CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

DRAFT EXPLANATORY REPORT

This document was prepared on the basis of the consolidated text of the modernised Convention 108 and the numbering of the articles does not correspond to the draft Amending Protocol of the Convention.

I. INTRODUCTION

Background

The Consultative Committee (T-PD) of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter referred to as 'Convention 108') decided at its 25th Plenary meeting (2-4 September 2009) to set as the first priority of its 'work programme for 2009 and beyond' the preparation of amendments to Convention 108.

In particular, the T-PD identified several angles of potential work on the convention, such as technological developments, information to be provided to the data subject, automated individual decisions, and the evaluation of the implementation of Convention 108 and its additional protocol by the contracting States.

This proposal of priority work was formally endorsed by the Committee of Ministers in March 2010, when the Ministers' Deputies (1079th meeting, 10 March 2010) welcomed the adoption of the T-PD work programme and encouraged the T-PD to start working on the modernisation of Convention 108.

The Ministers of Justice participating in the 30th Council of Europe Conference of Ministers of Justice (Istanbul, Turkey, 24 - 26 November 2010) furthermore expressed their support with the modernisation of Convention 108 in their Resolution n°3 on data protection and privacy in the third millennium.

The Parliamentary Assembly of the Council of Europe furthermore welcomed the modernisation exercise in its Resolution 1843(2011) on 'The protection of privacy and personal data on the Internet and online media'.

The T-PD started the work by commissioning an expert report[1] with a view to identifying areas in which a modernisation of Convention 108 would be needed to address new challenges posed by information and communication technologies.

A second report[2] was prepared with a view to tackling another crucial aspect of the modernisation: the evaluation of the implementation of Convention 108 by the contracting Parties.

[1] Report on the lacunae of the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No 108) resulting from technological developments (T-PD-BUR(2010)09), by Cécile de Terwangne, Jean-Marc Dinant, Jean-Philippe Moiny, Yves Poullet and Jean-Marc Van Gyzeghem of the CRIDS Namur.

[2] Report on the modalities and mechanisms for assessing implementation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) and its Additional Protocol (T-PD-BUR(2010)13Rev) by Marie Georges.

On the basis of the first report, the T-PD developed a list of issues to be examined in the context of the modernisation and a consultation document[3] containing 30 questions.

The 30 questions were publicly submitted for reactions and comments on the occasion of the 30th Anniversary of Convention 108, on 28 January 2011 (5th edition of Data Protection Day). This public consultation was aimed at enabling all actors concerned (individuals, civil society, private sector, regulators, supervisory authorities) – from around the globe – to share their views on what the new Convention 108 should look like in the future.

Numerous responses were received from the public sector (governmental authorities and data protection authorities), the private sector (banking, insurance, electronic commerce, marketing, audio-visual distribution, socio-economic research, etc.), academia and interested associations, and from various continents, not only from Europe.

It took three meetings of the Bureau of the T-PD in 2011 to convert this dense and extremely rich material[4] into concrete modernisation proposals[5] of Convention 108, which were examined in first reading by the 27th Plenary meeting of the T-PD (30 November-2 December 2011).

Further to the discussions held during this 27th Plenary meeting and subsequent submissions of the draft for comments, revised versions[6] of the modernisation proposals were prepared by the Bureau of the T-PD. The successive drafts were not only submitted to the T-PD for comment, but also to various Council of Europe committees, as well as to private sector and civil society stakeholders (in particular, on the occasion of an exchange of views held on 2 May 2012 at the Council of Europe premises in Brussels).

During its 28th Plenary meeting (19-22 June 2012), the T-PD gave a second reading of the proposals for modernisation of Convention 108[7] and instructed its Bureau to finalise the proposals having regard to these discussions and comments, with a view to their examination at the 29th plenary meeting (27-30 November 2012).

The proposals[8] and related written comments[9] were examined in third reading by the 29th Plenary meeting of the T-PD and modernisation proposals[10] were adopted for transmission to the Committee of Ministers, while the finalisation of the proposals would be entrusted to an intergovernmental ad hoc committee.

Draft terms of reference for an ad hoc committee on data protection (CAHDATA) were prepared and examined by the Bureau of the T-PD[11] before being transmitted to the Steering Committee on Media and Information Society (CDMSI), with a view to their submission to the Committee of Ministers, along with the technical proposals of the T-PD for modernising the Convention.

On 10 July 2013, at their 1176th meeting, the Ministers' Deputies took note of the work carried out by the T-PD regarding the modernisation of Convention 108 and, with a view to pursuing this work, approved the terms of reference of the CAHDATA.

The CAHDATA held three meetings, one meeting in 2013 (12 – 14 November 2013) and two more meetings in 2014 (28 – 30 April 2014 and 1-3 December 2014). At its first meeting the CAHDATA carried out an exhaustive reading of the modernisation proposals adopted by the Consultative Committee in November 2012, which enabled the production of a new working document for the second CAHDATA meeting.

---

[3] http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf
[4] Document T-PD-BUR(2011) 01 MOS rev 6
[5] Document T-PD-BUR(2011)27 of 15 November 2011
[6] Documents T-PD-BUR(2012)01Rev of 5 March 2012 , T-PD-BUR(2012)01 of 18 January 2012
[7] Documents T-PD-BUR(2012)01Rev2 of 27 April 2012and T-PD(2012)04 Rev
[8] Document T-PD(2012)04Rev2
[9] Documents T-PD(2012)11Mos and addendum.
[10] See Appendix III to the abridged report of the 29th Plenary meeting of the T-PD
[11] 29th Bureau meeting (5-7 February 2013)

During the second and third meeting the CAHDATA discussed, article by article, the modernisation proposals and introduced amendments, textual changes and adjustments. The ad hoc Committee approved the text of the modernised Convention at its 3rd meeting[12] and instructed the Secretariat to prepare the draft amending Protocol. The draft amending Protocol of Convention 108 was transmitted, together with the Explanatory report, to the Committee of Ministers for examination and adoption.
In 2016, …

Modernisation: objectives and main features

With new challenges to human rights and fundamental freedoms, notably to the right to private life, arising every day, it appeared clear that Convention 108 should be modernised in order to better address emerging privacy challenges resulting from the increasing use of new information and communication technologies, the globalisation of processing operations and the ever greater flows of personal data, and, at the same time, to strengthen the Convention's evaluation and follow-up mechanism.

It was clear from the contributions received through the 2011 public consultation and subsequent discussions in various fora, that there is broad consensus that: the general and technologically neutral nature of the Convention's provisions must be maintained; the Convention's coherence and compatibility with other legal frameworks must be preserved; and the Convention's open character, which gives it a unique potential as a universal standard, must be reaffirmed. The text of the Convention is of a general nature and can be supplemented with more detailed soft-law sectoral texts in the form notably of Committee of Ministers' Recommendations elaborated with the participation of interested stakeholders.

The modernisation of the Convention is highly topical, as with increasing globalisation of processing of personal data (flows of ubiquitous data) and associated legal uncertainty as to the applicable law, it is necessary to ensure that common core principles guarantee in as many countries as possible around the globe an appropriate level of protection of individuals with regard to the processing of personal data.

Greater harmonisation of data protection legislation around the globe can be achieved through increased accession to Convention 108.

The amendment of international treaties is governed by general treaty law, which is to a large extent embodied in the 1969 Vienna Convention on the Law of Treaties (VCLT). According to this Convention, the amendment of treaties depends on the consent of the Parties. Article 39 of the VCLT provides that "a treaty may be amended by agreement between the parties" without requiring any formality for the expression of this agreement. The modification of a treaty does not require the adoption of another treaty in written form. In its commentary to Article 39 of the VCLT, the International Law Commission stated that amendments may also be adopted by verbal or even tacit agreement. Within the context of the Council of Europe, it is usual practice to amend conventions through the adoption of amending protocols. Such protocols usually enter into force after acceptance or ratification by all the Parties to the Convention.

Convention 108 and other international frameworks

<u>Organisation for Economic Co-operation and Development (OECD) -1980</u>

The cooperation which governed the drafting of the Council of Europe's Convention and OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data was repeated during the parallel modernisation exercise and the review[13] of the 1980 Guidelines. A close liaison was maintained between the two organisations at the Secretariat level as well as at Committee level (respectively attended under observer status) with a view to maintaining consistency between the two texts.

<u>United Nations - 1990</u>

[12] 3rd CAHDATA meeting (1-3 December 2014).
[13] The revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data was adopted by the OECD Council on 11 July 2013.

Attention was duly paid to the United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990).

European Union (EU) - 1995 onwards

Recital 11 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (hereafter referred to as “Directive 95/46/EC”) reads as follows:

“*Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;*”

While the Directive drew much inspiration from Convention 108, and aimed at spelling out and expanding on the principles it enshrines, it is not identical to Convention 108. While the consistency and compatibility of both frameworks have to be preserved in the future, the general nature of the provisions of Convention 108 and the modernisation proposals can certainly continue to be given substance to and be amplified by the European Union proposed legal framework, duly taking into account the specificity of each system.

Concerning transborder data flows, both regimes should in the future be articulated in order to be compatible and complementary, aiming at ensuring the necessary protection of individuals under each regime. The fact that a State is a Party to Convention 108 is one element which can be considered when the European Union assesses the adequacy of the level of protection of a given State.

The European Union in its priorities of cooperation[14] with the Council of Europe for 2014-2015 identified data protection as one of the priority thematic areas and supported ‘the worldwide promotion of the norms of this Convention’.

Asia-Pacific Economic Cooperation (APEC) - 2004

The APEC Privacy Framework and APEC’s Cross Border Privacy Rules (CBPRs) system were considered when reflecting on the need to increase cooperation among regions and systems, in particular with regard to international enforcement and transborder data tranfers.

Other instruments

Finally, attention was also paid to the ”International Standards on the Protection of Privacy with regard to the processing of Personal Data” endorsed by the International Conference of Data Protection and Privacy Commissioners (Madrid, 2009).

[14] Document ‘EU priorities for cooperation with the Council of Europe in 2014-2015’ of 7 November 2013, reference 15857/13.

II. DRAFT EXPLANATORY REPORT

1. The purpose of this [Protocol] is to modernise the provisions contained in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108) and its additional protocol on supervisory authorities and transborder flows (ETS No. 181), and to strengthen their application.

2. In the thirty years that have elapsed since Convention 108 was opened for signature, the Convention has served as the backbone for international data protection law in over 40 European countries. It has also influenced policy and legislation far beyond Europe's shores. The Council of Europe is modernising the Convention to address new data protection challenges arising in the context of technological, economic and social developments in the information and communication society, as well as of the increasing globalisation of data exchanges.

3. The explanatory reports to Convention 108 and its additional protocol remain relevant: they provide the historical context and the normative process of both instruments. Those reports should be read in conjunction with the present one for those particular aspects.

4. The modernisation work was carried out in the broader context of various parallel reforms of international data protection instruments and taking due account of the 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD), the 1990 United Nations Guidelines for the Regulation of Computerized Personal Data Files, the European Union's framework (1995 onwards), the Asia-Pacific Economic Cooperation Privacy framework (2004) and the 2009 "International Standards on the Protection of Privacy with regard to the processing of Personal Data"[15] .

5. The Consultative Committee set up by Article 18 of the Convention (T-PD) prepared the modernisation proposals which were adopted at its 29th Plenary meeting (27-30 November 2012) and submitted to the Committee of Ministers. The Committee of Minsters subsequently entrusted the CAHDATA with the task of finalising the modernisation proposals. This was completed on the occasion of the 3rd and last meeting of the CAHDATA (1-3 December 2014). Further to the finalisation of the EU data protection framework on 15 December 2015, another CAHDATA was established with a view to examine outstanding issues.

6. The text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Protocol, however, it might be of such a nature as to guide and facilitate the application of the provisions contained therein. This Protocol has been open for signature in ..., on ... .

Preamble

7. The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms.

8. A major objective of the Convention is to put individuals in a position to know, to understand and to control the processing of their personal data by others. Accordingly, the preamble expressly refers to the right to personal autonomy and the right to control one's personal data, which stems in particular from the right to privacy, as well as to the dignity of individuals. Human dignity implies that safeguards be put in place when processing personal data, in order for individuals not to be treated as mere objects or commodities. Consequently, measures and decisions which significantly affect an individual and are

[15] Welcomed by the 31st International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009.

based solely on the grounds of automated processing of data cannot be made final without the individual having the right to have his or her views taken into consideration.

9. Taking into account the role of the right to protection of personal data in society, the preamble underlines the principle that the interests, rights and fundamental freedoms of individuals have, where necessary, to be reconciled, and that the right to data protection is to be considered alongside these interests, rights and fundamental freedoms, in particular freedom of expression. A careful balance should be struck so as not to unduly restrict one of these interests, rights and fundamental freedoms. The right to 'freedom of expression' as laid down in Article 10 of the European Convention on Human Rights includes the freedom to hold opinions and to receive and impart information. Furthermore, the Convention confirms that the exercise of the right to data protection, which is not absolute, should not be used as a general means to prevent public access to official documents[16].

10. Convention 108, through the principles it lays down and the values it enshrines, protects the individual and defines an appropriate environment for the flow of information. This is important as global information flows are an important societal feature, enabling the exercise of fundamental rights and freedoms while triggering innovation and fostering social and economic progress. The flow of personal data in an information and communication society must take place in respect of the rights of individuals. Furthermore, the use of innovative technologies should respect those rights as well. This will help to build trust in innovations and new technologies and further enable their development.

11. As international cooperation between supervisory authorities is a key element for effective protection of individuals, the Convention aims to reinforce such cooperation, notably by allowing Parties to render mutual assistance, and providing the appropriate legal basis for a framework of cooperation and exchange of information for investigations and enforcement.

Chapter I – General provisions

Article 1 – Object and purpose

12. The first article describes the Convention's object and purpose. This article focuses on the subject of protection: individuals are to be protected when their personal data is processed. The right to such protection has acquired a specific meaning, starting from the case-law of the European Court of Human Rights which established that "the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8"[17]. It has been enshrined as a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union as well as in the constitutions of several Parties to the Convention. The right to the protection of personal data is not an isolated right but an enabling one, without which other rights and fundamental freedoms – such as the right to privacy, freedom of expression, freedom of association, freedom of movement and the right to a fair trial - could not be exercised and enjoyed in the same manner.

13. The guarantees set out in the Convention are extended to every individual regardless of nationality or residence. No discrimination between citizens and third country nationals in the application of these guarantees is allowed.[18] Clauses restricting data protection to a State's own nationals or legally resident foreign nationals would be incompatible with the Convention.

[16] See the Convention on Access to Official Documents (CETS 205).
[17] ECtHR MS v. Sweden 1997 para 41.
[18] See Council of Europe Commissioner on Human Rights, The rule of law on the Internet and in the wider digital world, Issue Paper, CommDH/IssuePaper(2014)1, 8 December 2014, p. 48, pt 3.3 'Everyone' without discrimination.

Article 2 – Definitions

14. The definitions used in this Convention are meant to enable the uniform application of terms to express certain fundamental concepts in national legislation.

Litt. a – 'personal data'

15. "Identifiable individual" means a person who can be directly or indirectly identified. An individual is not considered 'identifiable' if his or her identification would require unreasonable time, effort or means. Such is the case for example when identifying a data subject would require excessively complex, long and costly operations or when identifying an individual would require to breach a legal secrecy obligation sanctioned under criminal law (a doctor breaching his professional duty of secrecy to reveal the patient's name hidden behind a code in a research context).The determination of what constitutes 'unreasonable time, effort or means' should be assessed on a case by case basis, in light of the purpose of the processing and taking into account objective criteria such as the cost, the benefits of such an identification, the type of controller, the technology used, etc. Further, technological and other developments may change what constitutes 'unreasonable' time, effort or other means.

16. The notion of 'identifiable' does not only refer to the individual's civil or legal identity as such, but also to what may allow to "individualise" or single out (and thus allow to treat differently) one person from others. This "individualisation" could be done, for instance, by referring to him or her specifically, or to a device or a combination of devices (computer, mobile phone, camera, gaming devices, etc.) on the basis of an identification number, a pseudonym, biometric or genetic data, location data, an IP address, or other identifier. The use of a pseudonym or of any digital identifier/digital identity does not lead to anonymization of the data as the data subject can still be identifiable or individualized. Pseudonymous data is thus to be considered as personal data and is covered by the provisions of the Convention.

17. Data is to be considered as anonymous only as long as it is impossible to re-identify the data subject or if such re-identification would require unreasonable time, effort or means. Data that appears to be anonymous because it is not accompanied by any obvious identifying element may, nevertheless in particular cases (not requiring unreasonable time, effort or means), permit the identification of the relevant individual. This is the case, for example, where it is possible for the controller or any person to identify the individual through the combination of physical, physiological, genetic, mental, economic, cultural or social data (such as age, sex, occupation, geolocation, family status, etc.). Where this is the case, the data may not be considered anonymous and is covered by the provisions of the Convention.

18. When data is made anonymous, all means should be put in place to avoid re-identification, in particular, all technical means should be secured in order to guarantee that the individual is not or no longer identifiable . The anonymity of data should be re-evaluated regularly in light of the fast pace of technological development.

19. The notion of "data subject" also entails the idea that a person has a subjective right with regard to the data about himself or herself, even where this is processed by others.

20. While the Convention applies in principle to processing of data relating to living individuals, Parties may extend the protection to deceased natural persons and to legal persons (cf. n° 33)

Litt. b [/c] – 'data processing'

21. "Data processing" covers an open-ended general notion capable of flexible interpretation which starts from the collection or creation of personal data and covers all automated operations, whether partially or totally automated. Data processing also occurs where no automated operation is performed but data is organised in a structure which allows the controller or any other person to search, combine or correlate the data related to a specific data subject.

Litt. c [/d] – 'controller'

22. "Controller" refers to the person or body having the decision-making power concerning the processing whether this power derives from a legal designation or factual circumstances that are to be assessed on a case by case basis. In some cases, there may be multiple controllers or co-controllers (jointly responsible for a processing and possibly responsible for different aspects of that processing). The following factors are relevant to assess whether the person or body is a controller: that person or body should have control over for instance the reasons justifying the processing; the processing means and methods; the choice of data to be processed; and who is allowed to access to it. The controller remains responsible for the data involved in a processing wherever that data is located and independently of who carries out the processing operations. In this respect, persons who are not subordinated to the controller and carry out the processing on the controller's behalf, and solely according to his instructions, are to be considered processors.

23. The decision-making power of a controller can derive from the fact that processing of personal data is the main activity of the controller (e.g. an advertising company processing personal data to deliver targeted ads, etc.) or because the processing constitutes a contribution to the main activity (e.g. when establishing a database of customers or employees, processing customers' data to perform a contract, etc.).

24. Under the terms of Article 7bis on the transparency of processing, the identity and habitual residence or establishment of the controller or co-controllers as the case may be, are to be provided to the data subject.

Litt. d [/e] – 'recipient'

25. "Recipient" is an individual or an entity who receives personal data or to whom personal data is made available. A recipient may be internal (a service or a department of the controller entity) or external (a third party). Depending on the circumstances, the recipient may be a controller, a processor or the data subject himself or herself. For example, an enterprise can send employees' data to a government department that will process it as a controller for tax purposes. It can send it to a company offering storing service and acting as a processor. It can give a copy to the data subjects in order to ensure transparency or for quality check. The recipient can be a public authority but where the data received by the public authority is processed in the framework of a particular inquiry in accordance with the applicable law, that public authority shall not be regarded as a recipient.

Litt. e [/f] – 'processor'

26. "Processor" is any person (other than an employee of the data controller) who processes data on behalf and for the needs of the controller and according to his instructions. The instructions given by the controller establish the limit of what the processor is allowed to do with the personal data. A processor who does not respect those instructions is illegally processing the data.

Article 3 – Scope

27. According to *paragraph 1,* all Parties should apply the Convention to all processing - within the public or private sector alike - subject to the jurisdiction of the concerned Party. The concept of 'jurisdiction' is meant to refer to the traditional competences of the State, i.e. prescriptive, adjudicative and enforcement jurisdiction on, in principle, its territory.[19] Any data processing carried out by a public sector entity falls

[19] See Council of Europe Commissioner on Human Rights, "The rule of law on the Internet and in the wider digital world", Issue Paper, CommDH/IssuePaper(2014)1, 8 December 2014, p. 50-54, pt 3.4. "Within [a contracting state's] [territory and] jurisdiction", specially : « A state that uses its legislative and enforcement powers to capture or otherwise exercise control over personal data that are not held on its physical territory but on the territory of another state, for example, by using the physical infrastructure of the Internet and global e-communications systems to extract those data from servers, personal computers

directly within the jurisdiction of the Party, as it is the result of the Party's exercise of its jurisdiction. Processing carried out by controllers of the private sector fall within the jurisdiction of a Party when they have a sufficient connection with the territory of that Party. For instance, this could be the case where the controller is established within the territory of that Party, when activities involving data processing are performed in that territory or are related to the monitoring of a data subject's behaviour that takes place within that territory, or when the processing activities are related to the offer of services or goods to a data subject located in that territory. The Convention must be applied when the data processing is carried out within the jurisdiction of the Party, whether in the public or private sector.

28. Making the scope of the protection dependent on the notion of 'jurisdiction' of the Parties, is justified by the objective to better standing the test of time and continual technological developments, as well as the evolution of the legal concept of State jurisdiction according to international law[20] and to reinforce the commitment to individuals' protection.

29. *Paragraph 1bis* excludes processing carried out for [purely] personal or household activities from the scope of the Convention. This exclusion aims at avoiding the imposition of unreasonable obligations on data processing carried out by individuals in their private sphere for activities relating to the exercise of their private life. Personal or household activities are activities which are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others. These activities have no professional or commercial aspects and exclusively correspond to personal or household activities such as storing family or private pictures on a computer, creating a list of the contact details of friends and family members, corresponding, etc. The private sphere notably relates to a family, a restricted circle of friends or a circle which is limited in its size and based on a personal relationship or a particular relation of trust.

30. Whether activities are ['purely] personal or household activities' will depend on the circumstances. For example, when personal data is made available to a large number of persons or to persons obviously external to the private sphere, such as a public website on the Internet, the exemption will not apply. Likewise, the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, cannot be regarded as an activity which is a [purely] 'personal or household' activity. [21]

31. The Convention nonetheless applies to data processing carried out by providers of the means for processing personal data for such personal or household activities. [The Convention nonetheless applies to data processing carried out by providers of the services or products used in the context of personal or household activities]. .

32. While the Convention concerns data processing relating to individuals, the Parties may extend the protection in their domestic law to data relating to legal persons in order to protect their legitimate

---

or mobile devices in the other state, or by requiring private entities that have access to such data abroad to extract those data from the servers or devices in another country and hand them over to the state, is bringing those data – and in respect of those data, the data subjects – within its "jurisdiction" in the sense in which that term is used in the ECHR […]. » .

[20] See notably ECtHR, *Issa and Others v. Turkey*, no. 31821/96, 16 November 2004, paras. 66-71, specially 68 : "[…] the concept of 'jurisdiction' within the meaning of Article 1 of the Convention is not necessarily restricted to the national territory of the High Contracting Parties […]. In exceptional circumstances the acts of Contracting States performed outside their territory or which produce effects there ("extraterritorial act") may amount to exercise by them of their jurisdiction within the meaning of Article 1 of the Convention. »
See also the European Court of Human Rights Factsheet on "Extra-territorial jurisdiction of ECHR States Parties", December 2013, at www.echr.coe.int/Documents/FS_Extraterritorial_jurisdiction_ENG.pdf.

[21] See Court of Justice of the EU, 11 December 2014, (Frantisek) C-212/13

interests. The Convention applies to living individuals: it is not meant to apply to personal data relating to deceased persons. However, this does not prevent Parties from extending the protection to deceased persons (e.g. to address the increasing needs for protection of the reputation or interests of the deceased person and/or heirs).

Chapter II – Basic principles of data protection

Article 4 – Duties of the Parties

33. As this article indicates, the Convention obliges Parties to incorporate data protection provisions into their law. The Convention may according to the legal system concerned be self-executing, with the result that individual rights can be directly exercised independently of a prior implementation in a Party's law.

34. The term "law of the Parties" denotes, according to the legal and constitutional system of the particular country, all enforceable rules, whether of statute law or case law. It must meet the qualitative requirements of accessibility and previsibility (or 'foreseeability'). This implies that the law should be sufficiently clear to allow individuals and other entities to regulate their own behaviour in light of the expected legal consequences of their actions, and that the persons who are likely to be affected by this law should have access to it. It covers all measures, including organisational measures or instruments to be taken to implement the Convention, applying to an unlimited number of cases and an indeterminate number of persons. It encompasses rules that place obligations or confer rights on persons (whether natural or legal) or which govern the organisation, powers and responsibilities of public authorities or lay down procedure. In particular, it includes States' constitutions and all written acts of legislative authorities (laws in the formal sense) as well as all regulatory measures (decrees, regulations, orders and administrative directives) based on such laws. It also covers international conventions applicable in domestic law, including European Union law. Further, it includes all other statutes of general nature, whether of public or private law (including law of contract), together with court decisions in common law countries, or in all countries, established case law interpreting a written law. In addition, it includes any act of a professional body under powers delegated by the legislator and in accordance with its independent rule-making powers.

35. Such binding measures may be usefully reinforced by voluntary regulation measures in the field of data protection, such as codes of good practice or codes for professional conduct. However, such voluntary measures are not by themselves sufficient to ensure full compliance with the Convention.

36. Where international organisations are concerned[22], in some situations, the law of such international organisations may have a self-executing effect at the national level of the member States of such organisations.

37. The effectiveness of the application of the measures giving effect to the provisions of the Convention is of crucial importance. Beyond the specific legislative provisions, the role of the supervisory authority (or authorities), together with any remedies that are available to data subjects, should be considered in the overall assessment of the effectiveness of a Party's implementation of the Convention's provisions.

38. It is further stipulated in paragraph 2 of Article 4 that the measures giving effect to the Convention (to all the provisions of the Convention) shall be taken by the Parties concerned and shall have come into force by the time of ratification or accession, i.e. when a Party becomes legally bound by the Convention. This provision aims to enable the Convention Committee to verify whether all "necessary measures" have been taken, to ensure that the Parties to the Convention observe their commitments and provide the expected level of data protection in their national law. The process and criteria used for this check are to be clearly defined in the Convention Committee's rules of procedure.

[22] International organisations are defined as intergovernmental organisations (1986 Vienna Convention on the Law of Treaties between States and International Organisations or between International Organisations).

39. Parties commit in paragraph 3 of Article 4 to contribute actively to the evaluation of their compliance with their commitments, with a view to ensuring regular assessment of the implementation of the principles of the Convention (including its effectiveness). Regular submission of reports by the Parties on the application of their data protection law is one possible element of this active contribution.

40. The evaluation of a Party's compliance will be carried out by the Convention Committee on the basis of an objective, fair and transparent procedure established by the Convention Committee and fully described in its rules of procedure.

Article 5 – Legitimacy of data processing and quality of data

41. Paragraph 1 provides that data processing must be proportionate, that is, appropriate in relation to the legitimate purpose pursued and necessary in the sense that this purpose cannot be pursued by other appropriate and less intrusive means with regard to the interests, rights and freedoms of the data subject or of society as a whole. Such data processing should not lead to a disproportionate interference with these interests, rights and freedoms in relation to those of the controller or of the society. The principle of proportionality is to be respected at all stages of processing, including at the initial stage, i.e. when deciding whether or not to carry out the processing.

42. Paragraph 2 prescribes two alternate essential pre-requisites for a lawful processing: the individual's consent or a legitimate basis prescribed by law. Paragraphs 1, 2 and 3 of Article 5 are cumulative and must be respected in order to ensure the legitimacy of the data processing.

43. The data subject's consent must be freely given, specific, informed and [unambiguous]. The consent represents a declaration of the individual's intention: it is the free expression of an intentional choice, given either by a statement (which can be written, including by electronic means, or oral) or by a clear affirmative action and which clearly indicates in this specific context the acceptance of the proposed processing of personal data. Mere silence, inactivity or pre-validated forms or boxes should not, therefore, constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes (in the case of multiple purposes, consent should be given for each different purpose). There can be cases with different consent decisions (e.g. where the nature of the data is different even if the purpose is the same – such as health data versus location data: in such cases the data subject can consent to the processing of his or her location data but not to the processing of the health data).The data subject must be made fully aware of the implications of his or her decision (what the fact of consenting entails and the extent to which consent is given), and, to this end, have been adequately informed. No influence or pressure (which can be of an economic or other nature) whether direct or indirect, may be exercised on the data subject and consent should not be regarded as freely given where the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment (such as an increase in the price of the service where the person refuses the processing of personal data which is are not necessary for the execution of a contract).

44. An expression of consent does not waive the need to respect the basic principles for the protection of personal data set in Chapter II of the Convention and the proportionality of the processing, for instance, still has to be weighed.

45. The data subject has the right to withdraw the consent he or she gave at any time (which is to be distinguished from the separate right to object to a processing). This will not affect the lawfulness of the data processing that occurred before his or her withdrawal of consent but does not allow processing of data any more, except if another legal basis justifies it.

46. The notion of 'legitimate basis' laid down by law, referred to in paragraph 2, encompasses data processing necessary for the fulfilment of a contract (or pre-contractual measures at the request of the data subject) to which the data subject is party, data processing necessary for the protection of the vital

interests of the data subject, data processing carried out on the basis of grounds of public interest or for overriding legitimate interests of the controller.

47. Data processing carried out on grounds of public interest should be provided for by law notably for monetary, budgetary and taxation matters, public health and social security, the prevention, investigation, detection and prosecution of criminal offences and the execution of criminal penalties, the protection of national security, the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions, the enforcement of civil law claims and the protection of judicial independence and judicial proceedings . Data processing may serve both a ground of public interest and the vital interests of the data subject as, for instance, in the case of data processed for humanitarian purposes including monitoring a life-threatening epidemic and its spread or in humanitarian emergencies. This last case may occur in situations of natural disasters where processing of personal data of missing persons may be necessary for a limited time for purposes related to the emergency context – which is to be evaluated on a case-by-case basis. It can also occur in situations of armed conflicts or other violence[23].

48. The conditions for legitimate processing are set out in paragraphs 3 and 4. Personal data should be processed lawfully, fairly and in a transparent manner, and it must satisfy criteria guaranteeing its quality. Personal data must also have been collected for explicit, specified and legitimate purposes, and the processing of that particular data must serve those purposes, or at least not be incompatible with them. The reference to specified "purposes" indicates that it is not permitted to process data for undefined, imprecise or vague purposes. What is considered a legitimate purpose depends on the circumstances as the objective is to ensure that a balancing of all rights, freedoms and interests at stake is made in each instance; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society. In all cases, data processing serving an unlawful purpose cannot be considered to be based on a legitimate purpose.

49. The concept of compatible use has to be interpreted restrictively, so as not to hamper the transparency, legal certainty, predictability or fairness of the processing. In particular, personal data should not be further processed in a way that the data subject might consider unexpected, inappropriate or otherwise objectionable.

50. The further processing of personal data, referred to in paragraph 4(b), for statistical, historical or scientific purposes is *a priori* considered as compatible provided that other safeguards exist (such as, for instance, anonymisation of data or data pseudonymisation, except if retention of the identifiable form is absolutely necessary, rules of professional secrecy, provisions governing restricted access and communication of data for the above-mentioned purposes, notably in relation with statistics and public archives, other technical and organisational data-security measures) and that the operations, by definition, exclude any use of the information obtained for decisions or measures concerning a particular individual. "*Statistical purposes"* refers to the elaboration of statistical surveys or the production of statistical results. Statistics aim at analysing and characterising mass or collective phenomena in a considered population.[24] Statistical purposes can be pursued either by the public or the private sector. Processing of data for "*scientific purposes"* aims at providing researchers with information contributing to an understanding of phenomena in varied scientific fields (epidemiology, psychology, economics, sociology, linguistics, political science, criminology, etc.) in view of establishing permanent principles, laws of behaviour or patterns of

[23] Where the four Geneva Conventions of 1949, the Additional Protocols thereto of 1977, and the Statutes of the International Red Cross and Red Crescent Movement apply.

[24] Recommendation No. R (97) 18 of the Committee of Ministers to member states, 30 September 1997, concerning the protection of personal data collected and processed for statistical purposes, Appendix, point 1.

causality which transcend all the individuals to whom they apply[25]. "*Historical purposes"* includes archiving purposes in the public interest and also genealogical research.

51. Personal data undergoing processing should be adequate, relevant and not excessive. Furthermore, the data should be accurate and, where necessary, regularly kept up to date.

52. The requirement of paragraph 4(c) that data be "not excessive" first requires that data processing should be limited to the minimum necessary for the purpose for which it is processed. It shall only be processed if, and as long as, the purposes cannot be fulfilled by processing information that does not involve personal data. Furthermore, this requirement not only refers to the quantity, but also to the quality of personal data. Personal data which is adequate and relevant but would entail a disproportionate interference in the fundamental rights and freedoms at stake should be considered as excessive and not be processed. Such is the case, for instance, in the recruitment procedure for a standard administrative post where collecting HIV data from the candidates could be considered as processing relevant data (in view of the management of future absences for instance) but is actually excessive as the collection of data of this nature by the potential employer entails a disproportionate interference with the right to privacy of the candidate in comparison with the interest that such data represents for the potential employer.

53. The requirement of paragraph 4(e) concerning the time-limits for the storage of personal data means that data should be deleted once the purpose for which it was collected has been achieved or it should only be kept in a form that prevents any direct or indirect identification of the data subject.

Article 6 – Special categories of data

54. Processing of certain types of data, or processing of data for the sensitive information it reveals, may lead to encroachments on interests, rights and freedoms. This can for instance be the case where there is a potential risk of discrimination or injury to an individual's dignity or physical integrity, where the data subject's most intimate sphere, such as his or her sex life or sexual orientation, is being affected, or where processing of data could affect the presumption of innocence. It shall only be permitted where strengthened protection through appropriate safeguards, which complement the other protective provisions of the Convention, is provided for by law. .

55. In order to prevent adverse effects for the data subject, processing of sensitive data for legitimate purposes need to be accompanied with appropriate safeguards (which are adapted to the risks at stake and the interests, rights and freedoms to protect), such as, alone or cumulatively, the data subject's explicit consent, a specific law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be admitted, a professional secrecy obligation, measures following a risk analysis, a particular and qualified organisational or technical security measure (data encryption for example).

56. Specific types of data processing may entail a particular risk for data subjects independently of the context of the processing. It is, for instance, the case with the processing of genetic data, which can be left by individuals and can reveal information on the health or filiation of the person, as well as of third parties. Genetic data are all data relating to the genetic characteristics of an individual which have been either inherited or acquired during early prenatal development, as they result from an analysis of a biological sample from the individual concerned: chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained. Similar risks occur with the processing of data related to criminal offences (which includes suspected offences), criminal convictions (based on criminal law and in the framework of criminal proceedings) and related security measures (involving deprivation of

[25] Explanatory Memorandum to Recommendation No. R (97) 18 of the Committee of Ministers to member states, 30 September 1997, concerning the protection of personal data collected and processed for statistical purposes,§ 11 and 14.

liberty for instance) which require the provision of appropriate safeguards for the rights and freedoms of data subjects.

57. Processing of biometric data, that is data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification or authentication of the individual, is also considered sensitive when it is precisely used to uniquely identify the data subject.

58. The processing of photographs will not systematically be a processing of sensitive data as the photographs will only be covered by the definition of biometric data when being processed through a specific technical mean allowing the unique identification or authentication of an individual. Furthermore, where processing of images is intended to reveal racial or health information (see the following point), such a processing will be considered as a processing of sensitive data. On the contrary, processing images by a video surveillance system for security reasons in a shopping area will not be considered as processing of sensitive data.

59. Processing of sensitive data has the potential to adversely affect data subjects' rights when it is processed for specific information it reveals. While the processing of family names can in many circumstances be void of any risk for individuals (e.g. common payroll purposes), such a processing could in some cases involve sensitive data, for example when the purpose is to reveal the ethnic origin or religious beliefs of the individuals based on the linguistic origin of their names. Processing data for the information it reveals concerning health includes information concerning the past, present and future, physical or mental health of an individual, and which may refer to a person who is sick or healthy. Processing photographs of persons with thick glasses, a broken leg, burnt skin or other visible health element will not be considered as processing sensitive data as long as the health information is not extracted from the pictures and not processed as such.

60. Where sensitive data have to be processed for a statistical interest (for instance in order to have equality statistics or to obtain information about the population's health), it should be collected in such a way that the data subject is not identifiable. Collection of sensitive data without identification data is a safeguard within the meaning of Article 6 of the Convention. Where there is a legitimate need to collect sensitive data for statistical purposes in identifiable form (so that a repeat survey can be carried out, for example), appropriate safeguards should be put in place: measures to dissociate sensitive data and identification data as from the stage of collection except if not feasible, the necessity to obtain the data subject's explicit consent preceding the survey (the mere fact of providing data could not be regarded as amounting to consent) except if justified by an important public interest, and the non-publication and non-dissemination of personal data.[26]

Article 7 – Data security

61. The controller or where applicable the processor should take specific security measures, both of technical and organisational nature, for each processing, taking into account: the potential adverse consequences for the individual, the nature of the personal data, the volume of personal data processed, the degree of vulnerability of the technical architecture performing the processing, the need to restrict access to the data, requirements concerning long-term storage, and so forth.

62. Security measures should be based on the current state of the art of data security methods and techniques in the field of data processing. Their cost should be commensurate to the seriousness and probability of the potential risks. Security measures should be reviewed and regularly updated as needed.

[26] See Recommendation R (97)18 of the Committee of Ministers of the Council of Europe to member states, 30 September 1997, concerning the protection of personal data collected and processed for statistical purposes.

63. While security measures are aimed at preventing a number of risks, paragraph 2 contains a specific obligation occurring *ex post facto*, where a data breach has nevertheless occurred that may seriously interfere with the fundamental rights and freedoms of the individual. For instance, the disclosure of data covered by professional confidentiality, which may cause financial, reputational, physical harm or humiliation, could be deemed to constitute a "serious" interference.

64. Where such a data breach has occurred, the controller is requested to notify the relevant supervisory authorities of the incident. This is the minimum requirement. The controller should also notify the supervisory authorities of any measures taken and/or proposed to address the breach and its potential consequences.

65. The notification made by the controller to the supervisory authorities should not preclude other complementary notifications. For instance, the controller should be encouraged to notify the data subjects in particular when the data breach is likely to result in a significant risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, and to provide them with adequate and meaningful information on, notably, the contact points and possible measures that they could take to mitigate the adverse effects of the breach. If the controller does not spontaneously inform the data subject of the data breach, the supervisory authority, having considered the likely adverse effects of the breach, should be allowed to require the controller to do so. Notification to other relevant authorities such as those in charge of computer systems security may also be required.

Article 7bis – Transparency of processing

66. The controller is required to be transparent when processing data in order to secure fair processing and to enable data subjects to understand and thus fully exercise their rights in the context of such data processing.

67. Certain minimum information has to be compulsorily provided by the controller to the data subjects when directly or indirectly (not through the data subject) collecting their data. While the transparency requirements are compulsory, information on the name and address of the controller, the legal basis and the purposes of the data processing, the categories of data processed and recipients (be them obvious or not), as well as the means of exercising the rights can be rendered in any appropriate format (either through a website, technological tools on personal devices, etc.) provided that it is fairly and effectively presented to the data subject. The information presented should be easily accessible, legible, understandable and adapted to the relevant data subjects (in a child friendly language where necessary for instance). Any additional information that is necessary to ensure fair data processing, such as the preservation period, the logic underpinning the data processing, or information on data transfers to a foreign country (including whether that particular country provides an appropriate level of protection and the measures taken by the controller to guarantee such an appropriate level of data protection) shall also be provided.

68. The controller is not required to provide this information where the data subject has already received it and the controller can prove it, or in the case of an indirect collection of data through third parties where it is expressly prescribed by a precise and well detailed law, or where this proves to be impossible or it involves disproportionate efforts because the data subject is not directly identifiable or the controller has no way to contact the data subject. Such impossibility can be both of a legal nature (in the context of a criminal investigation or when the persons who hold the necessary information are bound by professional secrecy for instance) or of a practical nature (for instance when a controller is only processing pictures and does not know the names and contact details of the data subjects).

69. When such impossibility is of a practical nature, the data controller shall nonetheless use any available, reasonable and affordable means to inform data subjects in general or individually. It can be done at a later stage, for instance when the controller is put in contact with the data subject for any new reason.

Article 8 – Rights of the data subject

70. The provisions set out in this Article list a set of rights that every individual should be able to exercise and defend concerning the processing of personal data relating to him or her.

71. These rights include the following main elements which are essential tools for the data subject:
– the right not to be submitted to a purely automated decision without having one's views taken into consideration (littera a) ;
– the right to be informed about the existence of a processing relating to him or her and to access the data (littera b);
– the right to be informed about the reasoning on which the processing is based (littera c);
– the right to object to a processing of personal data relating to him or her (littera d);
– the right to rectification or erasure of inaccurate, false, or generally, unlawfully processed data (littera e);
– the right to a remedy if any of the previous rights is not respected (littera f);
– the right to obtain assistance from a supervisory authority (littera g).

72. Those rights may have to be reconciled with other rights and legitimate interests. They can, in accordance with Article 9, be limited only where this constitutes a necessary and proportionate measure in a democratic society. For instance, the right to be informed about the reasoning on which the processing is based may be limited in order to protect the rights of others, such as "legally protected secrets" (e.g. trade secrets).

73. The Convention does not specify from whom a data subject may obtain confirmation, communication, rectification, etc., or to whom to object or express his or her views. In most cases, this will be the controller, or the processor on his or her behalf. But, in exceptional cases laid down in Article 9 (national security for instance), the rights to access, rectification and erasure can be exercised through the intermediary of the supervisory authority. Concerning health data, rights may also be exercised in a different manner than through direct access. They may be exercised for instance with the assistance of a health professional when it is in the interest of the data subject, notably to help him/her understand the data or ensure that the data subject's psychological state is appropriately considered when imparting information – in line, of course, with deontological principles.

74. *Littera a.* It is essential that an individual who may be subject to a purely automated decision has the right to challenge such a decision by putting forward, in a meaningful manner, his or her point of view and arguments. In particular, the data subject should have the opportunity to substantiate the possible inaccuracy of the personal data before it is used, the irrelevance of the profile to be applied to his or her particular situation, or other factors that will have an impact on the result of the automated decision. This is notably the case where individuals are stigmatised [as potentially guilty of fiscal or social fraud] by application of algorithmic reasoning [or where they see their credit capacity evaluated by a software].

75. *Littera b.* Data subjects should be entitled to know about the processing of their personal data. While the right of access should, in principle, be free of charge, the wording of *littera b.* is intended to allow the controller to charge a reasonable fee where the requests are excessive and to cover various formulas that could be adopted by a Party for appropriate cases: communication of the data free of charge but with a minimum interval between two communications, or communication for a lump sum fee taking into account the administrative actual costs of responding to the request. Such a fee should be exceptional and in any case reasonable, and not prevent or dissuade data subjects from exercising their rights. The controller

could also refuse to respond to manifestly unfounded or excessive requests. To ensure a fair exercise of the right of access, the communication “in an intelligible form” applies to the content as well as to the form of a standardised digital communication.

76. *Littera c.* Data subjects should be entitled to know the reasoning underlying the processing of their data, be it automated or not, including the consequences of such a reasoning, which led to any resulting conclusions. For instance in the case of credit scoring, they should be entitled to know the logic underpinning the processing of their data and resulting in a ‘yes’ or ‘no’ decision, and not simply information on the decision itself. Without an understanding of these elements there could be no effective exercise of other essential safeguards such as the right to object and the right to complain to a competent authority.

77. *Littera d.* As regards the right to object, the controller may have a legitimate ground for data processing, which overrides the interests or rights and freedoms of the data subject. The establishment, exercise or defence of legal claims could be considered as overriding legitimate grounds justifying the continuation of the processing. This will have to be demonstrated on a case-by-case basis and failure to demonstrate such compelling legitimate grounds while pursuing the processing could be considered as unlawful.

78. Objection to data processing for marketing purposes should lead to unconditional erasing or removing of the personal data covered by the objection.

79. The right to object may be limited by virtue of a law, for example, for the purpose of the investigation or prosecution of criminal offences. When data processing is based on a valid consent given by the data subject, the right to object gives way to the right to withdraw consent. Anyone may withdraw his or her consent provided that he or she assumes the consequences possibly deriving from other legal texts such as the obligation to compensate the controller.

80. *Littera e.* The rectification or erasure, if justified, must be free of charge. In the case of rectifications and deletions obtained in conformity with the principle set out in *littera e*, those rectifications and deletions should, where possible, be brought to the attention of the recipients of the original information, unless this proves to be impossible or involves disproportionate efforts.

81. *Littera g* aims at ensuring effective protection of individuals by providing them the right to an assistance of a supervisory authority in exercising the rights provided by the Convention. When the individual resides in the territory of another Party, he or she should be given the option of submitting the request through the intermediary of the authority designated by that Party. The request for assistance should contain all the necessary particulars, relating inter alia to: the name, address and any other relevant details identifying the individual making the request; the data processing to which the request pertains, or its controller; the purpose of the request, the elements in the possession of the applicant which allow determination of the data processing in question. This right can be limited according to Article 9 of the Convention or adapted in order to safeguard the interests of a pending judicial procedure.

82. Furthermore, it should be noted that the specification of the purpose, the conditions for the legitimacy of the processing, the requirements as regards the data quality, the right of rectification or erasure, together with the provision on the length of time for data storage (article 5.4. *littera e*.), coupled with an effective right to object and the right to withdraw consent, offer an effective level of protection for the data subject. This set of rights and requirements pragmatically corresponds to the effect of what is referred to as a ‘right to be forgotten’.

Article 8bis - Additional obligations

83. In order to ensure that the right to the protection of personal data is effective, additional obligations have to be placed on the controller as well as, where applicable, the processor(s).

84. According to *paragraph 1*, the obligation on the controller to ensure adequate data protection is linked to the responsibility to verify and demonstrate that data processing is in compliance with the applicable law. The data protection principles set out in the Convention, which are to be applied at all stages of processing, including the design phase, are also a mechanism for enhancing trust. Notably, the controller and processor will have to take appropriate measures, such as: training employees; setting-up appropriate notification procedures (for instance to indicate when data have to be deleted from the system); establishing specific contractual provisions where the processing is delegated, to give effect to the Convention; as well as setting up internal procedures to enable the verification and demonstration of compliance.

85. A possible measure that could be taken by the controller to facilitate such a verification and demonstration of compliance would be the designation of a 'data protection officer' entrusted with the means necessary to fulfil his or her mission independently. Such a data protection officer, whose designation should be notified to the supervisory authority, could be internal or external to the controller.

86. *Paragraph 2* clarifies that before carrying out a data processing, the controller will have to examine its potential impact on the rights and fundamental freedoms of the data subjects. This examination can be informally done and does not necessarily involve a full and formal data protection impact and risks assessment. It will also have to consider the respect of the proportionality principle, on the basis of a comprehensive overview of the processing taking into account the nature of the data, the scope, context and purposes of the processing as well as the likelihood and severity of the risks for the rights and freedoms of individuals. In some circumstances, where a processor is involved in addition to the controller, the obligation to examine the risks may also be imposed on the processor and the determination of the existence of such an obligation will be made taking into account the comprehensive overview of the processing. The assistance of IT systems developers, including security professionals, or designers, together with users and legal experts, in examining the risks would be an advantage and could reduce the burdens linked to this exercise.

87. *Paragraph 3* specifies that in order to better guarantee an effective level of protection, controllers, and, where applicable, processors, should ensure that data protection requirements are integrated as early as possible – i.e. ideally at the stage of architecture and system design – in data processing operations through technical and organisational measures (data protection by design). This implementation of data protection requirements should be achieved not only as regards the technology used for processing the data, but also the related work and management processes. Easy-to-use functionalities that facilitate compliance with applicable law should be put in place. For example, secure online access to one's own data should be offered to data subjects where possible and relevant. There should also be easy-to-use tools for data subjects to take their data to another provider of their choice or keep the data themselves (data portability tools). When setting up the technical requirements for default settings, controllers and processors should choose privacy-friendly standard configurations so that the usage of applications and software does not infringe individuals' right to personal data protection, notably the principle of data minimisation (data protection by default). For example, social networks should be configured by default so as to share posts or pictures only with restricted and chosen circles and not with the whole Internet.

88. *Paragraph 4* allows Parties to scale and to adapt the additional obligations listed in paragraphs 1 to 3 taking into consideration the risks at stake for the interests, rights and fundamental freedoms of the data subjects. Such adaptation should be done considering the nature and volume of data processed, the nature, scope and purposes of the data processing and, in certain cases, the size of the processing entity. The obligations could be scaled, for example, so as not to entail excessive costs for SMEs processing only non-sensitive personal data received from customers in the framework of commercial activities and not re-using or re-selling it for other purposes. Certain categories of data processing, such as processing which does not entail any risk for individuals, may even be exempt from some of the additional obligations prescribed in this Article.

Article 9 – Exceptions and restrictions

89. Exceptions to the principles for protection of personal data are allowed in a strictly restrictive manner, for a limited number of provisions when such exceptions are provided for by law and are necessary in a democratic society for the specific grounds exhaustively listed in *litterae a.* and *b*. of the first paragraph of Article 9. A measure which is "necessary in a democratic society" must pursue a legitimate aim and thus meet a pressing social need which cannot be achieved by less intrusive means. Such a measure should furthermore be proportionate to the legitimate aim being pursued and the reasons adduced by the national authorities to justify it should be relevant and sufficient. Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed.

90. The necessity of such measures needs to be examined on a case-by-case basis and in light of limited legitimate aims only, as is detailed in litterae a and b of the first paragraph. Littera a lists the major interests of the State or of the international organisation which may require exceptions. These exceptions are very specific to avoid giving Parties unduly wide leeway with regard to the general application of the Convention.

91. The notion of "national security" should be restrictively understood in the sense of protecting the national sovereignty of the concerned Party against internal or external threats, including the protection of the international relations of the Party, and interpreted on the basis of the relevant case-law of the European Court of Human Rights which includes in particular the protection of state security and constitutional democracy from espionage, terrorism, support for terrorism and separatism. Where national security is at stake, safeguards against unfettered power must be provided.[27] Any measure affecting human rights must be subject to a form of adversarial proceedings before an independent body competent to review the reasons for the decision and relevant evidence.[28] The individual must be able to challenge the executive's assertion that national security is at stake[29]. Everyone affected by a measure based on national security grounds has to be guaranteed protection against arbitrariness[30]. The long-term storage of information in security files must be supported by reasons relevant and sufficient with regard to the protection of national security[31].

92. The term "important economic and financial interests" should be read restrictively and covers, in particular, tax collection requirements and exchange control. The term "prevention, investigation and suppression of criminal offences" in this *littera* includes the prosecution of criminal offences.

93. *Littera b*. concerns major interests of private parties, such as those of the data subject himself or herself (for example when a data subject's vital interests are threatened because he or she is missing) or of third parties, such as freedom of expression, including freedom of academic, artistic or literary expression, and the right to receive and impart information, confidentiality of correspondence and communications, or else business or commercial secrecy and other legally protected secrets.

94. The third paragraph leaves open the possibility of restricting the rights with regard to certain data processing carried out for historical, statistical or scientific purposes which pose no identifiable risk to the protection of personal data and where restrictions to the data subject's rights are justified. For instance, the use of data for statistical work, in the public and private fields alike, in so far as this data is published in aggregate form and having all their identifiers stripped enters into that hypothesis provided that appropriate data protection safeguards are in place (see paragraph 51).

---

[27] See European Court of Human Rights Research Division, « National security and European case-law », November 2013, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/judgments_EN.asp?

[28] ECtHR, Klass and Others v. Germany, 6 September 1978, série A, no 28 ; ECtHR, Al-Nashif v. Bulgaria, no 50963/99, 20 June 2002.

[29] ECtHR, Al-Nashif v. Bulgaria, no 50963/99, 20 June 2002.

[30] ECtHR, Dalea v. France (dec.), 964/07, 2 February 2010.

[31] ECtHR, Segerstedt-Wiberg and Others v. Sweden, no. 62332/00, ECHR 2006-VII.

Article 10 – Sanctions and remedies

95. In order for the Convention to guarantee an effective level of data protection, the duties of the controller and processor and the rights of data subjects should be reflected in the Parties' legislation with corresponding sanctions and remedies.

96. It is left to each Party to determine the nature (civil, administrative, criminal) of these judicial as well as non-judicial sanctions. These sanctions have to be effective, proportionate and dissuasive. The same goes for remedies: individuals must have the possibility to challenge in courts a decision or practice, the definition of the modalities to do so being left with the Parties. Non-judicial remedies have also to be open to unsatisfied data subjects. Financial compensation for all damages, including moral ones, caused by the processing and class actions could be considered too.

Article 11 – Extended protection

97. This article has been based on a similar provision, Article 60, of the European Convention on Human Rights. The Convention confirms the principles of data protection law which all Parties are ready to adopt. The text emphasises that these principles constitute only a basis on which Parties may build a more advanced system of protection.

Chapter III – Transborder flows of personal data

Article 12 – Transborder flows

98. The aim of this article is to facilitate the free flow of information regardless of frontiers (recalled in the Preamble), while ensuring an appropriate protection of individuals with regard to the processing of personal data.

99. The purpose of the transborder flow regime is to ensure that personal data originally processed within the jurisdiction of a Party (data collected or stored there for instance), which then subsequently appears to be submitted to the jurisdiction of a State which is not Party to the Convention, continues to be processed in line with data protection principles that are appropriate with regard to the Convention. What is important is that data subjects originally concerned by the data processed within the jurisdiction of a Party always remain protected by appropriate data protection principles no matter the particular law applicable to the processing at stake. While there may be a wide variety of systems of protection, protection afforded has to be of such quality as to ensure that human rights are not affected by globalisation and transborder data flows.

100. Most of the time, such a situation – a change of jurisdiction and applicable law – occurs when there is a data transfer from a State Party to the Convention to a foreign country. A data transfer occurs when personal data is disclosed or made available with the knowledge of the sender, to a recipient subject to the jurisdiction of another State or international organisation.

101. Article 12 only applies only to the outflow of data, not to its inflow, as for the latter, data are covered by the data protection regime of the recipient Party.

102. *Paragraph 1* applies to data flows between Parties to the Convention. This cannot be prohibited or subject to special authorisation, with the exception of flows of personal data relating to Parties regulated by binding harmonised rules of protection shared by States belonging to a regional organisation. This is the case of member States of the European Union. They are bound by rules adopted at the Union level that apply to transborder data flows. The rationale of this provision is that all Contracting States, having

subscribed to the common core of data protection provisions set out in the Convention, offer a level of protection considered appropriate. In the absence of additional regional binding harmonised rules governing data flows, personal data flows between Parties should operate freely.

103. This rule does not mean that a Party may not take certain measures to keep itself informed of data traffic between its territory and that of another Party, for example by means of declarations to be submitted by controllers. However, such measures cannot be used as a means for a Party to gain access to the personal data of individuals under its jurisdiction.

104. In some cases, personal data flows will be made from a Party simultaneously to several foreign States or international organisations, some of which are Parties to the Convention and some of which are not. In those cases, the Party transferring the data, which has export procedures for non-Parties, may not be able to avoid applying those procedures also to the data destined for a Party, but it should proceed in such a way as to ensure that these procedures are not an obstacle to data transfers to the latter Party.

105. *Paragraph 2* regulates transborder flows of personal data to a recipient that is not subject to the jurisdiction of a Party. As for any personal data flowing outside national frontiers, an appropriate level of protection in the recipient State or organisation is to be guaranteed. As this cannot be presumed since the recipient is not a Party, the Convention establishes two main means to ensure that the level of data protection is indeed appropriate; either by law, or by ad hoc or approved standardised safeguards that are legally binding and enforceable, as well as duly implemented.

106. Both *paragraphs 2 and 3* apply to all forms of appropriate protection, whether provided by law or by standardised safeguards. The law must include the relevant elements of data protection as set forth by this Convention. The level of protection should be assessed on a case-by-case basis for each transfer or category of transfers. Various elements of the transfer should be examined such as: the type of data; the purposes and duration of processing for which the data are transferred; the respect of the rule of law by the country of final destination; the general and sectoral legal rules applicable in the State or organisation in question; and the professional and security rules which apply there.

107. The content of the ad hoc or standardised safeguards must include the relevant elements of data protection. Moreover, the contractual terms could be such, for example, that the data subject is provided with a contact person on the staff of the person responsible for the data flows, whose responsibility it is to ensure compliance with the substantive standards of protection. The data subject would be free to contact this person at any time and at no cost in relation to the data processing or flows and, where applicable, obtain assistance in exercising his or her rights.

108. The assessment as to whether the level of protection is appropriate must take into account the principles of the Convention, the extent to which they are met in the recipient State or organisation – in so far as they are relevant for the specific case of transfer – and how the data subject is able to defend his or her interests where there is non-compliance. The enforceability of data subjects' rights and the provision of effective administrative and judicial redress for the data subjects whose personal data are being transferred should be taken into consideration in the assessment. Similarly, the assessment can be made for a whole State or organisation thereby permitting all data transfers to these destinations. The appropriate level of protection is determined by the competent supervisory authority of each Party.

109. *Paragraph 4* enables Parties to derogate, in a particular case, from the principle of requiring an appropriate level of protection and to allow a specific transfer to a recipient which does not ensure such protection. Such derogations are permitted in limited situations only: with the data subject's consent or specific interest and/or where there are prevailing legitimate interests provided by law. The prevailing legitimate interests are not those of the recipient State. Such derogations should respect the proportionality principle and should not be used for massive or repetitive data transfers. Where massive or repetitive data transfers are involved, provisions of article 12.3 should apply and adequate safeguards should be put in place.

110. *Paragraph 5* contemplates a complementary safeguard: namely that the competent supervisory authority be provided with all relevant information concerning the transfers of data referred to in paragraphs 3.b, such as transfers accompanied by ad hoc or approved standardised safeguards. In particular, the authority will be informed of the procedures of the transfers and of the content of the legally binding instruments providing the safeguards. Transfers corresponding to situations where no appropriate level of protection is secured but the specific interests of the data subject (paragraphs 4.b.) or prevailing legitimate interests (paragraph 4.c.) justify them, should also be subject to the competent supervisory authority's oversight. The authority should be entitled to require relevant information about the circumstances and justification of those transfers.

111. *According to paragraph 6,* the supervisory authority should be entitled to request that the effectiveness of the measures taken or the existence of prevailing legitimate interests be demonstrated, and to prohibit, suspend or impose conditions on the transfer if this proves necessary to protect the rights and fundamental freedoms of the data subjects. .

112. In respect of transborder flows of personal data, a specific exemption is allowed in view of protecting freedom of expression, including freedom of the press. Parties may allow exceptions to the provisions of this Article 12 on the condition that these exceptions are provided for by law and are necessary in a democratic society to protect the freedom of expression. A measure which is "necessary in a democratic society" must pursue a legitimate aim and thus meet a pressing social need which cannot be achieved by less intrusive means. Such a measure should be proportionate to the legitimate aim being pursued and the reasons adduced by the national authorities to justify it should be relevant and sufficient. Such a measure must be prescribed by an accessible and foreseeable law, which must be sufficiently detailed.

113. Data flows and the related need to increase the protection of personal data also require an increase in international enforcement cooperation among competent supervisory authorities.

Chapter III bis – Supervisory authorities
Article 12bis – Supervisory authorities

114. The effective application of the principles of the Convention necessitates the adoption of appropriate sanctions and remedies (Article 10). Most countries which have data protection laws have set up supervisory authorities to deal with evolving and complex personal data processing in light of organisational, social and societal evolutions. This context requires an external, independent and impartial entity, with fast reactive powers and specialised expertise. Such authorities may be a single commissioner or a collegiate body. In order for data protection supervisory authorities to be able to provide for an appropriate remedy, they need to have effective powers and functions and enjoy genuine independence in the fulfilment of their duties. They are an essential component of the data protection supervisory system in a democratic society.

115. This Article of the Convention aims at enforcing the effective protection of the individual by requiring the Parties to create one or more supervisory authorities that contribute to the protection of the individual's rights and freedoms with regard to the processing of personal data. Paragraph 1 clarifies that more than one authority might be needed to meet the particular circumstances of different legal systems (e.g. federal States). Specific supervisory authorities whose activity is limited to a specific sector (electronic communications sector, health sector, public sector, etc.) may also be put in place. These authorities may exercise their tasks without prejudice to the competence of legal or other bodies responsible for ensuring respect of the law giving effect to the principles of the Convention. The supervisory authorities should have the necessary infrastructure and financial, technical and human resources (lawyers, information and

communication technologies' specialists) to take prompt and effective action. These resources should be regularly assessed in the light of possible increasing of powers and duties.

116. Parties have certain discretion as to how to set up the authorities for enabling them to carry out their task. According to paragraph 2, however, they must have at least the powers of investigation and intervention and the powers to issue decisions and impose administrative sanctions to public authorities or to private sector actors. Furthermore, they must be consulted in the legislative and administrative normative processes relating to data protection, have specific powers in the context of data flows (notably the approval of standardised safeguards), have the power to hear individuals' complaints, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities any violations of the relevant provisions, and finally the mandate to raise awareness on data protection.

117. The authority shall be endowed with powers of investigation, such as the possibility to ask the controller and processor for information concerning the processing of personal data and to obtain it. By virtue of Article 8 of the Convention, such information should be made available, in particular, when the supervisory authority is approached by a person wishing to exercise the rights provided for in Article 8.

118. The supervisory authority's power of intervention provided for in paragraph 1, may take various forms in the Parties' law. For example, the authority could be empowered to oblige the controller to rectify, delete or destroy inaccurate or illegally collected data on its own account or if the data subject is not able to exercise these rights personally. The power to seek mandatory injunctions against controllers who are unwilling to communicate the required information within a reasonable time would also be a particularly effective demonstration of the power of intervention. This power could also include the possibility to issue opinions prior to the implementation of data processing operations (where processing present particular risks to the rights and fundamental freedoms, the supervisory authority should be consulted by controllers from the earliest stage of design of the processes), or to refer cases to national parliaments or other state institutions.

119. Moreover, according to paragraph 3 every individual should have the possibility to request the supervisory authority to investigate a claim concerning his or her rights and liberties in respect of personal data processing. This helps to guarantee the right to an appropriate remedy, in keeping with Article 10 and Article 8 of the Convention. Further to such investigations, paragraphs 2(c) and 2(d) uphold that the supervisory authorities may, in particular, decide to impose an administrative sanction, or refer the offence to a competent judicial authority by bringing the case to its attention or engaging in legal proceedings (see the following paragraph). In some jurisdictions, supervisory authorities may not have standing to engage in legal proceedings. Therefore, the power to impose administrative sanctions is very important for their enforcement capacities. Since such powers are given to the supervisory authorities, the necessary resources to fulfil this duty should be provided. According to their available resources, the supervisory authorities should be given the possibility to define priorities to deal with the requests and complaints lodged by data subjects.

120. The Parties should give to the supervisory authority the power either to engage in legal proceedings or to bring any violations of data protection rules to the attention of the judicial authorities as provided for in paragraphs 2(c) and 2(d). This power derives from the power to carry out investigations, which may lead the authority to discover an infringement of an individual's right to protection. The Parties may fulfil the obligation to grant this power to the authority by enabling it to make decisions.

121. Where an administrative decision produces legal effects, every affected person has a right to have an effective judicial remedy. However, a Party's law may provide for the lodging of a claim with the supervisory authority as a condition of this judicial remedy.

122. Paragraph 2(e) deals with the awareness raising role of the supervisory authorities. Whilst contributing to the protection of individual rights, the supervisory authority also acts as an intermediary between the data subject and the controller. In this context, it seems particularly important that the

supervisory authority proactively ensures the visibility of its activities, functions and powers. To this end, the supervisory authority must inform the public through periodical reports (see paragraph 129), It may also publish opinions or use any other means of communication and issue public recommendations to the head of State, government and Parliament in order to improve the data protection system. Moreover, it must provide information to individuals and to data controllers and processors about their rights and obligations concerning data protection. While raising awareness on data protection issues, the authorities have to be attentive to specifically address children and vulnerable categories of persons through adapted ways and languages.

123. As provided for under paragraph 2bis, supervisory authorities must be entitled to give opinions on any legislative or administrative measures which provide for the processing of personal data. Only general measures are meant by this consultative power, not individual measures.

124. In addition to this consultation foreseen under paragraph 2bis, the authority could also be asked to give its opinion when other measures concerning personal data processing are in preparation, such as for instance codes of conduct or technical norms.

125. A supervisory authority's competences are not limited to the ones listed in Article 12bis. An authority may find it appropriate to issue general recommendations concerning the correct implementation of data protection rules. It can consult stakeholders. Supervisory authorities could keep a data processing register open to the public. It should finally be borne in mind that the Parties have other means of making the task of the supervisory authority effective. For example, it could be possible for associations to lodge complaints with the authority, in particular when the rights of the persons that it represents are restricted in accordance with Article 9 of the Convention.

126. Paragraph 4 clarifies that supervisory authorities cannot effectively safeguard individual rights and freedoms unless they exercise their functions in complete independence. A number of elements contribute to safeguarding the independence of the supervisory authority in the exercise of its functions. These should include: the composition of the authority; the method for appointing its members; the possibility for them to participate in meetings without any authorisation or instruction; the option to consult technical or other experts or to hold external consultations; the duration of exercise and conditions of cessation of their functions; the allocation of sufficient resources to the authority; the possibility to hire its own staff according to internal rules; or the adoption of decisions without being subject to external orders or injunctions.

127. The prohibition of seeking or accepting instructions covers the performance of the duties as a supervisory authority. This does not prevent supervisory authorities from seeking specialised advice (for instance from psychologists, information and communication technologies' specialists, other consultants and counterparts, etc.) where it is deemed necessary as long as the supervisory authorities exercise their own independent judgment.

128. Transparency on the work and activities of the supervisory authorities is required; through, for instance, the publication of annual activity reports comprising inter alia information related to their enforcement actions as set out under paragraph 5bis.

129. As a counterpart to this independence it must be possible to appeal against the decisions of the supervisory authorities through the courts in accordance with the principle of the rule of law, as provided for under paragraph 6.

130. Moreover, while supervisory authorities should have the legal capacity to act in court and seek enforcement, the intervention (or lack of) of a supervisory authority shall not prevent an affected individual from seeking a judicial remedy.

131. Paragraph 7 is the first out of three sets of provisions of the Convention dealing with the co-operation between Parties, through their various authorities, in giving effect to the data protection laws implemented pursuant to the Convention (the others being Arts 13-17 on mutual assistance and Arts 18-20 on the Convention Committee). The Convention distinguishes between two levels of co-operation: (1) between *Parties*, on behalf of whom any designated authority can act, and (2) between *supervisory authorities*. The present provision deals with the latter, while the subsequent provisions address the former.

132. The necessity to co-operate between Parties, thus between various jurisdictions, is predominantly imposed by globalisation and the rapid developments in technology, which both have given rise to ubiquitous transfers of personal data across jurisdictions, thus elevating various risks for the individuals, and requiring coordinated and rapid reaction. The Convention not only aims at *adequately* responding to this necessity, but also at offering means for co-operation that achieves *efficiency*. To that end, it offers a variety of possibilities through the above-mentioned three sets of provisions.

133. The notion of co-operation is not of a uniform nature and varies from some 'hard' forms, such as enforcement of data protection laws, in which the legality of action of each supervisory authority is indispensable, to some 'soft' forms, such as awareness-raising, training, staff exchange (cf. "joint actions" in Art 12bis(7)(b)).

134. Supervisory authorities are both empowered and obliged to exercise all their duties and powers listed in Art 12bis(2) whenever there is an extraterritorial element at stake. This could include a situation of individual complaint against a data controller/processor processing personal data in more than one jurisdiction.

135. The catalogue of possible co-operation activities is not exhaustive. In the first place, supervisory authorities shall provide each other mutual assistance, especially by providing any relevant and useful information. This information could be of a twofold nature: (1) "information and documentation on their law and administrative practice relating to data protection", which normally does not raise any issues, i.e. such information could be exchanged freely and further made publicly available, and (2) confidential or otherwise privileged information, such as state or trade secrets as well as personal data.

136. As far as personal data is concerned, it can be exchanged only if: (1) its provision is essential for the co-operation, i.e. if without its provision the co-operation would be rendered ineffective or (2) the "data subject concerned has given explicit, specific, free and informed consent". In any case, the transfer of personal data cannot contradict the provisions of the Convention, and in particular Chapter II. (Cf. also Art 16(b) providing for the grounds for refusal.)

137. Further to the provision of relevant and useful information, the goals of co-operation can be achieved by coordinated investigations or interventions as well as joint actions. For the applicable procedures, supervisory authorities shall refer to their enabling legislation at national level, e.g. codes of administrative, civil or criminal procedure, or supra or international commitments their jurisdictions are bound by, e.g. mutual legal assistance treaties, having assessed their legal capacity to enter into a co-operation of that type.

138. The provisions on mutual assistance among supervisory authorities shall be read in conjunction with the provisions of Arts 13-17, as these provisions would apply *mutatis mutandis*.

139. Paragraph 8 refers to a network of supervisory authorities, as a means to contribute to the rationalisation of the co-operation process and thus to the efficiency of the protection of personal data. It is important to note that the Convention refers to "a network" in singular form. This seems not to prohibit supervisory authorities originating from the Parties to take part in other relevant networks.

140. In order to safeguard the independence of judges in the performance of their judicial tasks, paragraph 9 of Article 12bis states that supervisory authorities shall not be competent with respect to processing carried out by bodies when acting in their judicial capacity. Such exemption from supervisory

powers should be strictly limited to genuine judicial activities in court cases and not apply to other activities where judges might be involved in, in accordance with national law.

Chapter IV – Mutual assistance

Article 13 – Co-operation between Parties

141. Chapter IV (Arts 13-17) forms a second set of provisions on co-operation between Parties, through their various authorities, in giving effect to the data protection laws implemented pursuant to the Convention (*cf*. para **Error! Reference source not found.**). Mutual assistance is obligatory. To that end, the Parties shall designate one or more authorities and communicate their contact details, as well as their substantive and territorial competences, if applicable, to the Secretary General of the Council of Europe. Subsequent articles provide for a detailed framework for mutual assistance.

142. While the co-operation between Parties will generally be carried out by the supervisory authorities established under Article 12bis of the Convention, it cannot be excluded that a Party designates another authority to give effect to the provisions of Article 13.

143. Article 16(b) enables an authority to refuse a request of assistance if it "does not comply with the provisions of this Convention", and here in particular Chapter II is meant to be complied with.

144. The co-operation and general assistance is relevant for controls *a priori* as well as for controls *a posteriori* (for example to verify the activities of a specific data controller). The information exchanged may be of a legal or factual character.

Article 14 – Assistance to data subjects

145. Paragraph 1 ensures that data subjects, whether in a Party to the Convention or in a third country will be enabled to exercise their rights recognised in article 8 of the Convention regardless of their place of residence or their nationality.

146. According to paragraph 2, where the data subject resides in another Contracting State he or she is given the option to pursue his or her rights either directly in the country where information relating to the data subject concerned is processed, or indirectly, through the intermediary of that country's designated authority.

147. Moreover, it goes without saying that data subjects residing abroad always have the opportunity to pursue their rights with the assistance of the diplomatic or consular agents of their own country.

148. Paragraph 3 specifies that requests be as specific as possible in order to expedite the procedure.

Article 15 – Safeguards concerning assistance

149. This article ensures that supervisory authorities shall be bound by the same obligation to observe discretion and confidentiality toward foreign data protection authorities and persons residing abroad, as they have to observe in their own country.

150. Assistance from a supervisory authority on behalf of a data subject may only be given in response to a request from this data subject. The authority must have received a mandate from the data subject and may not act autonomously in his or her name. This provision is of fundamental importance for mutual trust, on which mutual assistance is based.

Article 16 – Refusal of requests for assistance

151. This article states that Parties are bound to comply with requests for assistance. The grounds for refusal to comply are enumerated exhaustively. They correspond generally with those provided for by other international treaties in the field of mutual assistance.

152. The term "compliance" which is used in littera c should be understood in the broader sense as covering not only the reply to the request, but also the action preceding it. For example, a requested authority might refuse action not only if transmission to the requesting authority of the information asked for might be harmful for the rights and fundamental freedoms of an individual, but also if the very fact of seeking the information might prejudice his or her rights and fundamental freedoms.

Article 17 – Costs and procedures of assistance

153. The provisions of this Article are analogous to those found in other international conventions on mutual assistance.

154. "Experts" in the sense of paragraph 1 covers data processing experts whose intervention is required to make test runs or check the data security of a processing.

155. With a view to not burdening the Convention with a mass of implementing details, paragraph 3 of this Article provides that procedure, forms and language to be used can be agreed between the Parties concerned. The text of this paragraph does not require any formal procedures, but allows for administrative arrangements, which may even be confined to specific cases. Moreover, it is advisable that Parties leave to the designated authorities the power to conclude such arrangements. The forms of assistance may also vary from case to case. It is obvious that the transmission of a request for access to sensitive medical information will have requirements which differ from routine inquiries about entries in a population record.

Chapter V – Convention Committee

156. The purpose of Articles 18, 19 and 20 is to facilitate the effective application of the Convention and, where necessary, to perfect it. The Convention Committee constitutes the third means of co-operation of the Parties in giving effect to the data protection laws implemented pursuant to the Convention (*cf*. paras **Error! Reference source not found.** and 141).

157. A Convention Committee is composed of representatives of all Parties, from the national supervisory authorities or from the government.

158. The nature of the Convention Committee and the procedure followed by it are similar to those set up under the terms of other conventions concluded in the framework of the Council of Europe.

159. Since the Convention addresses a constantly evolving subject, it can be expected that questions will arise both with regard to the practical application of the Convention (Article 19, littera a) and with regard to its meaning (same article, littera d).

160. According to Article 21, the Convention Committee is entitled to propose amendments to the Convention and examine other proposals for amendment formulated by a Party or the Committee of Ministers (Article 19 litterae b and c).

161. In order to guarantee the implementation of the data protection principles set by the Convention and seeking to harmonise a high level of protection between Parties to the Convention, the Convention Committee will have a key role in assessing compliance with the Convention, either when preparing an assessment of the level of data protection provided by candidate for accession (Article 19 littera e) or when periodically reviewing the implementation of the Convention by the Parties (Article 19 littera h). The Convention Committee will also have the power to assess the compliance of the data protection system of a State or international organisation with the Convention (Article 19 littera f).

162. In providing such opinions on the level of compliance with the Convention, the Convention Committee will work on the basis of a fair, transparent and public procedure detailed in its Rules of Procedure.

163. Furthermore, the Convention Committee will be entitled to approve models of standardised safeguards for data transfers (Article 19 littera g).

164. Finally, the Convention Committee may help to solve difficulties arising between Parties (Article 19 littera i). Where friendly settlements of disputes are concerned, the Convention Committee will seek a settlement through negotiation or any other amicable means.

Chapter VI – Amendments

Article 21 – Amendments

165. The Committee of Ministers, which adopted the original text of this Convention, is also competent to approve any amendments.

166. In accordance with paragraph 1, the initiative for amendments may be taken by the Committee of Ministers itself, by the Convention Committee and by a Party (whether a member State of the Council of Europe or not).

167. Any proposal for amendment that has not originated with the Convention Committee should be submitted to it, in accordance with paragraph 3, for an opinion.

Chapter VII – Final clauses

Article 22 – Entry into force

168. Since for the effectiveness of the Convention a wide geographic scope is considered essential, paragraph 2 sets at five the number of ratifications by member States of the Council of Europe necessary for the entry into force.

Article 23 – Accession by non-member States and international organisations

169. The Convention, which was originally developed in close co-operation with OECD and several non-European member countries, is open to any country around the globe complying with its provisions. The Convention Committee is entrusted with the task of assessing such compliance and preparing an opinion for the Committee of Ministers relating to the level of data protection of the candidate for accession.

170. Considering the frontier-less nature of data flows, accession by countries and international organisations from all over the world is sought. International organisations that can accede to the Convention are solely international organisations which are defined as intergovernmental organisations

(1986 Vienna Convention on the Law of Treaties between States and International Organisations or between International Organisations).

Article 24 – Territorial clause

171. The application of the Convention to remote territories under the jurisdiction of Parties or on whose behalf a Party can make undertakings is of practical importance in view of the use that is made of distant countries for data processing operations either for reasons of cost and manpower or in view of the utilisation of alternating night and daytime data processing capability.

Article 25 – Reservations

172. The rules contained in this Convention constitute the most basic and essential elements for effective data protection. For this reason, the Convention allows no reservations to its provisions, which are, moreover, reasonably flexible, having regard to the derogations permitted under certain articles.

Article 26 – Denunciation

173. In accordance with Article 80 of the United Nations Vienna Convention on the Law of Treaties, any Party is allowed to denounce the Convention.

Article 27 - Notifications

174. These provisions are in conformity with the customary final clauses contained in other conventions of the Council of Europe.