COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 10 May 2013 T-PD-BUR(2013)3ENrev

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

Draft Explanatory report of the modernised version of Convention 108 (based on the proposals adopted by the 29th Plenary meeting of the T-PD)

DG I – Human Rights and Rule of Law

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, automated individual decisions, information to be provided to the data subject, 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 in its Resolution 1843(2011) on 'The protection of privacy and personal data on the Internet and online media' the modernisation exercise.

The T-PD started the work by commissioning a report[1] to scientific experts 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.

On the basis of the first report, a list of issues to examine in the context of the modernisation was drawn up, and a consultation document[3] containing 30 questions was prepared.

---

[1] Report en 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 Jean-Marc Dinant, Cécile de Terwangne, Jean-Marc Moiny, Yves Poullet and Jean-Marc Van Gyzeghem of the CRID 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.

Those 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 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, audiovisual 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 translate 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 comments, but also to various Council of Europe committees, as well as to stakeholders of the private sector and civil society (in particular on the occasion of an exchange of views held on 2 May 2012 in 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 decided to instruct its Bureau to finalise these proposals in the light of the discussions and of comments made, 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 T-PD for modernising the Convention.

---

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 29 th Bureau meeting (5-7 February 2013)

Modernisation: objectives and main features

With new data protection challenges arising everyday, it appeared clear that Convention 108 should be modernised in order to better address challenges for privacy resulting from the use of new information and communication technologies, and to strengthen the Convention's evaluation and follow-up mechanism.

A broad consensus clearly emerged from the contributions made to the 2011 public consultation and the subsequent discussions held in various fora, which is that the general and technologically neutral nature of the Convention's provisions must be maintained (with more detailed sectoral texts by way of soft-law instruments), that the coherence and compatibility with other legal frameworks must be preserved and that the Convention's open character which gives it a unique potential of universal standard must be reaffirmed.

The topicality of the modernisation is to be underlined, as with increasing flows of ubiquitous data and related legal uncertainty as to the applicable law, ensuring that common core principles guarantee in as many countries as possible around the globe a certain minimum protection of personal data has become an absolute necessity.

Convention 108 and other international frameworks

<u>European Union (EU)</u>

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;*"

If 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 and 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.

Greater harmonisation of data protection legislations around the globe through increased accession to Convention 108 can only continue to be supported by the European Union.

Concerning transborder data flows, both regimes should in the future be articulated in order to be compatible and complementary, allowing for the free flow of data. The modernisation of Convention 108, aiming notably at strengthening the effectiveness and implementation of the Convention, should enable that consideration be given to parties of Convention 108 when the EU assesses the adequacy of the level of protection of a particular.

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

The co-operation spirit 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 review of the 1980 Guidelines as 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 compatibility between the two texts.

Asia-Pacific Economic Cooperation (APEC)

The APEC Privacy Framework and its recent Cross-Border Privacy Rules (CBPRs) system was considered, in particular when reflecting on modernising the transborder data flows provisions and underlining the need of greater cooperation between the various systems.

DRAFT EXPLANATORY REPORT

1. The purpose of this [Protocol] is to modernise the principles 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 strengthen their application.

2. Convention 108 which, in the thirty years elapsed since its opening for signature, served as the backbone of international law in over 40 European countries and influenced policy and legislation far beyond Europe's shores is to be modernised in order to fully apprehend the new data protection challenges arising in the context of technological developments of the information and communication society as well as of the increasing globalisation of exchanges.

3. The explanatory report to Convention 108 and the one to its additional protocol keep all their relevance in respect of the historical context and normative process of both instruments and should be read in connexion to the present one for those particular aspects.

4. The modernisation work was carried out taking duly account of the European Union's framework, the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development (OECD), the Asia Pacific Economic Cooperation Privacy framework as well as other relevant work such as the "International Standards on the Protection of Privacy with regard to the processing of Personal Data"[12]..

5. The Consultative Committee set up by virtue of Article 18 of the Convention prepared the modernisation proposals which were adopted at its 29th Plenary meeting (27-30 November 2012) and submitted to the Committee of Ministers. [...]

6. The text of this explanatory report does not constitute an instrument providing an authoritative interpretation of the Protocol, although 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. Putting individuals in control of their personal data being a major objective of the Convention, the preamble expressly refers to the right to control one's data, which stems from the right to privacy, and to the dignity of individuals. Indeed, human dignity implies that individuals can not be treated as mere objects which would be submitted to machines. Consequently, decisions based solely on the grounds of an automated processing of data can not be made without individuals having the right to have their views taken into consideration.

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

9. Taking into account the role of the right to protection of personal data in the society, the preamble underlines that the different rights and interests of individuals have, where necessary, to be reconciled, and that the right to data protection is to be considered alongside freedom of expression (which takes on another dimension with the Internet) as well as other fundamental rights and 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 opinion and to receive and impart information. It is furthermore acknowledged that the exercise of the right to data protection, which is not absolute, is not meant to be used as a general means to prevent public access to official documents[13]. Every time that the exercise of the rights to freedom of expression and access to public documents are considered to be limited due to the rights to privacy and data protection, a careful balance should be struck between all interests at stake in that particular situation.

10. The Convention, through the principles it lays down and values it protects, defines an appropriate environment for the free flow of information, which importance is to be underlined in particular as global information flows are an important societal feature, ultimately enabling the exercise of fundamental rights and freedoms. While data protection should not be intentionally used and employed as a means to erect barriers to information flows, to restrain the exchange of information or stiffle innovation, it can in some instances be a legitimate obstacle.

11. International cooperation between the competent authorities being a key aspect of an effective protection of the individuals, the Convention aims at enabling a reinforcement of such cooperation, notably through the possibility given to Parties to render to each other mutual assistance, and providing the appropriate legal basis for a formal framework of exchange.

Chapter I – General provisions

Article 1 – Object and purpose

12. The first article is devoted to a description of the Convention's object and purpose.

13. The guarantees set out in the Convention are extended to every individual regardless of nationality or residence, subject to the jurisdiction of the Parties. Clauses restricting data protection to a State's own nationals or legally resident aliens would be incompatible with the Convention.

14. The protection applies on the basis of the notion of 'jurisdiction' of the Parties, in order to better stand the test of time and continual technological developments, as well as the evolution of the legal concept of [State] jurisdiction according to international law. The concept of 'jurisdiction' is meant to refer to the traditional competences, i.e. prescriptive, adjucative and enforcement jurisdiction.

15. Finally, this article focuses on the subject of protection: the individuals are to be protected when their personal data are undergoing processing. This right has acquired an autonomous meaning over the last thirty years, 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

[13] See the Convention on Access to Official Documents (CETS 205).

Article 8" and as subsequently enshrined as a fundamental right in Article 8 of the Charter of Fundamental Rights of the European Union. The right to the protection of personal data is not an isolated right but an enabling one, without which other rights – such as the right to privacy - and fundamental freedoms could not be exercised and enjoyed in the same manner.

Article 2 – Definitions

16. Definitions used in this Convention are meant to enable a uniform application of different terms used in national legislation to express certain fundamental concepts.

Litt. a – 'personal data'

17. "Identifiable individual" means a person who can be easily identified. An individual is not considered 'identifiable' if his or her identification requires unreasonable time or effort for the controller or for any other person from whom the controller could reasonably and legally obtain the identification. The determination of the 'unreasonable' nature of the time or effort required to identify is to be assessed on a case by case basis, taking into account criteria such as the purpose of the identification by the data controller and the means employed.

18. Where such identification is not possible, the controller is not requested to provide supplementary efforts to identify the person with a view to complying with the obligations prescribed by the Convention.

19. The notion of 'identifiable' does not only refer to the individual's civil identity as such but also to what may allow to "individualise" or single out (and thus allow to treat differently) one person amongst others, such as an identification number, location data, an IP address, but also physical, physiological, genetic, mental, economic, cultural or social features. This identification can be done by referring to a specific person or to an access point or device (computer, mobile, etc).

20. Where an individual is not identifiable, data are said to be anonymous and are not covered by the Convention. Data that appear to be anonymous because they are notaccompanied of any identification data may nevertheless in some cases be indirectly identifiable where the piecing together of informative data (such as age, sex, occupation, geolocation, family status, etc.) makes it possible in fact to single out the person concerned. Where this is a possibility, the data may not be considered to be anonymous and must therefore be protected.

21. The notion of "data subject" expresses the idea that a person has a subjective right with regard to information about himself or herself, even where this is gathered by others.

Litt. b [/c] – 'data processing'

22. "Data processing" covers an open-ended general notion capable of flexible interpretation which starts from the collection of data and covers all automated operations performed on such data, as well as 'manual' operations organised in a structure which easily allows to search, combine or correlate the data related to a specific data subject.

Litt. c [/d] – 'controller'

23. "Controller" means the person or body responsible for the processing, who has the decision-making power concerning it. In order to identify who has effective control over the processing operations and holds such a power, various aspects for which a decision is to be made are to be considered: purposes and conditions of the processing, the means used for the processing, as well as the reasons justifying the processing, the operations to apply, the choice of data to be processed or who has access to it. The controller remains responsible of the data concerned by the processing wherever that data is located. This decision-making power can be exercised by a single controller or jointly by several co-controllers. Persons who carry out the operations according to the instructions given by the controller are not covered by this definition and are considered to be processors.

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

Litt. d [/e] – 'recipient'

25. "Recipient" is to operate in the context of disclosure or making available of data, thus possibly coinciding in practice with the definition of controller or processor or even with a third person.

Litt. e [/f] – 'processor'

26. "Processor" is a separate legal entity with respect to the controller acting on his/her behalf (this does not include the employees of the controller) carrying out the processing in the manner thatwas requested by the controller and for the needs of the controller.Going beyond the given mandate and acquiring a margin of decision in the processing leads to a change of legal status from processor to (joint) controller.

Article 3 – Scope

27. According to *paragraph 1,* the Convention is to be applied by the Parties to all processing - by public or private sector alike - subject to the jurisdiction of the concerned Party. Any processing carried out by a public authority falls directly within the jurisdiction of the Party, as it is the result of the Party's exercise of jurisdiction. Processing carried out by controllers of the private sector only fall within the jurisdiction of a Party when they present a sufficient connexion with the territory of that Party (e.g. when the controller is established on the territory of that Party or when services involving the processing of personal data are offered to a data subject habitually residing within that Party's territory) since the main criteria of definition of the jurisdiction is still linked to the territory). The Convention has to be applied when the processing is carried out entirely within the jurisdiction of the Party, as well as - in respect of the provisions of Article 12 - when transborder data flows occur, whether in the public or private sector.

28. *Paragraph 1bis* excludes from the scope of the Convention processing carried out for purely personal or household activities. This exclusion aims at avoiding the imposition of unreasonable obligations on data processing carried out by individuals in their private sphere, which have no professional or commercial grounds and exclusively correspond to personal (possibly collective when the processing is carried out in the context of thefamily sphere) or household activities such as storing pictures on a computer, creating a list of the contact details of friends and family members, corresponding, etc.

29. ‘Purely personal or household activities’ are to be illustrated according to several criteria, such as for instance the fact that when personal data is made available to an ‘indefinite number of persons’ (criteria used in cases dealing with Internet jurisdiction) or to someone obviously external to a private sphere, the exemption does not apply.

30. The Convention applies to providers of services and products used in the context of personal or household activities.

31. While the processing concerns data relating to natural persons, it has nevertheless been envisaged that the Parties could provide in their domestic laws for an extension of the protection to the data relating to legal persons. The Convention applies to living individuals and the personal data relating to deceased persons is not meant to be covered by it but this does not prevent Parties to extend the protection to deceased persons (e.g. to address the increasing number of cases of protection of such data on social media platforms).

Chapter II – Basic principles of data protection

Article 4 – Duties of the Parties

32. As this article indicates, the Convention obliges Parties to incorporate data protection provisions into their domestic legislation. The Convention was not designed to be self-executing, with the result that individual rights cannot be derived from it.

33. It should be specified that the notion of ‘law’ in the Convention encompasses statute law, including the Constitution and legislative acts as well as enactments of lower rank than statutes, and also, according to the legal system of the Party,the case law. The law has to be predictable and accessible, which implies that the law should be sufficiently clear to allow the individuals to regulate their own behaviour in light of expected legal consequences of their actions, and that the persons who are likely to be affected by this law should have access to it. Furthermore, where international organisations are concerned[14], ‘domestic law’ is to be understood as relating to the law and other legislative acts of such international organisations, which in some situations may legally have self-executing effect at the national level of the member States of such organisations.

34. The term “domestic law” denotes, according to the legal and constitutional system of the particular country, all substantive rules, whether of statute law or case-law, which meet the qualitative requirements, including those of accessibility and previsibility. It covers all measures 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 member states' constitutions and all written acts of legislative authorities (laws in the formal sense). It also covers not only all regulatory measures (decrees, regulations, orders, and administrative directives) based on such laws but also international conventions applicable in domestic law, including Community law in the case of European Union. It further includes all other acts whether of public or private law (including law of contract) together with court decisions in the common law countries or which interpret a written law. In

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

addition it includes any act of a professional body under powers delegated by parliament and in accordance with its independent rule-making powers.

Such binding measures may usefully be reinforced by measures of voluntary regulation 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.

35. The effectivity of the application of the measures giving effect to the provisions of the Convention is of crucial importance and beyond the specific legislative provisions, the role of the supervisory authority together with the remedies available to data subjects should be considered in the assessment of this effectivity.

36. 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) should be taken by the Parties concerned prior to the ratification or accession, thus prior to them being legally bound by the Convention. This provision aims at enabling the Convention Committee to verify *a priori* whether all "necessary measures" have been taken, in order to ensure that the Parties to the Convention observe their commitment and provide the expected level of data protection. The procedure and criteria used in this prior-check process are to be clearly defined in the rules of procedure of the Convention Committee.

37. Parties commit in Paragraph 3 of Article 4 to contribute actively to the evaluation of the compliance of their own system with their commitments, with a view to ensuring regular assessment of the effectiveness and implementation of the principles of the Convention. The regular submission of reports by the Parties on their data protection system is one possible element of this active contribution.

38. The evaluation of the compliance will be carried out by the Convention Committee on the basis of an objective, fair and transparent procedure set by the Convention Committee itself and fully described in its rules of procedure.

Article 5 – Legitimacy of data processing and quality of data

39. Data processing must be proportionate, that is, appropriate in relation to the legitimate aims pursued and necessary in the sense that these aims cannot be pursued by other appropriate and less intrusive measures with regard to the interests, rights and freedoms of the data subject or society. Such a processing should not lead to a disproportionate interference with these interests, rights and freedoms in relation to those of the controller or society. Finally, the proportionality is to be respected at all stages of the processing.

40. Paragraph 2 prescribes two alternative essential pre-requisites to a lawful processing: the individual's consent or a legitimate basis prescribed by law.

41. The data subject's consent must be freely given, specific, informed and explicit/unambiguous. No influence or pressure (which can also be of an economic nature, for instance when the data subject is consenting to a processing to benefit of services), whether direct or indirect, may be exercised on the data subject, who must be fully aware of the implications of his/her decision, and have been to this end adequately informed. An explicit consent translates a declaration of will, it is the expression of a freedom and consists of an affirmative action.

42. Consent does not override the necessity for the processing to be proportionate.

43. The data subject has the right to withdraw a given consent at any time (which is to be distinguished from the right to object to a processing), which will not affect the lawfulness of the processing before his/her withdrawal.

44. What is to be considered as alegitimate purpose may vary as it aims at ensuring that a balancing of all rights, freedoms and interests at stake be made; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as for instance between the legitimate interests of the data subject and the interest of the controller.

45. The reference to a "purpose" indicates that it should not be permitted to process data for undefined purposes, on the contrary, the particular purpose of the processing should be very carefully specified.

46. Where the law allows a processing, the presumption of its legitimacy will be reinforced when additional safeguards are provided and the basic principles of the Convention are respected.

47. The notion of 'legitimate basis' prescribed by law encompasses the processing necessary for the fulfilment of a contract (or pre-contractual measures), for the protection of the vital interests of the data subject or of the public interest [Processing for overriding legitimate interests can only be prescribed by law].

48. The conditions for the processing to be legitimate are set out in Paragraph 3: data should be processed lawfully and fairly and should respond to a number of criteria guaranteeing its quality. Data must have been collected in relation to an explicit, specified and legitimate purpose, and the processing of that particular data must continue to respond to that purpose, or at least not be incompatible with it. The concept of compatible use has to be interpreted restrictively, so as not to hamper transparency, legal certainty, predictability and fairness of the processing. In particular, personal data should not be further processed in a way that the data subject might find unexpected, inappropriate or otherwise objectionable.

49. The further processing of personal data for statistics, historical or scientific research purposes is *a priori* considered as compatible provided that other safeguards exist (such as for instance rules of professional secrecy, provisions governing communication of data or technical or organisational data-security measures) and that the processing is not the ground for a decision to be taken concerning the data subject, particularly decisions of an administrative, judicial, fiscal or other such nature. It should be underlined that statistics operations exclude by definition any use of the information obtained for decisions or measures concerning a particular individual.

50. Data undergoing processing should be adequate, relevant, not excessive and limited to the minimum necessary for the purposes for which they are processed. Data should furthermore be accurate and, where necessary, regularily kept up to date.

51. The requirement that data be not excessive in relation to the purposes for which they are processed reflects the principle of proportionality: data which would be relevant but would entail a disproportionate infringement to the basic rights at stake should not be processed. Such is the case for instance in the insurance sector : to allow the subscription of a life insurance, it may be

relevant to have the full health file of the subscriber but this is clearly excessive in regard of the purposes of the processing. The requirement for data not to be excessive does not duplicate the requirement to limit data to the minimum necessary.

52. The requirement concerning the time-limits for the storage of personal data means that data should after some time be irrevocably separated from the name of the person to whom they relate, so that the identification of the data subject would require unreasonable time or effort for the controller or for any other person from whom the controller could reasonably and legally obtain the identification.

Article 6 – Processing of sensitive data

53. The processing of certain types of data, or a certain processing of data, may be harmful to persons as they are likely to lead to encroachments on interests, rights and fundamental freedoms and shall only be permitted where a strengthened protection through appropriate safeguards, which complement the provisions of the Convention, are provided for by law. Such harm can for instance be created by the fact that the data subject's most intimate sphere is being affected, or by a potential risk of discrimination or injury to an individual's dignity or physical integrity.

54. In order to prevent such potential risks, processing of sensitive data need to be accompanied of appropriate safeguards (which are adapted to the risk at stake), such as the data subject's consent or a statutory regulation of the intended process ensuring the confidentiality of the data processed.

55. Specific types of data may entail a particular risk for the data subjects when they are processed, independently of the context of the processing.It is for instance the case with genetic data (which means 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 an equivalent information to be obtained), data related to offences, criminal convictions (based on criminal law and in the framework of a criminal procedure) and related security measures (involving deprivation of liberty for instance).

56. The processing of biometric data uniquely identifying a person (data resulting from a specific technical processing of data concerning the physical, biological or physiological characteristics of an individual which allows the unique identification of the latter) is also considered sensitive *per se*. This does not imply that all processing of 'biometric data' (such as pictures for instance) is to be considered as a sensitive processing but solely the processing which will lead to the unique identification of an individual.

57. Data can be sensitive according to the information their processing could reveal . While the processing of family names can in some circumstances be void of any risk for the individuals, such a processing could concern sensitive data when aimed at revealing the racial origin or religious beliefs of the individuals based on the linguistic origin. Concerning the processing of data for the information they reveal concerning heatlh, this 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.

58. The list of this article is not meant to be exhaustive. A Party may, in conformity with Article 11, include in its domestic law other categories of sensitive data, the processing of which is prescribed or restricted.

59. Sensitive data may have to be processed for statistical purposes (for instance in order to have equality statistics) and should be processed in a form in which data subjects are not identifiable.

Article 7 – Data security

60. There should be specific security measures, both of technical and organisational nature, for each processing, taking into account the degree of technical vulnerability of the structure performing the processing, the need to restrict access to the information, requirements concerning long-term storage, and so forth. The security measures which are to be applied to the data as much as to the processing itself must be appropriate, i.e. adapted to the nature of the data, the specific function of the processing and the risks involved.

61. Security measures should be based on the current state of the art of data security methods and techniques in the field of data processing and their cost should be commensurate to the seriousness of the potential risks.

62. 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 occurred and may seriously interfere with the fundamental rights and freedoms of the individual. A significant risk of financial, reputational, physical harm or humiliation could be deemed to constitute a “serious” interference.

63. Where such a data breach has occurred, the controller is requested to notify the supervisory authorities of the incident, and should expose measures taken and/or proposed in order to address the breach and its potential consequences.

64. The notification made by the controller to the supervisory authorities should in no circumstances preclude other complementary notifications. The controller should for instance be encouraged to notify, where necessary, the data subjects 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. Notification of other relevant authorities such as the ones in charge of computer systems security may also be required.

Article 7bis – Transparency of processing

65. Transparency is required from the controller in order to secure a fair processing and enable data subjects to fully exercise their rights in the context of that particular data processing.

66. Several elements of information have to be provided by the controller to the data subjects when directly or indirectly collecting their data.While the transparency requirements are compulsory, theinformation can be provided under any format (either through a website, technological tools on personal devices, newspaper, etc.) provided that it is easily accessible to the data subject. The information should be readable and adapted to the data subjects. Any information proving to be necessary to ensure a fair data processing, such as for instance the preservation period, 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 where the country does not provide any data protection regime for instance) also have to be provided.

67. The controller is not requested to provide this information where the data subject has already received it, or in the case of an indirect collection of data, where it is expressly prescribed by law (the law should be precise and well detailed) or where this proves to be impossible or involves disproportionate efforts. Such impossibility can both be of a legal nature (in the context of a criminal investigation or with lawyers bound by confidentiality for instance) or of a material nature (for instance with the controller who is only processing pictures and doesn't know the names and contact details of the data subjects).

Article 8 – Rights of the data subject

68. The provisions set out in this article are designed to enable a data subject to exercise and defend his or her rights concerning the processing of personal data relating to him/her.

69. These safeguards include the following main elements:

– right not to be submitted to a purely automated decision without having one's views taken into consideration ;
– right to object to a processing of personal data relating to him/her;
– right to be informed about the existence of a processing relating to him/her and about the content of the information;
– right to be informed about the reasoning of the processing;
– right of rectification orf erasure of data;
– right to a remedy if any of the previous elements are not respected;
– assistance of a supervisory authority.

70. Those rights are not absolute and have to be reconciled with other rights and legitimate interests. They can, in accordance with Article 9, be limited where this is necessary in a democratic society. The right to be informed about the reasoning of the processing can for instance be limited to protect the rights of others, such as "legally protected secrets" (e.g. trade secrets or the intellectual property or copyright protecting a software). In the same manner, the right to object to a processing will not apply where the processing is prescribed by law (for example for the purpose of investigation or prosecution of criminal offences) or where a valid consent was given for that particular processing (it should nevertheless be underlined that a given consent can be withdrawn).

71. It is not specified 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/her behalf but in exceptional cases (security or health related for instance) the right of accesscan be indirectly exercised through the intermediary of the supervisory authority.

72. The lack of respect of an objection to a processing, for instance if the controller doesn't seize the processing or continues to make use of the data, should have legal consequences.

73. The wording of littera c is intended to cover various formulas followed by national legislation: communication free of charge at fixed intervals as well as communication against payment at any other time, etc. 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. The term "expense" means the fee charged to the data subject, not the actual cost of the operation.

74. In the case of rectifications obtained in conformity with the principle set out in littera e, those rectifications should where possible be brought to the recipients of the original information, unless this proves to be impossible or involves disproportionate efforts.

75. Concerning the assistance foreseen under littera g, when the person resides in the territory of another Party, he/she shall be given the option of submitting the request through the intermediary of the authority designated by that Party. The request for assistance shall contain all the necessary particulars, relating inter alia to: the name, address and any other relevant particulars identifying the person making the request; the 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 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.

76. Furthermore, it should be noted that the right of rectification or erasure, together with the provision on the length of time of data storage (article 5.3. littera e), coupled with an effective right to object and the right to withdraw consent offer an effective protection to the data subject and pragmatically correspond to the effects of the so-called ‘right to be forgotten’.

Article 8bis - Additional obligations

77. In order to ensure an effective right to the protection of personal data, additional obligations have to be prescribed in respect of the actors of the processing, the controller as well as, where applicable the processor. The proactive drive of the controller in ensuring data protection is to be linked to the responsibility to verify and demonstrate compliance of the data processing concerned with the applicable law. Those obligations, which are to be applied at all stages of the processing, including the designing phase are meant to enable the controller to drive and demonstrate compliance with the applicable provisions, thereby enhancing trust. They will notably have to take the appropriate measures, such as the training of employees, setting-up various notification procedures (indicating for instance that data has to be deleted from the system) or specific contractual provisions in the delegation of the processing, to implement the provisions giving effect to the Convention, as well as setting up internal mechanisms aimed at enabling the verification and demonstration of the compliance.

78. It is worth noting that in respect of those additional obligations, particular attention has been given to the requirements established under APEC Cross-Border Privacy Rules (CBPRs) program for the certified controller.

79. A possible measure to be taken by the controller in order to allow such a verification and demonstration of compliance could consist of the designation of a ‘data protection officer’ who would be entrusted with the means necessary to fulfil its mission independently. Such a data protection officer, whose designation should be notified to the supervisory authority, can be internal or external to the controller.

80. Before carrying out a processing, an analysis of the risk of such a processing on the rights and fundamental freedom of the data subject will have to be made. The risk will notably have to be assessed in light of the principle of proportionality. In cases where the comprehensive

overview of the processing envisaged is held by the processor, this obligation may be imposed on the processor rather than on the controller. Assistance of IT systems developers or designers in analysing the risks could certainly reduce the administrative burdens linked to this exercise.

81. In order to better guarantee an effective data protection, processing operations should integrate as early as possible, i.e. at the stage of architecture and system design, data protection requirements and this should not only apply to the technology used for the processing but also to the related work and management processes. Easy-to-use functionalities allowing the compliance of the processing with the applicable law should be put in place, aiming for instance at facilitating the portability of data from one provider to another. Developers and designers should pay due regard to the principle of data minimisation when setting up technical requirements in default settings.

82. Those additional obligations have to be meaningful and cost-effective, they can be scaled and adapted to the size of the processing entity, the volume of data processed and the risks at stake. Certain categories of processing, such as processing which do not entail any risk for the individuals may be exemptedfrom some of the obligations in this Article.

Article 9 – Exceptions and restrictions

83. As a general statement, no exceptions to the basic principles for protection of personal data are to be allowed. It is nevertheless permitted, for a limited number of provisions, to benefit of derogations when such a derogation is provided for by law and is necessary for the protection of fundamental values in a democratic society in specific cases. The text of the first paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Convention on Human Rights. The criteria to define a measure which is "necessary in a democratic society" should be considered in the light of the given situation in each country but such a measure shall pursue a legitimate aim and thus meet a "pressing social need" which cannot be achieved by less intrusive means. Especially, such a measure should be proportionate to the legitimate aim pursued and the reasons adduced by the national authorities to justify it should appear "relevant and sufficient".

84. The necessity of such measures is to be examined in light of limited legitimate aims only, detailed in littera a and b of the first paragraph. Littera a lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the Convention, States would have an unduly wide leeway.

85. The notion of "national security" should be understood restrictively and in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State.

86. The term "important economic and financial interests of the State" covers in particular tax collection requirements and exchange control. The term "prevention and suppression of criminal offences" in this littera includes the investigation as well as the prosecution of criminal offences.

87. Littera b concerns major interests of private parties, such as those of the data subject himself (for example psychiatric information) or of third parties such as freedom of expression, confidentiality of communications and business or commercial secrecy and other legally protected secrets, etc.

88. In respect of transborder flows of personal data, a specific restriction is allowed on the basis of freedom of expression.

89. The third Paragraph leaves the possibility of restricting the rights with regard to certain data processing carried out for statistical or scientific research purposes which pose no risk for the protection of personal data. The use of data for statistical work, in the public and private fields alike, in so far as these data are presented in aggregate form and stripped of their identifiers is for instance possible, provided that appropriate data protection safeguards are in place (see para. 49).

Article 10 – Sanctions and remedies

90. In order for the Convention to guarantee an effective data protection, the duties of the data users and the rights of data subjects should be reflected in the national legislation of the Parties by corresponding sanctions and remedies.

91. In keeping with the non self-executing character of the Convention, it should be left to each Party to determine the nature (civil, administrative, criminal / judicial, non judicial) of these sanctions and remedies. Financial compensation of damages caused by the processing as well as class actions could also be considered.

Article 11 – Extended protection

92. 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. It is underlined in the text 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

93. The aim of this article is to facilitate, where applicable, the free flow of information, regardless of frontiers, (recalled in the Preamble) while ensuring an appropriate protection of personal data.

94. As a general rule, any data flows implying a change of jurisdiction requires that an appropriate level of data protection, based on the principles of the Convention, be guaranteed (in the recipient's jurisdiction), with various safeguards where the recipient is not subject to the jurisdiction of a Party to the Convention. Indeed, the effective protection of personal data means that there should in principle be no transborder flows of personal data to recipient countries or organisations where the protection of such data is not guaranteed.

95. Transborder data flows relate to the processing of data involving a movement of data outside the jurisdiction of a Party. This movement of data can take a variety of forms depending on the technique used (cloud computing, localised transfer, etc.) the circuit followed (direct from one point of origin to another of destination, or via one or more other points of transit); the relations between the Party transferring data and the recipient (within one organisation or different organisations); etc.

96. Article 12 only applies to the export of data, not to their import. The latter presents no problems because imported data are in any case covered by the data protection regime of the recipient Party. Some problems might however arise in case of re-import of data processed abroad in violation of certain provisions of the law of the jurisdiction of origin, Party to the Convention. In such cases, it will be up to the jurisdiction of origin to take, before export, the necessary measures according to Article 12.

97. Paragraph 1 applies to data flows between Parties to the Convention, which can not be prohibited or subject to special authorisation, with the exception of Parties belonging to a regional organisation with binding harmonised rules of protection governing such flows of data. 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 certain minimum level of protection considered appropriate, in the absence of regional binding harmonised rules governing data flows, and data flows between Parties should operate freely.

98. 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.

99. In some cases flows will be made from a Party simultaneously to several foreign States or international organisations, some of which are Parties to the Convention whereas others are not. In those cases, the Party transferring the data, which has a procedure of export licences may not be able to avoid applying those procedures also to the data destined for a Party, but it should then proceed in such a way as to ensure that a licence for data transfers to the latter Party is agreed.

100. Paragraph 2 regulates transborder flows of data to a recipient which is not subject to the jurisdiction of a Party. As for any data flowing outside the national frontiers, an appropriate level of protection in the recipient State or organisation is to be guaranteed, and as this cannot be presumed since the recipient is not a Party, the Convention establishes two main possibilities 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.

101. An appropriate level of data protection can be ensured provided that the persons involved in the transfer (legal as well as natural persons) provide sufficient guarantees, such as approved standardised safeguards binding both the controller who transfers data and the recipient who is not subject to the jurisdiction of a Party. The adoption of common approved standardised safeguards for the Parties to the Convention should be sought.

102. The content of the contracts concerned must include the relevant elements of data protection. Moreover, in procedural terms, contract terms could be such, for example, that the data subject has a contact person on the staff of the person responsible for the data flow, whose responsibility it is to ensure compliance with the substantive standards of protection. The subject would be free to contact this person at any time and at no cost and, where applicable, obtain assistance in exercising his or her rights.

103. The level of protection should be assessed on a case-by-case basis for each transfer or category of transfers and various elements of the transfer should be examined such as, in particular, the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral

rules of law applicable in the State or organisation in question and the professional and security rules which apply there.

104. The assessment of an appropriate level of protection must take into account the principles of the Convention and the extent to which they are met in the recipient State or organisation – as far as they are relevant for the specific case of transfer – and how the data subject can defend his or her interests in case of non compliance in a specific case.

105. Paragraph 4 enables Parties to derogate, in a particular case, from the principle of an appropriate level of protection and to allow a specific transfer to a recipient which does not ensure such a protection. Such derogations are permitted in limited situations only (data subject's consent or specific interest and prevailing legitimate interests provided by law) and subject to the competent supervisory authority's oversight. Such derogations should not be disproportionate and should not be used for massive or repetitive data transfers.

106. A complementary safeguard is foreseen in Paragraph 5 with the possible intervention of the competent supervisory authority, entitled to request that the quality and effectiveness of the measures taken be demonstrated, and to prohibit, suspend or subject to condition the transfer. In the particular case of ad hoc safeguards, the competent supervisory authority shall be informed of the modalities of the transfer.

107. Data flows and the related necessary appropriate data protection could in the future increasingly rely on the benefits of a closer articulation of existing privacy frameworks around the globe, such as the OECD Guidelines or the APEC Privacy Framework and its CBPRs certified controllers.

Chapter III bis – Supervisory authorities

Article 12bis – Supervisory authorities

108. 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, generally a commissioner, a commission, an ombudsman or an inspector general. These data protection supervisory authorities provide for an appropriate remedy if they have effective powers and functions and enjoy genuine independence in the fulfilment of their duties. They have become an essential component of the data protection supervisory system in a democratic society.

109. This Article of the Convention aims to enforce 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. More than one authority might be needed to meet the particular circumstances of different legal systems. These authorities may exercise their tasks without prejudice to the competence of legal or other bodies responsible for ensuring respect of domestic law giving effect to the principles of the Convention. The supervisory authorities should have the necessary technical and human resources (lawyers, computer experts) to take prompt and effective action.

110. Parties have considerable discretion as to the powers which the authorities should be given for carrying out their task. According to the Convention however, they must at least be given powers of investigation and intervention, be consulted in the legislative and administrative normative processes relating to data protection, have specific powers in the context of data flows, be given the power to issue decisions and sanction administrative offences, 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 raise awareness on data protection.

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

112. The supervisory authority's power of intervention – where processing presents particular risks to rights and fundamental freedoms - may take various forms in domestic 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 in person. The power to issue injunctions on controllers who are unwilling to communicate the required information within a reasonable time would be a particularly effective manifestation 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, 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.

113. Whilst contributing to the protection of individual rights, the supervisory authority also serves as an intermediary between the data subject and the controller. In this context, it seems particularly important that the supervisory authority should be able to provide information to individuals or data users about the rights and obligations concerning data protection.

114. Moreover, every person should have the possibility to request the supervisory authority to investigate a claim concerning his/her rights and liberties in respect of personal data processing. This helps to guarantee people's right to an appropriate remedy, in keeping with Article 10 and Article 8 of the Convention. Further to such investigations, the supervisory authorities may in particular decide to impose an administrative sanction, or where this is not in their powers, refer the offence to another competent authority which will do so. In some jurisdictions, the lack of legal personality of the supervisory authorities will prevent them from engaging in legal proceedings, the power to sanction administrative offences thus being very important for their enforcement capacities. When such powers are given to the supervisory authorities, the necessary resources to fulfill this duty should be provided.

115. It is recalled that where an administrative decision produces legal effects, every person concerned has a right to have a judicial remedy. However, domestic law may provide for the lodging of a claim with the supervisory authority as a condition of this judicial remedy.

116. 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. This power derives in particular from the power to carry out investigations, which may lead the authority to discover an infringement of a person's right to protection. The Parties may fulfil the obligation to grant this power to the authority by enabling it to make judgments.

117. The supervisory authority’s competences are not limited to the ones listed in Article 12bis. It should be borne in mind that the Parties have other means of making the task of the

supervisory authority effective. 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. The authority could keep a data processing register open to the public. The authority are also to be asked to give its opinion when legislative, regulatory or administrative measures concerning personal data processing are in preparation, or on codes of conduct.

118. 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, 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 or the adoption of decisions without being subject to external orders or injunctions.

119. The prohibition of seeking or accepting instructions only covers the performance of the duties as a supervisory authority, and not when the authority acts as an employer for example. This doesn't prevent the supervisory authorities to seek advice (for instance from consultants, counterparts, etc.) where it is deemed necessary.

120. Transparency on the work and activities of the supervisory authorities should be encouraged; through for instance the publication of annual activity reports comprising inter alia information related to their enforcement actions. The supervisory authority should have the power to inform the public through regular reports, the publication of opinions or any other means of communication.

121. 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.

122. Moreover, in cases where the supervisory authority does not itself have judicial competence, the intervention of a supervisory authority shall not constitute an obstacle to the possibility for the individual to have a judicial remedy.

123. Strengthening co-operation between the supervisory authorities must contribute to the development of the level of protection in the Parties' practice under the Convention. This co-operation is in addition to the mutual assistance provided for in Chapter IV of the Convention and the work of the Convention Committee. Its purpose is to provide improved protection to the people concerned. With increasing frequency people are directly affected by data processing operations which are not confined to one country and therefore involve the laws and authorities of more than one country. The development of international electronic networks and increasing cross-border flows in the service industries and the work environment are examples. In such a context international co-operation between supervisory authorities ensures that people are able to exercise their rights on an international as well as a national level. The promotion of co-operation could take the form of networks or meetings, taking advantage of already existing opportunities for authorities to meet and discuss matters of common interest. The importance, for those authorities, of keeping abreast of technological developments shall be stressed. Whenever an authority wishes to draft general recommendations, it can decide to consult stakeholders.

Chapter IV – Mutual assistance

Article 13 – Co-operation between Parties

124. The authorities will render each other general assistance for controls *a priori* (for example certifying whether terminals in one country, linked to a data centre in another country meet data security requirements) as well as specific assistance for controls *a posteriori* (for example to verify the activities of a specific data centre). The information may be of a legal or factual character.

125. This cooperation should in no way adversely affect existing cooperation instruments in the civil and criminal spheres.

Article 14 (deleted)

Article 15 – Safeguards concerning assistance

126. This article ensures that data protection 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.

127. This provision is of fundamental importance for mutual trust, on which mutual assistance is based.

Article 16 – Refusal of requests for assistance

128. This article states first 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.

129. 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 the individual, but also if the very fact of seeking the information might prejudice his/her rights and fundamental freedoms.

Article 17 – Costs and procedures of assistance

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

131. "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.

132. 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 also administrative arrangements which may even be confined to specific cases. It is moreover 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 require a different form than routine inquiries about entries in a population record.

Chapter V – Convention committee

133. The purpose of Articles 18, 19 and 20 is to facilitate the smooth running of the convention and, where necessary, to perfect it.

134. A Convention Committee, composed of representatives of all Parties, will endeavour to formulate proposals or render advice to those Parties for the solution of these problems.

135. 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.

136. 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).

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

138. In order to guarantee the implementation of the data protection principles set by the Convention and ensure an harmonised 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 faculty to assess the compliance with the Convention of the data protection system of a State or international organisation (Article 19 littera f).

139. It shall be stressed that to provide such opinions on the level of compliance with the Convention, the Convention Committee will be working on the basis of a fair, transparent and public procedure detailed in its Rules of Procedure.

140. The Convention Committee will furthermore be entitled to approve models of standardised safeguards for data transfers (Article 19 littera g).

141. 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 peaceful means.

Chapter VI – Amendments

Article 21 – Amendments

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

143. 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).

144. Any proposal for amendment which 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

145. Since for the effectiveness of the convention a wide geographic scope is considered essential, paragraph 2 fixes 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

146. The Convention which was elaborated 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.

147. Considering the frontier less nature of data flows, accession by countries and international organisations from all over the world is sought.

Article 24 – Territorial clause

148. 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

149. 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

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

Article 27 - Notifications

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