Data protection commission (Netherlands),
- New Zealand privacy commissioner,
- National data protection commission (Portugal),
- Information commissioner of the republic of Slovenia, Spanish data
- Protection agency (Spain),
- Catalan data protection authority (Spain),
- Data protection agency of Madrid (Spain),
- Basque data protection agency (Spain),
- Federal data protection commissioner (Switzerland),
- Information commissioner’s office (United Kingdom)

4.5.1 Definitions

The Madrid resolution gives definitions.

4.5.2 Determinate purpose

The article 7 specifies that the purpose must be determinate and legitimate.

> *1. The processing of personal data should be limited to the fulfillment of the specific, explicit and legitimate purposes of the responsible person.*
>
> *2. The responsible person should not carry out any processing that is non-compatible with the purposes for which personal data were collected, unless he has the unambiguous consent of the data subject.*

The articles 12 and 13 are also concerned with legitimacy.

> *Article 12*
>
> *1. As a general rule, personal data may only be processed in one of the following situations:*
>
> *a. After obtaining the free, unambiguous and informed consent of the data subject;*
>
> *b. Where a legitimate interest of the responsible person justifies the processing, and the legitimate interests, rights and freedoms of data subjects do not prevail;*
>
> *c. Where the processing is necessary for the maintenance or the performance of a legal relationship between the responsible person and the data subject; or d. Where the processing is necessary for complying with an obligation imposed on the responsible person by the applicable national legislation, or is carried out by a public authority where necessary for the legitimate exercise of its powers.*
>
> *e. Where there are exceptional situations that threaten the life, health or security of the data subject or of another person.*
>
> *2. The responsible person shall provide simple, fast and efficient procedures that allow data subjects to withdraw their consent at any time and that shall not entail undue delay or cost, nor any gain whatsoever for the responsible person.*
>
> *Article 13*
>
> *1.The following personal data shall be deemed to be sensitive:*
>
> *a. Data which affect the data subject's most intimate sphere; or*
>
> *b.Data likely to give rise, in case of misuse, to:*
>
> *i. Unlawful or arbitrary discrimination; or*
>
> *ii A serious risk to the data subject..*

2. In particular, those personal data which can reveal aspects such as racial or ethnic origin, political opinions, or religious or philosophical beliefs as well as those data relating to health or sex life, will be considered sensitive data. The applicable national legislation may lay down other categories of sensitive data where the conditions referred to in the previous paragraph are met.

3. Due guarantees shall be established to preserve the rights of the data subjects by applicable national legislation, which shall lay down additional conditions for processing sensitive personal data.

4.5.3 Necessity/proportionality

The principle of necessity is included in the articles 8 and 12.

The article 8 specifies that the data must be appropriate, relevant and not excessive to the purpose which implies that they have to be necessary to the purpose. It also specifies a limitation to the collection.

1. The processing of personal data should be limited to such processing as is adequate, relevant and not excessive in relation to the purposes set out in the previous section.

2. In particular, the responsible person should make reasonable efforts to limit the processed personal data to the minimum necessary.

The article 12 specifies the necessity at the level of the processing itself.

1. As a general rule, personal data may only be processed in one of the following situations:

a. After obtaining the free, unambiguous and informed consent of the data subject;

b. Where a legitimate interest of the responsible person justifies the processing, and the legitimate interests, rights and freedoms of data subjects do not prevail;

c. Where the processing is necessary for the maintenance or the performance of a legal relationship between the responsible person and the data subject; or d. Where the processing is necessary for complying with an obligation imposed on the responsible person by the applicable national legislation, or is carried out by a public authority where necessary for the legitimate exercise of its powers.

e. Where there are exceptional situations that threaten the life, health or security of the data subject or of another person.

2. The responsible person shall provide simple, fast and efficient procedures that allow data subjects to withdraw their consent at any time and that shall not entail undue delay or cost, nor any gain whatsoever for the responsible person.

4.5.4 Data quality/categories of data

The article 9 specifies the concept of quality of the data as it is done in the previous regulations.

> *1. The responsible person should at all times ensure that personal data are accurate, as well as sufficient and kept up to date in such a way as to fulfill the purposes for which they are processed.*
>
> *2. The responsible person shall limit the period of retention of the processed personal data to the minimum necessary. Thus, when personal data are no longer necessary to fulfil the purposes which legitimized their processing they must be deleted or rendered anonymous.*

The articles 12 and 13 make a difference between categories of data which must be processed as follows.

> *Article 12*
>
> *1. As a general rule, personal data may only be processed in one of the following situations:*
>
> *a. After obtaining the free, unambiguous and informed consent of the data subject;*
>
> *b. Where a legitimate interest of the responsible person justifies the processing, and the legitimate interests, rights and freedoms of data subjects do not prevail;*
>
> *c. Where the processing is necessary for the maintenance or the performance of a legal relationship between the responsible person and the data subject; or d. Where the processing is necessary for complying with an obligation imposed on the responsible person by the applicable national legislation, or is carried out by a public authority where necessary for the legitimate exercise of its powers.*
>
> *e. Where there are exceptional situations that threaten the life, health or security of the data subject or of another person.*
>
> *2. The responsible person shall provide simple, fast and efficient procedures that allow data subjects to withdraw their consent at any time and that shall not entail undue delay or cost, nor any gain whatsoever for the responsible person.*
>
> *Article 13*
>
> *1.The following personal data shall be deemed to be sensitive:*
>
> *a. Data which affect the data subject's most intimate sphere; or*
>
> *b.Data likely to give rise, in case of misuse, to:*
>
> *i. Unlawful or arbitrary discrimination; or*

> *ii A serious risk to the data subject..*
>
> *2. In particular, those personal data which can reveal aspects such as racial or ethnic origin, political opinions, or religious or philosophical beliefs as well as those data relating to health or sex life, will be considered sensitive data. The applicable national legislation may lay down other categories of sensitive data where the conditions referred to in the previous paragraph are met.*
>
> *3. Due guarantees shall be established to preserve the rights of the data subjects by applicable national legislation, which shall lay down additional conditions for processing sensitive personal data.*

4.5.5 Security

The article 20 specifies that the data must be protected against unauthorized loss, access, use or disclosure.

> *1. Both the responsible person and any processing service provider must protect the personal data subject to processing with the appropriate technical and organizational measures to ensure, at each time, their integrity, confidentiality and availability. These measures depend on the existing risk, the possible consequences to data subjects, the sensitive nature of the personal data, the state of the art, the context in which the processing is carried out, and where appropriate the obligations contained in the applicable national legislation.*
>
> *2. Data subjects should be informed by those involved in any stage of the processing of any security breach that could significantly affect their pecuniary or non-pecuniary rights, as well as the measures taken for its resolution. This information should be provided in good time, in order to enable data subjects to seek the protection of their rights.*

The security must be technical and organizational.

The article 21 specifies a duty of confidentiality.

> *The responsible person and those involved at any stage of the processing shall maintain the confidentiality of personal data. This obligation shall remain even after the ending of the relationship with the data subject or, when appropriate, with the responsible person.*

The data processing is specifically established in these two articles.

4.5.6 Transparency

The transparency is specifically specified in the article 10 and the article 16 setting the data subject rights is an extension of the transparency.

> *Article 10 – Openness principle*

1. Every responsible person shall have transparent policies with regard to the processing of personal data.

2. The responsible person shall provide to the data subjects, as a minimum, information about the responsible person's identity, the intended purpose of processing, the recipients to whom their personal data will be disclosed and how data subjects may exercise the rights provided in this Document, as well as any further information necessary to guarantee fair processing of such personal data.

3. When personal data have been collected directly from the data subject, the information must be provided at the time of collection, unless it has already been provided.

4. When personal data have not been collected directly from the data subject, the responsible person must also inform him/her about the source of personal data. This information must be given within a reasonable period of time, but may be replaced by alternative measures if compliance is impossible or would involve a disproportionate effort by the responsible person.

5. Any information to be furnished to the data subject must be provided in an intelligible form, using a clear and plain language, in particular for any processing addressed specifically to minors.

6. Where personal data are collected on line by means of electronic communications networks, the obligations set out in the first and second paragraphs of this section may be satisfied by posting privacy policies that are easy to access and identify and include all the information mentioned above.

Article 16 – Right of access

1. The data subject has the right to obtain from the responsible person, upon request, information on the specific personal data subject to processing, as well as the source of such data, the purposes of processing and the recipients or categories of recipients to whom such data are or will be disclosed.

2. Any information to be furnished to the data subject must be provided in an intelligible form, using a clear and simple language.

3. Applicable national legislation may limit the repetitive exercise of this right that would require the responsible person to respond to multiple requests within short periods of time, unless the data subject states a legitimate reason when exercising this right.

4.5.7 Accountability

The article 11 sets clearly the accountability principle:

The responsible person shall:

a. Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation,

and

b. have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23.

4.5.8 Data subject rights

The articles 16 and following specify the data subject rights which are the rights of access, modification, deletion, etc.

Article 16 – right of access

1. The data subject has the right to obtain from the responsible person, upon request, information on the specific personal data subject to processing, as well as the source of such data, the purposes of processing and the recipients or categories of recipients to whom such data are or will be disclosed.

2. Any information to be furnished to the data subject must be provided in an intelligible form, using a clear and simple language.

3. Applicable national legislation may limit the repetitive exercise of this right that would require the responsible person to respond to multiple requests within short periods of time, unless the data subject states a legitimate reason when exercising this right.

Article 17 – rights to rectify and to delete

1. The data subject has the right to request from the responsible person the deletion or rectification of personal data that might be incomplete, inaccurate, unnecessary or excessive.

2. Where justified, the responsible person should carry out the rectification or deletion requested.

The responsible person should also notify this fact to third parties to whom personal data had been disclosed, where they are known.

3. Deletion of personal data is not justified where personal data must be retained for the performance of an obligation imposed on the responsible person by the applicable national legislation, or possibly by the contractual relations between the responsible person and the data subject.

Article 18 – Right to object

1. The data subject may object to the processing of personal data where there is a legitimate reason related to his/her specific personal situation.

2. The exercise of this right to object is not justified where the processing is necessary for the performance of a duty imposed on the responsible person by the applicable national legislation.

3. Any data subject may also object to those decisions which produce legal effects based solely on automated processing of personal data, except when the decision had been specifically requested by the data subject or when it is necessary for the establishment, the maintenance or the performance of a legal relation between the responsible person and the data subject. In the latter case, the data subject must be able to put his/her point of view

4.5.9 Sanction

None but it deals with liability in the article 25.

1. The responsible person will be liable for the pecuniary and/or non-pecuniary damages caused to the data subjects as a result of processing of personal data that had infringed the applicable laws on the protection of privacy with regard to the processing of personal data, except if the responsible person can demonstrate that the damage can not be attributed to him. This liability is without prejudice to any action by the responsible person against the processing service provider involved at any stage of the processing.

2. States will promote suitable measures to facilitate the access of data subjects to the relevant judicial or administrative processes that allow them to obtain compensation for the damage referred to in the preceding paragraph.

3. The aforementioned liability should exist without prejudice to the penal, civil or administrative penalties provided for, where appropriate, in case of violation of the provisions of domestic laws on the protection of privacy with regard to the processing of personal data.

4. The implementation of proactive measures such as those described in section 22 of this Document should be considered when determining the liability and penalties provided for in this section.

4.5.10 Data protection authority

The article 23 introduces the establishment of national data protection authorities which have a role of control with respect to the data protection regulation.

1. In every State there shall be one or more supervisory authorities, in accordance with its domestic law, that will be responsible for supervising the observance of the principles set out in this Document.

2. These supervisory authorities shall be impartial and independent, and will have technical competence, sufficient powers and adequate resources to deal with the claims filed by the data subjects, and to conduct investigations and interventions where necessary to ensure compliance with the applicable national legislation on the protection of privacy with regard to the processing of personal data.

3. In any case, without prejudice to any administrative remedy before the supervisory authorities referred to in the preceding paragraphs, including judicial oversight of their decisions, data subjects may have a direct recourse to the courts to enforce their rights under the provisions laid down in the applicable national legislation.

4.5.11 Transborder flows

One of the objectives of the Madrid resolution is the transborder flows. Therefore, such matter is specified in the resolution.

1. As a general rule, international transfers of personal data may be carried out when the State to which such data are transmitted affords, as a minimum, the level of protection provided for in this Document.

2. It will be possible to carry out international transfers of personal data to States that do not afford the level of protection provided for in this document where those who expect to transmit such data guarantee that the recipient will afford such level of protection; such guarantee may for example result from appropriate contractual clauses.

In particular, where the transfer is carried out within corporations or multinational groups, such guarantees may be contained in internal privacy rules, compliance with which is mandatory.

3. Moreover, national legislation applicable to those who expect to transmit data may permit an international transfer of personal data to States that do not afford the level of protection provided for in this Document, where necessary and in the interest of the data subject in the framework of a contractual relationship, to protect the vital interests of the data subject or of another person, or when legally required on important public interest grounds

4. Applicable national legislation may confer powers on the supervisory authorities referred to in section 23 to authorize some or all of the international transfers falling within their jurisdiction, before they are carried out. In any case, those who expect to carry out an international transfer of personal data should be capable of demonstrating that the transfer complies with the guarantees provided for in this Document and in particular where required by the supervisory authorities pursuant to the powers laid down in paragraph 23.2.

4.6 Asia-Pacific Economic Cooperation (APEC)

The APEC adopted a privacy framework in 2005.

The 21 members are:

- Australia
- Brunei Darussalam
- Canada
- Chile
- People's Republic of China
- Hong Kong, China
- Indonesia
- Japan
- Republic of Korea
- Malaysia
- Mexico
- New Zealand
- Papua New Guinea
- Peru
- The Philippines
- Russia
- Singapore
- Chinese Taipei
- Thailand
- The United States
- Vietnam

4.6.1 Definitions

The Privacy Framework gives definitions.

4.6.2 Determinate purpose

The principle of determinate purpose can be presumed from the article 15.

> *Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:*
>
> *(…)*
>
> *b) the purposes for which personal information is collected*
>
> *(…)*

4.6.3 Necessity/proportionality

The principle of necessity is included in the article 18.

The article 18 specifies that the data must be relevant to the purpose which implies that they have to be necessary to the purpose. It also specifies a collection limitation.

> *The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.*

The article 19 also introduces the concept of necessity.

> *Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except:*
>
> *a) with the consent of the individual whose personal information is collected;*
>
> *b) when necessary to provide a service or product requested by the individual; or,*
>
> *c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.*

4.6.4 Data quality/categories of data

The articles 18 and 21 specify the concept of quality of the data as is done in the previous regulations.

> *18.*
>
> *The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.*
>
> *19.*
>
> *Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.*

No difference is made between categories of data.

4.6.5 Security

The article 22 specifies that the data must be protected against unauthorized loss, access, use or disclosure.

> *Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized*

> *access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.*

The security looks to be technical and organizational.

The data processing is not specifically established in the Privacy framework.

4.6.6 Transparency

The transparency is not specifically specified but the article 23 that sets the data subject rights is an extension of the transparency.

> *23.*
>
> *Individuals should be able to:*
>
> *a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;*
>
> *b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;*
>
> *i. within a reasonable time;*
>
> *ii. at a charge, if any, that is not excessive;*
>
> *iii. in a reasonable manner;*
>
> *iv. in a form that is generally understandable; and,*
>
> *c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.*
>
> *25.*
>
> *If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.*

The article 24 sets some limitation to these rights:

> *24.*
>
> *Such access and opportunity for correction should be provided except where:*
>
> *(i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;*

(ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or

(iii) the information privacy of persons other than the individual would be violated.

4.6.7 Accountability

The accountability is set in the article 26:

A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

4.6.8 Data subject rights

The articles 23 and following specify the data subject rights which are the ones of access, modification, etc.

23.

Individuals should be able to:

a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them;

b) have communicated to them, after having provided sufficient proof of their identity, personal information about them;

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner;

iv. in a form that is generally understandable; and,

c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.

> *25.*
>
> *If a request under (a) or (b) or a challenge under (c) is denied, the individual should be provided with reasons why and be able to challenge such denial.*

The article 24 sets some limitations to these rights:

> *24.*
>
> *Such access and opportunity for correction should be provided except where:*
>
> *(i) the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question;*
>
> *(ii) the information should not be disclosed due to legal or security reasons or to protect confidential commercial information; or*
>
> *(iii) the information privacy of persons other than the individual would be violated.*

4.6.9 Sanction

The article 38 deals with the remedies/

> *38. A Member Economy's system of privacy protections should include an appropriate array of remedies for privacy protection violations, which could include redress, the ability to stop a violation from continuing, and other remedies. In determining the range of remedies for privacy protection violations, a number of factors should be taken into account by a Member Economy including:*
>
> *a) the particular system in that Member Economy for providing privacy protections (e.g., legislative enforcement powers, which may include rights of individuals to pursue legal action, industry self-regulation, or a combination of systems); and*
>
> *b) the importance of having a range of remedies commensurate with the extent of the actual or potential harm to individuals resulting from such violations.*

4.6.10 Data protection authority

None

4.6.11 Transborder flows

The articles 46 and following deal with this topic.

> *46.*

Member Economies will endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.

47.

To give effect to such cross-border privacy rules, Member Economies will endeavor to work with appropriate stakeholders to develop frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between and among the economies.

48.

Member Economies should endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable crossborder data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.

APEC also developed the APEC Cross Border Privacy Rules (CBPR) system[11] *"to build consumer, business and regulator trust in cross border flows of personal information. The APEC CBPR system requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework"*

[11] www.cbprs.org/default.aspx

Funded by the
European Commission

5 Panorama of the legislations

	ONU	OECD	Council of Europe	European Union	Madrid Resolution	APEC
Definitions	None	Paragraph 1	Article 2	Article 2	Article 2	Article 9
Determinate purpose	Article 3	Paragraph 9	Article 5	Article 6	Article 7	Article 15
Legitimacy	Article 3	Non explicit	Article 5	Article 6 Article 7 Article 8 Article 9	Article 7 Article 12 Article 13	None
Necessity/proportionality	Article 2	Paragraph 7 Paragraph 10	Article 5	Article 6 Article 7 Article 8 Article 9	Article 8 Article 12	Article 18 Article 19
Data quality	Article 2 Article 3	Paragraph 8	Article 5	Article 6	Article 9	Article18 Article 19
Categories of data	Article 5	Refusal	Article 6	Article 8 Article 9	Article 13	None
Security	Article 7	Paragraph 11	Article 7	Article 17 Article 5 (Dir 2002/58)	Article 20	Article 22
Confidentiality				Article 16	Article 21	None
Data processor	Article 2 (inference)	Article 7 (inference)	Article 7 (inference + debate)	Article 17	Article 20 Article 21	None
Openness	Article 3 (application) Article 4 (application)	Paragraph 12 Paragraph 7 (application)	Article 8 (application)	Article 12	Article 10 Article 16 (application)	Article 23 (application) Article 25 (application)
Accountability	None	Paragraph 14	None	None	Article 11	Article 26
Data subject rights	Article 4	Paragraph 13	Article 8 Article 9	Article 10 Article 11 Article 12 Article 13	Article 16 Article 17 Article 18	Article 23 Article 24 Article 25
Sanction	Article 8	Paragraph 14	Article 10	Article 24	Article 25	Article 38
Data protection authority	Article 8	Co-operation part and transborder flow.	Article 1 (Conv. 181)	Article 28	Article 23	None
Transborder flows	Article 9	Recommendation 2007	Article 2 (Conv. 181)	Article 25 Article 26	Article 15	Article 46 Article 47 Article 48

Funded by the European Commission

6 Conclusion

This report lists the international framework on data protection which has to be taken into account by the project.

This will be applicate all during the project in function of the evolution of it and the technics put in place.

In conclusion, this document will be completed during the project.

Funded by the
European Commission