COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, ~~25 March~~23 November 2014
CAHDATA(2014)~~xx~~06

AD HOC COMMITTEE ON DATA PROTECTION

(CAHDATA)

Draft Explanatory report of the modernised version of Convention 108

Directorate General 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 Sstates.

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 modernisation exercise~~.

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.

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.

---

[1] Report oen 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.

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

---

[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)

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 processings 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.

Convention 108 and other international frameworks

Organisation for Economic Co-operation and Development (OECD) -1980

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[12] 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.

United Nations - 1990

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:

[12] 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.

"*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. 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 of being 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 Sstate.

The European Union in its priorities of cooperation[13] 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 system (CBPRs) were considered when reflecting on the need to increase cooperation among regions and systems, in particular as regards international enforcement.

Other instruments

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

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

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, ~~commercial~~ 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 into 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"[14] .

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. [...]

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. Putting individuals in a position to know, to understand and thus to control the processing of their personal data by others is a major objective of the Convention. Accordingly, the preamble expressly refers to the right to control one's 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

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

place when processing personal data, in order for individuals not to be treated as mere objects. Consequently, decisions based solely on the grounds of automated processing of data cannot be made final without individuals having the right to have their 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 in order 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[15].

10. Convention 108, through the principles it lays down and the values it holds, protects the individuals 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. The flow of personal data must respect the rights of the individuals. Furthermore, innovative technologies should respect ~~the rights of the individuals~~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 the supervisory authorities is a key element for effective protection of the individuals, the Convention aims to enable reinforcement of such cooperation, notably by allowing Parties to render mutual assistance, and providing the appropriate legal basis for a [formal] framework of exchange of information for investigation and enforcement.

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. 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 Article 8"[16] 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 and fundamental freedoms – such as the right to privacy, the 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.

[15] See the Convention on Access to Official Documents (CETS 205).
[16] ECtHR MS v. Sweden 1997 para 41.

14. 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 foreign nationals would be incompatible with the Convention.

15. ~~The scope of the protection depends on 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 and to reinforce the commitment to individuals' protection. The concept of 'jurisdiction' is meant to refer to the traditional competences of the State, i.e. prescriptive, adjucative and enforcement jurisdiction.~~

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 directly or indirectly identified. An individual is not considered 'identifiable' if his or her identification would require unreasonable time, effort or means. The determination of what constitutes 'unreasonable time, effort or means' should be assessed on a case by case basis, in light of purpose of the processing and taking into account objective criteria such as the cost, the benefits of such an identification, the technology used, etc.

18. 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 among others. This "individualisation" can 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, biometric or genetic data, location data, an IP address, etc.

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

20. Data that appears to be anonymous because it is not accompanied by any obvious identifying data may, nevertheless in particular cases, permit to identify the related individual. This is the case where for example, alone or through the combination of physical, physiological, genetic, mental, economic, cultural or social data (such as age, sex, occupation, geolocation, family status, etc.) it is possible for the controller, or any ~~legitimate or illegitimate~~person ~~(in particular when the data was made publicly available) actor~~ to identify the ~~person concerned~~data subject. Where this is the case, the data may not be considered to be anonymous and must be covered by the provisions of the Convention.

21. When data ~~are~~ is made anonymous, all means should be put in place to avoid re-identification of individuals, in particular, all technical means should be secured in order to guarantee that data will remain anonymised. The anonymity of data should be re-evaluated in time as in light of the fast pace of technological development.~~,~~ W~~w~~hat could at a point in time be considered 'unreasonable' could after some time be considerably facilitated by technology and enable identification with reasonable ease.

22. 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 gathered by others.

Litt. b [/c] – 'data processing'

23. "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. A data processing also occurs where no automated operation is performed but data is organised in a structure which allows to search, combine or correlate the data related to a specific data subject.

Litt. c [/d] – 'controller'

24. "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. 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 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 under the controller's authority and carry out the processing solely according to the controller's instructions are to be considered processors. Furthermore, the processors who legitimately process data for their own purposes are to be considered as controllers for the processing operations linked to those purposes.

25. The decision-making power of a controller can rely in the fact that the processing of personal data is the main activity of the controller (e.g. a mailing company processing personal data to deliver targeted ads, etc.) or as the processing constitutes a support to the main activity (e.g. when establishing a database of customers, processing of data of customers to carry out their defence before courts, to perform a contract, etc.).

26. 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 as the case may be, are to be provided to the data subject.

Litt. d [/e] – 'recipient'

27. "Recipient" is an individual or an entity that receives personal data or to whom personal data ~~are~~ is made available. Depending on the circumstances, the controller, the processor, the data subject or a third party may also be a recipient.

Litt. e [/f] – 'processor'

28. "Processor" is a separate entity acting on behalf of the controller carrying out the processing in the manner that was requested by the controller and for the needs of the controller. An employee of a controller is not a processor.

Article 3 – Scope

29. 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 data processing carried out by a public sector entity 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 fall within the jurisdiction of a Party when they present a sufficient connexion with the territory of that Party, such as for instance when the controller is established on the territory of that Party or when activities involving the data processing are offered to a data subject in that territory, since the main criteria of definition of the jurisdiction is still linked to the territory. The Convention has to be applied when the data 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.

~~29.~~30. The scope of the protection depends on 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 and to reinforce the commitment to individuals' protection. The concept of 'jurisdiction' is meant to refer to the traditional competences of the State, i.e. prescriptive, adjucative and enforcement jurisdiction.

~~30.~~31. *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 for activities relating to the exercise of their private life. These activities have no professional or commercial grounds 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.

~~31.~~32. Whether activities are 'purely personal or household activities' will depend on the circumstances. For example, when personal data is intentionally made available to a large number of persons or to persons obviously external to the private sphere, such as an open website on the internet, the exemption does not apply.

~~32.~~33. The Convention applies to providers of services and products, such as softwares or applications, used in the context of personal or household activities and which process personal data.

~~33.~~34. While the Convention concerns data processing relating to natural persons the Parties can provide in their domestic laws for an extension of the protection to the data relating to legal persons in order to protect their legitimate 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 or heirs).

Chapter II – Basic principles of data protection

Article 4 – Duties of the Parties

~~34.~~35. As this article indicates, the Convention obliges Parties to incorporate data protection provisions into their domestic 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 domestic law.

~~35.~~36. The term “domestic law” denotes, according to the legal and constitutional system of the particular country, all substantive rules of binding nature, whether of statute law or case law, which 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)~~. It also covers not only~~ as well as all regulatory measures (decrees, regulations, orders, and administrative directives) based on such laws. It also covers ~~, but also~~ international conventions applicable in domestic law, including European Union law. It further 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.

~~36.~~37. 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.

~~37.~~38. Where international organisations are concerned[17], ‘domestic law’ is to be understood as relating to the law 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.

~~38.~~39. 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.

~~39.~~40. 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] ratification or accession, i.e. before a Party becomes legally bound by the Convention. This provision aims to enable the Convention Committee to verify *a priori* 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

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

and criteria used for this pre-accession check are to be clearly defined in the Convention Committee's rules of procedure.

40.41. 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). The regular submission of reports by the Parties on the application of their data protection law is one possible element of this active contribution.

41.42. 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 and fully described in its rules of procedure.

Article 5 – Legitimacy of data processing and quality of data

42.43. 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 society. Such data processing should not lead to a disproportionate interference with these interests, or rights and freedoms in relation to those of the controller or society. The principle of proportionality is to be respected at all stages of the processing, including at the initial one, i.e. when deciding whether or not to carry out the processing.

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

44.45. The data subject's consent must be freely given, specific, informed and explicit/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 or by a clear affirmative action and which clearly indicates in this specific context the acceptance of the proposed processing of personal data. The mere silence or inactivity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. The data subject must be fully aware of the implications of his/her decision, and have been, to this end, adequately informed. No influence or pressure (which can be of an economic nature) whether direct or indirect, may be exercised on the data subject.

45.46. 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 tested.

46.47. The data subject has the right to withdraw his or her consent 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 processing that occurred before his or her withdrawal of consent.

47.48. The notion of 'legitimate basis' laid down by law encompasses the 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, necessary for the protection of the vital interests of the data subject, the processing carried out on the basis of important grounds of public interest or for overriding legitimate interests of the controller.

~~48. What is to be considered a legitimate purpose depends on the circumstances as it aims 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 the society. In all cases, a processing serving a fraudulent intent cannot be based on a legitimate purpose.~~

49. Processing carried out on important grounds of public interest should be prescribed by law, as for instance in some situations of natural disasters, where the processing of personal data of missing persons (for a limited time) may be necessary for the purposes related to the emergency context – which will be evaluated on a case-by-case basis – in order to serve both important grounds of public interest and/or the vital interests of the data subject, for instance monitoring epidemic and its spread.

50. The conditions for legitimate processing are set out in paragraph 3: data should be processed lawfully and fairly, and satisfy criteria guaranteeing its quality. Data must have been collected for an explicit, specified and legitimate purpose, and the processing of that particular data must be for that purpose, or at least not be incompatible with it. The reference to a specified "purpose" indicates that it should not be permitted to process data for undefined, imprecise or vague purposes. What is to be considered a legitimate purpose depends on the circumstances as it aims 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 the society. In all cases, a processing serving a fraudulent intent cannot be based on a legitimate purpose.

~~50.~~51. 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.

~~51.~~52. 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 restricted access and communication of data for the above mentioned purposes, notably in relation with public 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.

~~52.~~53. Data undergoing processing should be adequate, relevant, not excessive and limited to the minimum necessary for the purposes for which ~~they are~~it is processed. Furthermore, the data should be accurate and, where necessary, regularly kept up to date.

~~53.~~54. The requirement that data be not excessive in relation to the purposes for which it is processed reflects the principle of proportionality: data which would be relevant but would entail a disproportionate infringement of the fundamental rights and freedoms at stake should not be processed. Such is the case, for instance, in a standard recruitment procedure where it is clearly excessive in relation to the purposes of the processing to collect HIV data of the candidates to the post, while this can be considered as relevant data (in terms of management of futures absences for instance). The requirement for data not to be excessive does not duplicate the requirement to limit the quantity of data to the minimum necessary.

~~54.~~55. The requirement 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 be kept in a form that prevents any direct or indirect identification of the data subject.

Article 6 – Processing of sensitive data

~~55.~~56. The processing of certain types of data, or the processing of data for the sensitive information it reveals, may lead to encroachments on interests, rights and freedoms and shall only be permitted where strengthened protection through appropriate safeguards, which complement the other protective provisions of the Convention, is provided for by law. This can for instance be the case where the data subject's most intimate sphere is being affected, or where there is a potential risk of discrimination or injury to an individual's dignity or physical integrity.

~~56.~~57. 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 in a cumulative manner, the data subject's explicit consent, a specific law covering the intended purpose and means of the processing, a professional secrecy obligation, a risk analysis, a particular organisational or technical security measure.

~~57.~~58. Specific types of 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 thirds. Genetic data is 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 and suspected 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).

~~58.~~59. The 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 latter, is also considered sensitive.

~~59.~~60. The processing of photographs will not systematically be a sensitive processing as they 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 their processing will aim at revealing racial or health information, such a processing will be considered as a sensitive one.

~~60.~~61. Some processing can be sensitive when data are processed for a specific information they reveal ~~and~~ that ~~have~~ has the potential of harming, in the circumstances at stake, data subjects. While the processing of family names can in some circumstances be void of any risk for the individuals (e.g. common payroll purposes), such a processing could be sensitive, 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 they reveal

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.

~~61.~~62. Where sensitive data may have to be processed for a statistical interest (for instance in order to have equality statistics), it should be kept in an identifiable form only for as long as necessary, and appropriate safeguards have to be put in place (such as for instance no publication or dissemination of the data).

Article 7 – Data security

~~62.~~63. ~~There should~~The controller or where applicable the processor should take ~~be~~ 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.

~~63.~~64. 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 updated as needed.

~~64.~~65. 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 secrecy, which may cause financial, reputational, physical harm or humiliation, could be deemed to constitute a “serious” interference.

~~65.~~66. Where such a data breach has occurred, the controller is requested to notify the supervisory authorities of the incident. The controller should also notify the supervisory authorities of any measures taken and/or proposed to address the breach and its potential consequences.

~~66.~~67. 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, 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 to other relevant authorities such as those in charge of computer systems security may also be required.

Article 7bis – Transparency of processing

~~67.~~68. The controller is required to be transparent in its data processing in order to secure a processing that is fair and to enable data subjects to understand and thus fully exercise their rights in the context of that particular data processing.

~~68.~~69. Certain minimum information has to be compulsorily provided by the controller to the data subjects when directly or indirectly (through third parties) collecting their data. While the transparency requirements are compulsory, the information on the name and address of the

controller, the purpose and recipients (be them obvious or not), can be provided 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 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) may also be provided.

69.70. 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 through third parties where it is expressly prescribed by law (the law should be precise and well detailed), 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 both be of a legal nature (in the context of a criminal investigation or with lawyers bound by confidentiality for instance) or of a practical nature (for instance with the controller who is only processing pictures and doesn't know the names and contact details of the data subjects).

70.71. When such impossibility is of a practical nature, the data controller shall nonetheless use any available, reasonable and affordable means making it possible to inform data subjects in general or individually as the case may be (for instance when the controller is put in contact with the data subject for any reason, or through the website of the controller, etc.).

Article 8 – Rights of the data subject

71.72. The provisions set out in this article list a set of rights that any data subject should be able to ~~are designed to enable a data subject~~ to exercise and defend ~~his or her rights~~ concerning the processing of personal data relating to him or her.

72.73. These ~~safeguards~~ 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 ;
– the right to object to a processing of personal data relating to him or her;
– the right to be informed about the existence of a processing relating to him or her and to access the data,;
– the right to be informed about the reasoning on which is based the processing;
– the right to rectification or erasure of inaccurate, false, or generally, unlawfully processed data;
– the right to a remedy if any of the previous rights is not respected;
– assistance of a supervisory authority.

73.74. 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 measure in a democratic society. For instance, the right to be informed about the reasoning on which ~~is based~~ the processing is based can be limited to protect the rights of others, such as "legally protected secrets" (e.g. trade secrets). As regards the right to object, the controller may have a compelling legitimate ground for the processing, which overrides the interests or rights and

freedoms of the data subject, and will have to be demonstrated on a case-by-case basis in order to pursue such processing. Failure to demonstrate such compelling legitimate grounds while pursuing the processing could be considered as unlawful.

~~74.~~75. 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. The right to object may not be applicable when the processing is necessary for the execution of a contract or follows a valid consent which has not been withdrawn.

~~75.~~76. 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, ~~however,~~ 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 and 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, for instance when it is in the interest of the data subject, with the assistance of a health professional.

~~76.~~77. It is essential that an individual who is subject to a purely automated decision has the right to put forward his or her point of view, in particular with a view to having the opportunity to substantiate the possible inaccuracy of the data used, the irrelevance of the profile applied to his or her particular situation, or other arguments that will have an impact on the result of the automated decision.

~~77.~~78. Data subjects should be entitled to know about the personal data processed and the reasoning (for instance in the case of credit scoring, the logic underpinning the processing and resulting in a 'yes' or 'no' decision, and not simply information on the decision itself) which led to any resulting conclusions as without an understanding of these elements there could be no effective exercise of other essential safeguards - the right to object and the right to complain to a competent authority.

~~78.~~79. While the right of access should in principle be free of charge, the wording of littera c is intended to cover various formulas followed by national legislation for appropriate cases: communication free of charge at fixed intervals as well as communication against a maximum lump-sum payment, 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, which should be reasonable in order not to prevent data subjects to exercise their rights and should in any case either be equal or inferior to the actual cost of the operation.

~~79.~~80. 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.

~~80.~~81. Concerning the assistance foreseen under littera g, when the person resides in the territory of another Party, he or 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 details 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.

~~81.~~82. Littera g aims at safeguarding an effective protection of the individuals by providing them the assistance of a supervisory authority in exercising the rights provided by the Convention.

~~82.~~83. Furthermore, it should be noted that the specification of the purpose, the conditions for the legitimacy of the processing, the right of rectification or erasure, together with the provision on the length of time for data storage (article 5.3. 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 collection of rights pragmatically corresponds to the effect of what is referred to as a 'right to be forgotten'.

Article 8bis - Additional obligations

~~83.~~84. 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). The obligation on the controller to ensuring adequate data protection is linked to the responsibility to verify and demonstrate that the 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 the 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 of employees; setting-up appropriate notification procedures (for instance to indicate when data has 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.

~~84.~~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.

~~85.~~86. Before carrying out the data processing, the controller will have to perform an analysis of its potential impact on the rights and fundamental freedoms of the data subjects. This analysis will also have to take into account the principle of proportionality, on the basis of the comprehensive overview of the processing (that is the entire ~~documentation and~~ description of the processing indicating what personal data will be processed and for which purpose, how it will be collected, how it will be used, internal flows, disclosures, security measures, etc.). In some circumstances, where a processor is involved in addition to the controller, the obligation to perform an analysis of risk 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 analysing the risks would be an advantage and could reduce the administrative burdens linked to this exercise.

~~86.~~87. In order to better guarantee an effective level of protection, data protection requirements (and for instance the related choice of the software to be used with regard to security) should be integrated as early as possible in processing operations, i.e. ideally at the stage of architecture and system design. This objective should apply not only to the technology used for the

processing, but also to the related work and management processes. Easy-to-use functionalities that facilitate compliance with applicable law should be put in place. For example, online access to one's 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). Application and software developers and designers should pay due regard to the principle of data minimisation when setting up the technical requirements for default settings.

~~87.~~88. These additional obligations should be scaled and adapted to the risk at stake, the nature and volume of data processed, the nature, scope and purpose of the processing and the size of the processing entity and should not entail excessive costs. Certain categories of processing, such as processing which does not entail any risk for individuals may be exempt from some ~~or all~~ of the additional obligations prescribed in this Article.

Article 9 – Exceptions and restrictions

~~88.~~89. No exceptions to the principles for protection of personal data are to be allowed. Nevertheless, it is permitted in a strictly restrictive manner, for a limited number of provisions, to allow the benefit of derogations when such derogations are provided for by law and are necessary in a democratic society in the specific cases 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 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.

~~89.~~90. The necessity of such measures needs to be examined 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 which may require exceptions. These exceptions are very specific to avoid giving States unduly wide leeway with regard to the general application of the Convention.

~~90.~~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 State, 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.

~~91.~~92. The term "important economic and financial interests of the State" should be read restrictively and 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.

~~92.~~93. Littera b concerns major interests of private parties, such as those of the data subject himself or herself (for example when vital interests are threatened as the data subject is missing) or of third parties such as freedom of expression and the right to receive and impart information, confidentiality of correspondence and communications, and business or commercial secrecy and other legally protected secrets.

~~93.~~94. ~~In respect of transborder flows of personal data, a specific restriction is allowed on the basis of freedom of expression.~~

~~94.~~95. The third paragraph leaves open the possibility of restricting the rights with regard to certain data processing carried out for statistical or scientific research purposes which pose no risk to the protection of personal data. For instance, 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 possible provided that appropriate data protection safeguards are in place (see paragraph 51).

Article 10 – Sanctions and remedies

~~95.~~96. 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' domestic legislation with corresponding sanctions and remedies.

~~96.~~97. It is left to each Party to determine the nature (civil, administrative, criminal / non judicial) of these sanctions, which 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. Financial compensation for all damages, including moral ones, caused by the processing and class actions could also be considered.

Article 11 – Extended protection

~~97.~~98. 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.~~99. 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.~~100. The purpose of the transborder flow regime is to ensure that information originally processed within the jurisdiction of a Party to the Convention (data collected or stored there for instance), when the processing 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 present Convention. What is important is that data subjects originally concerned by the data processed within the jurisdiction of a Party to the Convention 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, that different protection nevertheless has to be of a quality sufficient to

ensure that human rights are not affected by globalisation and the transborder nature of data flows.

~~100.~~101. 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 are disclosed or made available with the knowledge of the sender, to a recipient subject to the jurisdiction of another State or international organisation.

~~101.~~102. Article 12 only applies to the export of data, not to its import, as for the latter, data is covered by the data protection regime of the recipient Party. However, some problems might arise in case of re-import of data processed abroad in violation of certain provisions of the law of the jurisdiction of origin. In such cases, it will be up to the jurisdiction of origin (the disclosing Party) to take the necessary measures according to Article 12 before export.

~~102.~~103. 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. 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, data flows between Parties should operate freely.

~~103.~~104. 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.~~105. In some cases, 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 the procedures for data transfers to the latter Party is agreed.

~~105. 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.~~

106. Paragraph 2 regulates transborder flows of data to a recipient that is not subject to the jurisdiction of a Party. As for any 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.

~~107. The content of the contracts concerned~~ad hoc or standardised safeguards ~~must include the relevant elements of data protection. Moreover, in procedural terms, 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.~~

107. Both this paragraph and the following one apply to all forms of appropriate protection, whether provided by law or by standardised safeguards. The content of the law ~~concerned~~ must include the relevant elements of data protection. 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~~, in particular~~: the type of data; the purposes and duration of processing for which the data ~~are~~ is transferred; the respect of the rule of law by the country of final destination; the general and sectoral legal rules ~~of law~~ applicable in the State or organisation in question; and the professional and security rules which apply there.

108. 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.~~109. The assessment as to whether there is an appropriate level of protection 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 assessment can similarly be made for a whole State or organisation thereby permitting all data transfers to these destinations. ~~In that case, t~~The appropriate level of protection is determined by the competent supervisory authority of each Party.

~~109.~~110. 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 a 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). They should also be 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. Where massive or repetitive data transfers are involved, provisions of article 12.3 should apply.

111. Paragraph 5 contemplates a complementary safeguard. Namely that the competent supervisory authority be provided with all relevant information concerning the safeguards applying in the case of transfers of data referred to in paragraphs 3.b or the existence of prevailing legitimate interests, and be entitled to request that the ~~quality and~~ effectiveness of the measures taken be demonstrated, and to prohibit, suspend or impose conditions on the transfer where the safeguards are deemed not appropriate. In the particular case of ad hoc safeguards, the competent supervisory authority shall be informed of the modalities of the transfer.

~~110.~~112. In respect of transborder flows of personal data, a specific restriction is allowed on the basis of freedom of expression.

~~111.~~113. Data flows and the related need to increase the protection of personal data also require an increase of international enforcement cooperation among competent supervisory authorities.

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

~~112.~~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 impartial overview, with fast reactive powers and specialised expertise. Such authorities may for instance be a commissioner, a commission, an ombudsman or an inspector general. In order for the data protection supervisory authorities 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.

~~113.~~115. 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 (e.g. federal States). 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 financial, technical and human resources (lawyers, information and communication technologies' specialists) to take prompt and effective action.

~~114.~~116. Parties have a certain discretion as to how to set up the authorities for enabling them to carry out their task. According to the Convention, however, they must have at least the powers of investigation and intervention. Further, 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, issue decisions and impose administrative sanctions, 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.

~~115.~~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 domestic law.

~~116.~~118. The supervisory authority's power of intervention 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 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 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 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.

~~117.~~119. 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 controllers and processors about the rights and obligations concerning data protection.

~~118.~~120. Moreover, 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, 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 with the power to do so. 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.

~~119.~~121. Where an administrative decision produces legal effects, every affected person 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.

~~120.~~122. 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 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.~~123. 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. 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. The authority could keep a data processing register open to the public.

~~122.~~124. In addition to the consultation foreseen under Article 12bis 2~~a~~bis~~'~~, 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.

~~123.~~125. 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; or the adoption of decisions without being subject to external orders or injunctions.

124.126. 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.

125.127. 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. The supervisory authority should have the power to inform the public through regular reports, the publication of opinions or any other means of communication and to issue publicly recommendations to the head of State, government and Parliament in order to improve the data protection system.

126.128. 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.

127.129. 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.

128.130. Strengthening co-operation between the supervisory authorities would contribute to the development of the level of protection afforded by the Parties 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 persons concerned. With increasing frequency persons 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. Some examples are the development of international electronic networks and increasing cross-border flows in the service industries and the work environment. In such a context, international co-operation between supervisory authorities ensures that persons 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

129.131. The supervisory authorities will render each other general assistance for controls *a priori* 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.

Article 14 ~~(deleted)~~

~~130.~~ Paragraph 1 ensures that data subjects residing abroad, whether in a Contracting State or in a third country will be enabled to exercise their rights recognised at article 8 of the Convention.

~~131.~~132. . According to paragraph 2, where the data subject resides in another Contracting State he is given the option to pursue his rights either directly in the country where information relating to him is processed, or indirectly, through the intermediary of that country's designated authority.

~~132.~~133. 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.

~~133.~~134. Paragraph 3 specifies in order to expedite the procedure, that requests be as specific as possible.

Article 15 – Safeguards concerning assistance

~~134.~~135. 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.

~~135.~~136. This provision is of fundamental importance for mutual trust, on which mutual assistance is based.

Article 16 – Refusal of requests for assistance

~~136.~~137. 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.

~~137.~~138. 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

~~138.~~139. The provisions of this Article are analogous to those found in other international conventions on mutual assistance.

~~139.~~140. "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.

~~140.~~141. 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

~~141.~~142. The purpose of Articles 18, 19 and 20 is to facilitate the effective application of the Convention and, where necessary, to perfect it.

~~142.~~143. A Convention Committee is composed of representatives of all Parties, from the national supervisory authorities or from the government.

~~143.~~144. 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.

~~144.~~145. 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).

~~145.~~146. 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).

~~146.~~147. 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).

~~147.~~148. 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.

~~148.~~149. Furthermore, the Convention Committee will be entitled to approve models of standardised safeguards for data transfers (Article 19 littera g).

~~149.~~150. 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

~~150.~~151. The Committee of Ministers, which adopted the original text of this Convention, is also competent to approve any amendments.

~~151.~~152. 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).

~~152.~~153. 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

~~153.~~154. 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

~~154.~~155. The Convention, which was 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.

~~155.~~156. Considering the frontierless 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

~~156.~~157. 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

~~157.~~158. 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

~~158.~~159. 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

~~159.~~160. These provisions are in conformity with the customary final clauses contained in other conventions of the Council of Europe.