COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 15 June 2012

T-PD (2012)04Mos

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

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL (T-PD)

Final document on the modernisation of Convention 108

Document final sur la modernisation de la Convention 108

DG I – Human Rights and Rule of Law / Droits de l'Homme et État de droit

TABLE OF CONTENTS /
TABLE DES MATIERES

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 T-PD immediately commissioned a report[1] to scientific experts with a view to identifying the 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 states.

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 containing 30 questions was prepared.

Those 30 questions[3] 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.

---

[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.

[3] http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf

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 into concrete modernisation proposals 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[4] of the modernisation proposals were prepared by the Bureau of the T-PD early 2012, the latest version of which is dated 27 April 2012 (T-PD-BUR(2012)01Rev2) and will be examined at the 28th Plenary meeting of the T-PD (19-22 June 2012). This latest version was 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 (on the occasion of an exchange of views held on 2 May 2012 in the Council of Europe premises in Brussels).

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 follow-up mechanism.

A broad consensus clearly emerged from the contributions made to the 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 the legal framework of the European Union 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" 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*

[4] Documents T-PD-BUR(2012)01Rev of 5 March 2012 and T-PD-BUR(2012)01 of 18 January 2012.

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.

Consistency between the modernisation proposals and the corresponding provisions of the legislative proposals issued by the European Commission on 25 January 2012 (a draft Regulation setting out a general EU framework for data protection and a draft Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities) will have to be sought and carefully considered.

Concerning transborder data flows, both regimes should in the future be articulated in order to better contribute to the free flow of data and 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 assessing the adequacy of the level of protection of a particular country (Article 41.2.c of the draft Regulation).

The modernisation proposals are based on the current article 12 of the Convention and Article 2 of the Additional protocol. The current article 12 already secures free flow of data between Parties presumed to provide an adequate level of protection (the explanatory report specifies that obstacles to transborder data flows are not permitted between Parties, which, "having subscribed to the common core of data protection provisions set out in Chapter II, offer a certain minimum level of protection"). Furthermore, the possibility for the Committee to conclude that the level of data protection provided by a Party is not adequate (thus impacting on the free flow of data) has been introduced.

Organisation for Economic Co-operation and Development (OECD)

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 current 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 flexible approach of the APEC Privacy Framework and its recent Cross-Border Privacy Rules system was considered, in particular when reflecting on modernising the transborder data flows provisions and similarities between both frameworks, where applicable, were acknowledged, underlining the need of greater articulation of the various systems.

Timeframe and procedure

The 28th Plenary of the T-PD (19-22 June 2012) is expected to review the modernisation proposals in second reading, possibly reaching an agreement on those proposals and transmitting them to the Committee of Ministers during the second semester of 2012.

The Committee of Ministers would then consider the modernisation proposals and decide on the subsequent steps, noting the high possibility that it may decide to give terms of reference to an ad hoc committee which would enable political discussions by governmental representatives of the 47 member states of the Council of Europe as well as representatives of other interested countries (observers to the Council of Europe, observers to the T-PD, etc) to finalise the draft legal instrument. A formal mandate of negotiation given to the European Commission could at that stage guarantee consistency of the modernisation proposals and EU proposals.

II. LATEST MODERNISATION PROPOSALS (27/04) /

DERNIERES PROPOSITIONS DE MODERNISATION (27/04)

PROPOSALS
Title : Convention for the Protection of Individuals with Regard to the Processing of Personal Data
Preamble
The **signatories** of this Convention,
Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;
Considering that it is **necessary**, **given the increase in and diversification of processing and exchanges of personal data, to guarantee the dignity and** protection of fundamental **rights and** freedoms of every person, **in particular through the right to control one's own data and the use made of them.** *Explanatory report will underline that human dignity implies that individuals can not be treated as objects and be submitted to machines, and consequently that decisions based solely on the grounds of an automated processing of data can not be made without individuals having the right to express their views.*
Recognising that the right to data protection is to be considered in respect of its role in society and that it has to be reconciled with the other human rights and fundamental freedoms, including the freedom of expression; Recognising that it is necessary to promote at the global level the fundamental values of respect for privacy and data protection, thereby contributing to the free flow of information between peoples;

Recognising that this Convention is to be interpreted with due regard to its explanatory report,
The Explanatory Report will refer to the Madrid Resolution.
Have agreed as follows:
Chapter I – General provisions
Article 1 – Object and purpose
The purpose of this Convention is to secure for every individual, **subject to the jurisdiction of the Parties**, whatever their nationality or residence, **the right to the protection of personal data, thus ensuring the** respect for their rights and fundamental freedoms, and in particular **their** right to privacy, with regard to the processing of their personal data.
Article 2 – Definitions
For the purposes of this Convention:
a "personal data" means any information relating to an identified or identifiable individual ("data subject"); *Make an addition to the Explanatory Report, specifying in particular that an individual is not considered "identifiable" if identification requires unreasonable time or effort for the controller or for any person from whom the controller could reasonably obtain the identification.* *Also specify that "identifiable" does not only refer to the individual's civil identity but also to what allows to "individualise" one person amongst others.* b (c) "data processing" means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data;

where no automated processing is used, data processing means the operations carried out on personal data organised in a structured manner according to specified criteria allowing search by person concerned;
c (d) “controller” means the natural or legal person, public authority, agency or any other body which alone or jointly with others has the decision-making power with respect to data processing. *In the explanatory report, specify that ‘decision-making power’ covers the purposes and conditions of processing, the means used for the data processing, as well as the reasons justifying the processing and the choice of data to be processed.*
d (e) “recipient” shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed or made available;
e (f) “processor“ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; *In the Explanatory Memorandum indicate that this does not apply to the employees of the controller.*
Article 3 – Scope
1 Each Party undertakes to apply this Convention to data processing carried out by any controller subject to its jurisdiction. 1bis This Convention shall not apply to data processing carried out by a natural person for the exercise of purely personal or household activities, unless the data are made accessible to persons outside the personal or household sphere. 1ter Any Party may decide to apply this Convention to information on legal persons.

In the explanatory report, specify what is meant by the exercise of purely personal or household activities, and making accessible to persons outside the personal or household sphere (to be illustrated according to several criteria, including notably the indefinite number of persons of the CJUE judgement in the Lindqvist case). Also cover services and products offered in the context of domestic activities (if the service provider acts for his/herself or for a third party with respect for data which has been provided to him/her, in other words if it goes beyond what is necessary in terms of the service offered, he/she begins a processing of data. If he/she is within the jurisdiction of a Party to the Convention, he/she will be subject to the data protection law of that Party). *Specify that while the processing concerns data of natural persons, the Parties nevertheless have the possibility to extend the protection to legal persons.*
Chapter II – Basic principles for data protection
Article 4 – Duties of the Parties
1 Each Party shall take the necessary measures in its domestic law to give effect to the provisions set out in **this Convention.** 2 These measures shall be taken by each Party prior to ratification or accession to this Convention.
3 Each Party undertakes to allow the Conventional Committee foreseen in Chapter V to evaluate the observance of its engagements and to contribute actively to this evaluation.
Article 5 – Legitimacy of data processing and quality of data

1 Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect a fair balance between the public or private interests, rights and freedoms at stake. *The Explanatory Report will underline that data processing must be proportionate, that is to say, appropriate in relation to the legitimate aims pursued, necessary in the sense that there are no other appropriate and less intrusive measures with regard to the interests, rights and freedoms of data subjects or society, and it should not lead to a disproportionate interference with these interests, rights and freedoms in relation to the benefits expected from the controller.*
2 Each Party shall provide that data processing can be carried out only if: a. the data subject has freely given his/her explicit, specific and informed consent, or b. this processing is provided by domestic law for an overriding legitimate interest or is necessary to comply with legal obligations or contractual obligations binding the data subject; T*he Explanatory Report will explain the meaning of overriding legitimate interest (including by taking the examples of Section 7 of the Directive 95/46/CE) and that consent may be withdrawn.*
3 Personal data undergoing ~~automatic~~ processing shall be :
a ~~obtained and~~ processed lawfully and fairly.
b **collected** for **explicit**, specified and legitimate purposes and not **processed** in a way incompatible with those purposes**;** The *Explanatory Report will give examples of compatible purposes (statistics, historical or scientific research purposes that are a priori compatible provided that other safeguards exist and that the processing is not the ground for a decision to be taken concerning the data subject).*

c adequate, relevant, not excessive and limited to the strict minimum in relation to the purposes for which they are **processed**;
d accurate and, where necessary, kept up to date;
e preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are **processed**.
Article 6 – Processing of sensitive data
1 The processing of certain categories of personal data shall be prohibited, whether such data are sensitive: by their nature, namely genetic data, data related to health or sexual life, data related to criminal offences or convictions, or security measures; by the use made of them, namely biometric data, data whose processing reveals racial origin, political opinions [or trade-union membership], religious or other beliefs, or; where their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination. 2 Such data may nevertheless be processed where domestic law provides appropriate safeguards. The *Explanatory Report will explain that "serious risk" includes injury to dignity or to physical integrity, "genetic data" means all data concerning the hereditary characteristics of an individual or characteristics acquired during early prenatal development, "biometric data" means all data concerning the physical, biological of physiological characteristics of an individual that allow his/her unique identification.*
Article 7 – Data security

1 Every Party shall provide that the controller, and, where applicable the processor, takes the appropriate security measures against accidental or unauthorised modification, loss or destruction ~~accidental~~, as well as against unauthorised access or dissemination of personal data processed.
2 Each Party shall provide that the controller shall notify, without delay, at least the supervisory authorities within the meaning of Article 12 bis of this Convention of any violation of data which may seriously interfere with the fundamental rights and freedoms of the data subject. *The Explanatory Report will specify that the controller should be encouraged to also notify, where necessary, the data subjects.*
Article 7bis – Transparency of processing
1. Each Party shall provide that every controller must ensure the transparency of data processing and in particular provide data subjects with information concerning at least his/her identity and habitual residence or establishment, the purposes of the processing carried out by him/her, the data processed, the recipients of the personal data, the preservation period and the means of exercising the rights set forth in Article 8, as well as any other information necessary to ensure a fair data processing.

2. The controller shall nonetheless not be required to provide such information where this proves to be impossible or involves disproportionate efforts. The *Explanatory Report will specify when the information should be given, that the information should be direct, readable etc, and that "any other information necessary to ensure a fair data processing" notably includes information on transfers to other countries.* *The information should also include measures taken to guarantee data protection in the context of transfers to countries which do not have an adequate system of data protection.* *The collection of personal data includes both direct and indirect collection. The information regarding the recipients may also refer to categories of recipients.*
Article 8 – Rights of the data subject
Any person shall be entitled on request:
a not to be subject to a decision significantly affecting him/her or producing legal effects relating to him/her, based solely on the grounds of an automatic processing of data without having the right to express his/her views;
b to object at any time for legitimate reasons to the processing of personal data concerning him/her;
c to obtain at reasonable intervals and without excessive delay or expense confirmation or not of the existence of data processing relating to him/her, the communication in an intelligible form of the data processed, **all available information on their origin as well as any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7bis;** **d to obtain knowledge of the reasoning underlying in the data processing, the results of which are applied to him/her ;**

Explanatory Report: this right can, in accordance with Article 9, be limited where this is necessary in a democratic society, in order to protect "legally protected secrets".
e (c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;
f (e) to have a remedy if no response is given to a request for confirmation, communication, rectification, erasure or to an objection, as referred to in this Article;
g (f) to benefit, whatever his/her residence, from the assistance of a supervisory authority within the meaning of Article 12 bis, in exercising the rights provided by this Convention. *Explanatory report: 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.*
Article 8bis – Additional obligations

1- Each Party shall provide that the controller is responsible for ensuring respect for the right to the protection of personal data at all stages of the processing and for taking all appropriate measures to implement the domestic legal provisions giving effect to the principles and obligations of this Convention.

2- The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the foreseen data processing on the rights and fundamental freedoms of the data subject.

3- The controller, or where applicable the processor, shall design data processing operations in such a way as to prevent or at least minimise the risk of interference with the right to the protection of personal data.

4- The controller shall establish internal mechanisms to verify and demonstrate to the data subjects and to the supervisory authorities provided for in Article 12 bis of this Convention the compliance of the data processing for which he/she is responsible with the applicable law.

5- Each Party shall provide that the products and services intended for the data processing shall take into account the implications of data protection from the stage of their design and include easy-to-use functionalities allowing the compliance of the processing with the applicable law to be ensured.

6- The obligations included in the domestic law on the basis of the provisions of the previous paragraphs may be adapted according to the size of the controller, or where applicable the processor, the volume of data processed and the risks for the interests, rights and fundamental freedoms of the data subjects.

The Explanatory Report will specify that one of the possible measures could consist of the designation of a 'data protection officers' entrusted with the means necessary to fulfil its mission independently and of whose designation the supervisory authority has been informed. They can be internal or external to the controller.

Article 9 – Exceptions and restrictions
1 No exception to the basic principles expressed in this Chapter shall be allowed, except to the provisions of Articles 5.3 , 6, 7.2, 7bis and 8 when such derogation is provided for by law and constitutes a necessary measure in a democratic society to: *Explanatory Report: a measure shall be considered as "necessary in a democratic society" to pursue a legitimate aim if it meets a "pressing social need" which cannot be achieved by less intrusive means and, especially, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it appear "relevant and sufficient".*
a protect State security, public security, the economic and financial interests of the State or the prevention and suppression of criminal offences; *The Explanatory Report will clarify by means of examples the scope of the provision, referring to the confidentiality of communications and business or commercial secrecy and other legally protected secrets.*
b protect the data subject or the rights and freedoms of others, **notably freedom of expression and information**. *The Explanatory Report will specify that this provision concerns data processing carried out solely for communicating information to the public, ideas or opinions of general interest, or for literary or artistic expression.*
2 Restrictions on the exercise of the provisions specified in Articles **6, 7bis and** 8 may be provided by law with respect to ~~personal~~ data processing for statistical purposes or for the purposes of scientific research, when there is obviously no risk of an infringement **of the rights and freedoms** of the data subjects.
Article 10 – Sanctions and remedies

Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of domestic law giving effect to the provisions of this Convention.
Article 11 Extended protection
None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.
Chapter III – Transborder data flows
Article 12
1 Each Party shall ensure that personal data will only be disclosed or made available to a recipient who is not subject to its jurisdiction on condition that an adequate level of data protection is ensured.
2 When the recipient is subject to the jurisdiction of a Party to the Convention, the law applicable to this recipient is presumed to provide an adequate level of protection and a Party shall not, for the sole purpose of data protection, prohibit or subject to special authorisation the disclosure or making available of data. The Conventional Committee may nevertheless conclude that the level of protection is not adequate.

3 When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to the Convention, an adequate level of protection can be ensured by: a) the law of that State or organisation, in particular by applicable international treaties or agreements, or b) standardised or ad hoc legal measures, such as contract clauses, internal rules or similar measures that are binding, effective and capable of effective remedies, implemented by the person who discloses or makes personal data accessible and by the recipient. The competent supervisory authority within the meaning of Article 12 bis of the Convention [shall] [may] be informed of the ad hoc measures implemented and may request that the person who discloses or makes data available, or the recipient, demonstrate the quality and effectiveness of actions taken. This authority may suspend, prohibit or subject to condition the disclosure or making available of data.
4. Notwithstanding paragraphs 2 and 3 , each Party may provide that the disclosure or making available of data may take place without the law applicable to the recipient ensuring, for the purposes of this Convention, an adequate level of protection of data subjects, if in a particular case: a) the data subject has given his/her specific, free and explicit consent, after being informed of risks arising in the absence of appropriate safeguards, or b) the specific interests of the data subject require it in the particular case, or c) legitimate interests protected by law and meeting the criteria of Article 9, prevail.
5. The competent supervisory authority within the meaning of Article 12 bis of the Convention, may suspend, prohibit or subject to condition the disclosure or making available of data within the meaning of Articles 12.3.b and 12.4.
6. Each Party may foresee in its domestic law derogations to the provisions set out in this Chapter, providing they constitute a measure necessary in a democratic society to protection of freedom of expression and information.

Chapter III bis Supervisory authorities
Article 12bis Supervisory authorities
1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles **of this Convention**.
2 To this end, such authorities: a. are responsible for raising awareness of and providing information on data protection; b. have, in particular, powers of investigation and intervention; c. may pronounce decisions necessary with respect to domestic law measures giving effect to the provisions of this Convention and in particular to sanction administrative offences; d. are able to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the provisions **of this Convention**. *The Explanatory report will note that the powers of intervention should notably concern data processing which presents particular risks for rights and fundamental freedoms.*
3 Each supervisory authority can be seized by any person concerning the protection of his/her rights and fundamental freedoms with regard to the data processing ~~of personal data~~ within its competence and shall inform the data subject of the follow-up given to such a claim.
4 The supervisory authorities shall **accomplish their duties and exercise their powers** in complete independence. **They shall neither seek nor accept instructions from anyone.**
5 Each Party shall ensure that the supervisory authorities have adequate human, technical and financial resources and infrastructure necessary to accomplish their mission and exercise their powers autonomously and effectively.
6 Decisions of the supervisory authorities which give rise to complaints shall be subject to judicial remedies.

7 In accordance with the provisions of Chapter IV, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by:
a exchanging all useful information, in particular by taking, under their domestic law and solely for the protection of personal data, all appropriate measures to provide factual information relating to specific processing carried out on its territory, with the exception of personal data undergoing this processing, unless such data is essential for co-operation or that the data subject has previously explicitly agreed to; b coordinating their investigations or interventions or conducting joint actions; c providing information on their law and administrative practice in data protection.
8 In order to organise their co-operation and to perform the duties set forth in the preceding paragraph, the supervisory authorities of the Parties shall form a conference.
9 The supervisory authorities shall not be competent with respect to processing carried out by judicial bodies in the exercise of their judicial functions.
Chapter IV – Mutual assistance
Article 13 – Co-operation between Parties
1 The Parties agree to render each other mutual assistance in order to implement this Convention.
2 For that purpose:
a each Party shall designate one or more **supervisory** authorities within the meaning of Article 12bis of this Convention, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;
b each Party which has designated more than one **supervisory** authority shall specify in its communication referred to in the previous sub-paragraph the competence of each ~~authority.~~

Article 14 – Assistance to data subjects resident abroad
delete
Article 15 – Safeguards concerning assistance rendered by designated supervisory authorities
1 A **supervisory** authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.
2 Each Party shall see to it that the persons belonging to or acting on behalf of **the designated supervisory** authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.
3 In no case may a designated **supervisory** authority be allowed to make ~~under Article 14, paragraph 2,~~ a request for assistance on behalf of a data subject ~~[resident abroad~~], of its own accord and without the express consent of the person concerned.
Article 16 – Refusal of requests for assistance
A designated **supervisory** authority to which a request for assistance is addressed under Articles 13 ~~or 14~~ of this Convention may not refuse to comply with it unless:
a the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;
b the request does not comply with the provisions of this Convention;
c compliance with the request would be incompatible with the sovereignty, security or public policy (ordre public) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.
Article 17 – Costs and procedures of assistance

1 Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects [~~abroad~~] under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the **supervisory** authority making the request for assistance.
2 The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party. 3 Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.
Chapter V – Conventional Committee
Article 18 – Composition of the committee
1 A **Conventional** Committee shall be set up after the entry into force of this Convention. 2 Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the committee by an observer. 3 The **Conventional** Committee may, by a decision taken by **a majority of two-thirds of its representatives [voting] [entitled to vote]**, invite **an observer to be represented at its meetings**.
4 Any Party which is not member of the Council of Europe shall contribute to the funding of the activities of the **Conventional** Committee according to the modalities established by the Committee of Ministers in agreement with that Party.
Article 19 – Functions of the committee
The **Conventional** Committee:

a may make **recommendations** with a view to facilitating or improving the application of the Convention;
b may make proposals for amendment of this Convention in accordance with Article 21;
c shall formulate its opinion on any proposal for amendment of this Convention which is referred to it in accordance with Article 21, paragraph 3;
d may~~, at the request of a Party,~~ express an opinion on any question concerning the **interpretation or** application of this Convention;
e prepares, before any new accession to the Convention, an opinion for the Committee of Ministers relating to the level of data protection of the candidate for accession;
f may, at the request of a State or an international organisation, evaluate whether the rules of its domestic law ensure an adequate level of protection for the purposes of this Convention;
g may develop models of standardised legal measures referred to in Article 12;
h [periodically] reviews the implementation of this Convention by the Parties in accordance with the provisions of Article 4.3;
i provides its opinion on the adequate level of data protection foreseen by the provisions of paragraphs 2 and 3 of Article 12;
j does whatever is needful to facilitate a friendly settlement of any difficulty which may arise out of the implementation of this Convention.
Article 20 – Procedure 1 The **Conventional** Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once a year and in any case when one-third of the representatives of the Parties request its convocation.
2 A majority of representatives of the Parties shall constitute a quorum for a meeting of the **Conventional** Committee.

3 Every Party has a right to vote. Each State which is a Party to the Convention shall have one vote. On questions related to its competence, the European Union exercises its right to vote and casts a number of votes equal to the number of its member States that are Parties to the Convention and have transferred competencies to the European Union in the field concerned. In this case, those member States of the European Union do not vote. When the Committee acts according to provisions of litera (h), (i) and (j) of Article 19, however, both the European Union and its Member States vote. The European Union does not vote when a question which does not fall within its competence is examined.
4 After each of its meetings, the **Conventional** Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the Convention.
5. Subject to the provisions of this Convention, the **Conventional** Committee shall draw up its own Rules of Procedure and establish the procedure for the examination of the adequate level of protection.
Chapter VI – Amendments
Article 21 – Amendments
1 Amendments to this Convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the **Conventional** Committee.
2 Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the **Parties to the Convention, to the other** member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this Convention in accordance with the provisions of Article 23.
3 Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the **Conventional** Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.

4 The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the **Conventional** Committee and may approve the amendment.
5 The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance. 6 Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.
7. The Committee of Ministers may, however, after consulting the Conventional Committee, decide that a particular amendment shall enter into force at the expiration of a period of two years from the date on which it has been opened to acceptance, unless a Party notifies the Secretary General of the Council of Europe of an objection to its entry into force. If such an objection is notified, the amendment shall enter into force on the first day of the month following the date on which the Party to the Convention which has notified the objection has deposited its instrument of acceptance with the Secretary General of the Council Europe.
8. If an amendment has been approved by the Committee of Ministers but has not yet entered into force in accordance with the provisions set out in paragraphs 6 or 7, a State or the European Union may not express its consent to be bound by the Convention without at the same time accepting the amendment.
Chapter VII – Final clauses
Article 22 – Entry into force
1 This Convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the Convention in accordance with the provisions of the preceding paragraph.
3 In respect of any member State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of ratification, acceptance or approval.
Article 23 – Accession by non-member States or the European Union
1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may, **in light of the opinion prepared by the Conventional Committee in accordance with Article 19.e,** invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee**.**
2 In respect of any **new Party,** the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.
3 The European Union as well as States not members of the Council of Europe which have taken part in the drafting of the amending Protocol can accede to the Convention without prior invitation from the Committee of Ministers.
Article 24 – Territorial clause
1 Any State **or the European Union** may may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State **or the European Union** may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.
3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.
Article 25 – Reservations
No reservation may be made in respect of the provisions of this Convention.
Article 26 – Denunciation
1 Any Party may at any time denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
2 Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.
Article 27 – Notifications
The Secretary General of the Council of Europe shall notify the member States of the Council and **any Party** to this Convention:
a any signature;
b the deposit of any instrument of ratification, acceptance, approval or accession;
c any date of entry into force of this Convention in accordance with Articles 22, 23 and 24;

d any other act, notification or communication relating to this Convention.

III. DRAFT ELEMENTS FOR THE EXPLANATORY REPORT / *PROJET D'ELEMENTS POUR LE RAPPORT EXPLICATIF*

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, 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 modernisation work was carried out taking duly account of other relevant normative work such as the "International Standards on the Protection of Privacy with regard to the processing of Personal Data" (which were welcomed by the 31st International Conference of Data Protection and Privacy Commissioners, held in Madrid on 5 November 2009), the review of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the EU reform package issued by the European Commission on 25 January 2012 and the APEC Privacy framework.

4. The Consultative Committee set up by virtue of Article 18 of the Convention prepared this draft [Protocol] at its 28th meeting held from 19 to 22 June 2012 [...]. It was submitted to the Committee of Ministers. [...]

5. 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 facilitate the application of the provisions contained therein. This Protocol has been open for signature in ..., on ... .

Preamble

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

7. 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 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 express their views.

8. Taking into account the role of data protection in the society, the preamble underlines that the different rights and interests of individuals have 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.

9. The Convention, through the rights it lays down and values it protects, contributes to the free flow of information, which importance is to be underlined in particular as global information flows are an important societal feature, enabling the exercise of fundamental rights and freedoms. Data protection should in no circumstances be interpreted as a means to erect barriers to information flows, to restrain the exchange of information or constrain innovation.

Chapter I – General provisions

Article 1 – Object and purpose

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

11. 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.

12. The protection will apply on the basis of the notion of 'jurisdiction' of the Parties, in order to aligning the geographical scope of the Convention to that of the European Convention on Human Rights (more specifically its Article 8) as well as to better stand the test of time and continual technological developments.

13. The introduction of the concept of jurisdiction does not alter the validity of referring to the notion of territory when regulating transborder flows of data as in that context, the criterion of territory is a simple one : the recipient of the data merely needs to be located in order to ascertain whether the flow is permitted.

14. Finally, this article focuses on the right to the protection of personal data, which 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" and as subsequently enshrined as a fundamental right in Article 8 of the Charter of Fundamental Rights of the EU. The right to the protection of personal data is not an isolated right but an enabling one, without the 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

15. Definitions used in this Convention are meant to cover, where necessary, different terms or concepts used in national legislation to express certain fundamental concepts.

Litt. a – 'personal data':

16. "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 person from whom the controller could reasonably obtain the identification. The notion of 'identifiable' does not only refer to the individual's civil identity but also to what allows to "individualise" one person amongst others, such as an identification number.

17. 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 (unaccompanied by 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 discover the identity of the person concerned. Where this is a possibility, the data may not be considered to be genuinely anonymous and must therefore be protected.

18. 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

19. "Data processing" is an open-ended definition capable of flexible interpretation which starts from the collection of data and covers automated processes as well as 'manual' processing organised in a structured manner allowing to search by particular person.

Litt. c

20. "Controller" means only the person or body ultimately responsible for the file, who has the decision-making power concerning the purposes and conditions of the processing, the means used for the data processing, as well as the reasons justifying the processing and the choice of data to be processed. Persons who carry out the operations according to the instructions given by the controller are not covered by this definition.

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

Litt. d

22. "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.

Litt. e

23. "Processor" does not cover the employees of the controller and cases where the processing is carried out in a different manner than what was requested by the controller.

24. It should also be specified that the notion of 'law' in the Convention encompasses statute law, including the Constitutions, legislative acts and enactments of lower rank than statutes, as well as case law.

Article 3 – Scope

25. According to *paragraph 1,* the Convention is to be applied by the Parties to all processing - by public or private sector alike - carried out by a controller subject to the jurisdiction of the concerned Party. Although most transborder data flows occur in the private sector, the convention is nevertheless of great importance for the public sector and Parties to the Convention have to apply data protection principles even when they process public files – as is usually the case – entirely within their national borders.

26. *Paragraph 1bis* excludes from the scope of the Convention processing carried out for purely personal or household activities. This exclusion carefully considers the potential impact of the use of social networks, blogs etc. as in this particular context, it is proposed to fully apply the Convention whenever personal data is accessible to persons outside the personal or domestic sphere.

27. 'Purely personal or household activities' are to be illustrated according to several criteria, including notably the 'indefinite number of persons' criteria used by the Court of Justice of the European Union in the Lindqvist case, as well as in the Pammer and Alpenhof cases, and with leading decisions of national courts dealing with Internet jurisdiction.

28. Services and products offered in the context of domestic activities are also excluded but where the service provider acts for his/herself (or for a third party) exceeding what is necessary in terms of the service offered, the exclusion is not applicable.

29. While the processing concerns data of natural persons, the Parties nevertheless have the possibility to extend the protection to legal persons.

Chapter II – Basic principles of data protection

Article 4 – Duties of the Parties

30. 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.

31. The "measures within its domestic law" can take different forms, depending on the legal and constitutional system of the State concerned: apart from laws they may be regulations, administrative guidelines, etc. 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.

32. It is further stipulated that the measures giving effect to the convention should be taken by the countries concerned prior to 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 an adequate level in the field of data protection.

33. Parties commit to contribute actively to the evaluation of the compliance of their own system with their undertakings, with a view to ensuring regular assessment of the effectiveness and implementation of the principles of the Convention.

Article 5 – Legitimacy of data processing and quality of data

34. The way in which the legitimate purpose is specified may vary in accordance with national legislation but generally aims at ensuring that a balancing of interests be made, i.e. between the legitimate interests of the data subject and the interest of the controller. Where the purpose of a processing will be determined by law, its legitimacy will be presumed. The proposed wording corresponds to the case-law of the European Court of Human Rights, which requires a fair balance between the competing public and private interests (S. and Marper v UK [2008], § 118).

35. Data processing must be proportionate, that is, appropriate in relation to the legitimate aims pursued and necessary in the sense that there are no 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 the benefits expected by the controller.

36. The reference to "purpose" indicates that it should not be allowed to store data for undefined purposes, on the contrary, the particular purpose of the processing should be very carefully specified.

37. Paragraph 2 prescribes two alternative essential pre-requisites to a lawful processing : the individual's consent or legal requirements in the case of an overriding legitimate interest, as well as to satisfy legal or contractual obligations binding the data subject.

38. Overriding legitimate interests may prevail for instance when protecting the vital interests of the data subject or carrying out a processing in the public interest.

39. The data subject's consent must be freely given, explicit, specific and informed : no influence or pressure, whether direct or indirect, can be exercised on the data subject, who must be fully aware of the implications of this decision, and have been adequately informed in order to do so.

40. The data subject has the right to withdraw a given consent at any time, which will not affect the lawfulness of processing before its withdrawal.

41. Paragraph 3 prescribes the quality – or rather qualities – of both the processing (which should be lawful and fair) and of the data processed. The quality of data relies on the validity of a number of pre-requisites applicable to the collection phase : 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.

42. Statistics, historical or scientific research purposes are *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.

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

44. The requirement that data be not excessive in relation to the purposes for which they are processed reflects the data minimisation principle : 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 strict minimum.

45. The requirement concerning the time-limits for the storage of data in their name-linked form does not mean that data should after some time be irrevocably separated from the name of the person to whom they relate, but only that it should not be possible to link readily the data and the identifiers.

Article 6 – Processing of sensitive data

46. Data processing of 'sensitive' data, i.e. certain types of data, or a certain use of a data processing, may be harmful to persons and are to be forbidden as they are likely to lead to encroachments on individual rights and interests.

47. Data which are sensitive by nature are genetic data (data concerning the hereditary characteristics of an individual or characteristics acquired during early prenatal development), data related to health (which 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, healthy or deceased) or sexual life, data related to criminal offences or convictions (based on criminal law and in the framework of a criminal procedure) or security measures.

48. Data – which is not necessarily sensitive by nature - can be sensitive according to the purpose of the processing which will be made of it. Such is for instance the case of biometric data (all data concerning the physical, biological of physiological characteristics of an individual that allow his/her unique identification). Not all biometric data are sensitive by nature, but may, depending on the use made of it threaten individual rights and interests.

49. Some processing may also present a serious risk to the interests, rights and fundamental freedoms of individuals, notably a risk of discrimination or of injury to an individual's dignity or physical integrity and should also be forbidden.

50. The list of this article is not meant to be exhaustive. A Contracting State may, in conformity with Article 11, include in its domestic law other categories of sensitive data, the processing of which is prescribed or restricted. The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned.

51. Processing of such sensitive data may be possible, when the domestic law provides appropriate safeguards, such as the data subject's consent or a statutory regulation of the intended process ensuring the confidentiality of the data processed.

Article 7 – Data security

52. Security measures are to be applied to the data as well as to the processing.

53. There should be specific security measures for each processing, taking into account its degree of vulnerability, the need to restrict access to the information within the organisation, requirements concerning long-term storage, and so forth. The security measures must be appropriate, i.e. adapted to the specific function of the processing and the risks involved.

54. 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.

55. While security measures are aimed at preventing a number of risks, paragraph 2 contains a specific obligation occurring *ex post facto*, where a violation of data has occurred and may seriously interfere with the fundamental rights and freedoms of the individual. Where such a violation has occurred, the controller is requested to notify the supervisory authorities of the security breach, and should be encouraged to notify, where necessary, the data subjects in order to enable them to take the necessary measures.

Article 7bis – Transparency

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

57. Several elements of information have to be provided by the controller to the data subjects when collecting their data, and should be direct, readable and adapted to them. Any information proving to be necessary to ensure a fair data processing, such as for instance information on data transfers to a foreign country and measures taken by the controller to guarantee an adequate level of data protection in that country which does not provide any data protection regime, also have to be provided.

58. Paragraph 2 exempts the controller to provide the information listed in paragraph 1 where this proves to be impossible or involves disproportionate efforts. Such an impossibility can both be of a legal nature (in the context of a criminal investigation for instance) or of a material nature.

Article 8 – Rights of the data subject

59. The provisions set out in this article are designed to enable a data subject to exercise and defend his or her rights. Although in domestic legislation the contents of Article 8 clearly correspond to subjective rights, the present text expresses them in the form of safeguards which Contracting States offer to data subjects, in view of the non self-executing character of the convention.

60. These safeguards include the following main elements:

– right to express one's views on the consequences of a purely automated decision;
– right to object to a processing;
– knowledge about the existence of a processing and about the contents of the information;
– knowledge about the reasoning of the processing;
– rectification of erasure of data;
– right to a remedy if any of the previous elements are not respected;
– assistance of a supervisory authority.

61. 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 States this will be the controller, but in some States this right is exercised through the intermediary of the supervisory authority.

62. The wording of littera c is intended to cover various formulas followed by national legislation: communication at the request of the data subject or at the initiative of the controller; communication free of charge at fixed intervals as well as communication against payment at any other time, etc. 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.

63. Littera d sets out the right to be informed of the reasoning of the processing, right which can, in accordance with Article 9, be limited where this is necessary in a democratic society, in particular to protect the rights of others, such as "legally protected secrets" (for instance trade secrets or the intellectual property or copyright protecting a software). The right to know the reasoning of the processing is even more essential in the case of automated decision-making.

64. In the case of rectifications obtained in conformity with the principle set out in littera e, national law or practice provides usually that, where appropriate, those rectifications should be brought to the recipients of the original information.

65. 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.

66. 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.e), coupled with an effective right of opposition 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

67. 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. Those obligations are meant to enable them to drive and demonstrate their compliance with the applicable provisions, thereby enhancing trust. The controller will notably have to take the appropriate measures to implement such provisions, and to demonstrate such compliance. This obligation is to be applied at all stages of the processing, including the designing phase.

68. Before carrying out a processing, an analysis of the impact of such a processing on the rights and fundamental freedom of the data subject will have to be made. 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.

69. 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.

70. 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. One of the possible measures 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 and of. Such a data protection officer, whose designation has been notified to the supervisory authority, can be internal or external to the controller.

71. Those additional obligations have to be meaningful and cost-effective have to be scaled and adapted to the size of the processing entity, the volume of data processed and the risks at stake.

72. It is worth noting that those additional obligations greatly correspond to the requirements established under the APEC Privacy rules and that for that particular aspect, the Convention and the APEC framework have similarities.

Article 9 – Exceptions and restrictions

73. As a general statement, no exceptions to the basic principles for data protection are to be allowed. It is nevertheless permitted, for a limited number of provisions, to benefit of

derogations when such a derogation if 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".

74. 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. States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.

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

76. The term "important economic and financial interests of the State" covers all the different means of financing a State's policies. Accordingly, the term refers in particular to 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.

77. 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 and information, confidentiality of communications and business or commercial secrecy and other legally protected secrets, etc.

78. Paragraph 2 leaves the possibility of restricting the rights with regard to data processing which pose no risk. Examples are the use of data for statistical work, in so far as these data are presented in aggregate form and stripped of their identifiers. Similarly, scientific research is included in this category.

Article 10 – Sanctions and remedies

79. In order that this convention can guarantee effective data protection, the duties of the data users and the rights of data subjects should be reflected in the national legislation of member States by corresponding sanctions and remedies.

80. In keeping with the non self-executing character of the convention, it should be left to each State to determine the nature (civil, administrative, criminal / jurisdictional, non jurisdictional) of these sanctions and remedies. Financial compensation of damages caused by the processing could also be considered.

Article 11 – Extended protection

81. 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 Contracting States are ready to adopt. It is underlined in the text that these principles constitute only a basis on which States may build a more advanced system of protection.

Chapter III – Transborder data flows

Article 12 – Transborder data flows

82. The aim of this article is to enable the free flow of information, regardless of frontiers, (notably enshrined in Article 10 of the European Convention on Human Rights and recalled in the Preamble) while ensuring an adequate data protection.

83. As a general rule, any data flows implying a change of jurisdiction requires that an adequate level of data protection 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.

84. This article applies to wide variety of factors determining the way in which data are flowing across borders: mode of representation of the data; storage medium; vector (cloud computing, localised transfer, etc.) interface; circuit followed (direct from country of origin to country of destination, or via one or more countries of transit); the relations between the originating Party and recipient (within one organisation or different organisations); etc.

85. Article 12 only applies to the export of data, not their import. The latter presents no problems because imported data are in any case covered by the data protection regime of the importing State. Some problems might, however, arise in case of re-import of data processed abroad in violation of certain provisions of the law of the country of origin Party to the convention. But it is clear in such cases that it is up to the country of origin to take, before export, the necessary measures according to Article 12.

86. Paragraph 2 applies to data flows between Parties to the Convention, which can not be prohibited or subject to special authorisation. The rationale for 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 adequate and data flows between Parties can thus operate freely.

87. The Convention Committee may nevertheless conclude that the level of protection of a particular (recipient) Party is not adequate, which would render the free flow of data laid down in paragraph 1 inapplicable.

88. This rule does not mean that a Contracting State may not take certain measures to keep itself informed of data traffic between its territory and that of another Contracting State, for example by means of declarations to be submitted by controllers.

89. In some cases transfers will be made from a Party simultaneously to several foreign countries, some of which are Parties to the convention whereas others are non-contracting States. In those cases, the originating Party 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.

90. Paragraph 3 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 adequate level of protection in the recipient country or organisation is to be guaranteed, and as this can not be presumed, the convention establishes two main possibilities to ensure the adequate level of data protection; either by law, or by standardised or ad hoc legal measures that are binding, effective and capable of effective remedies.

91. An adequate level of data protection can be ensured provided that the person in charge of the data flow supplies sufficient safeguards. Such safeguards may in particular be the result of contractual clauses binding the originating controller and the recipient who is not subject to the jurisdiction of a Party.

92. 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.

93. The level of protection should be assessed on a case-by-case basis for each transfer or category of transfers made. Thus the circumstances of the transfer should be examined and, 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 obtain there.

94. An assessment of adequacy can similarly be made for a whole state or organisation thereby permitting all data transfers to these destinations. In that case, the adequate level of protection is determined by the competent authorities of each Party.

95. The assessment of an adequate level of protection must take into account the principles of the Convention and the extent to which they are met in the recipient country 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.

96. A complementary safeguard is foreseen with the possible intervention of the competent supervisory authority, entitled to request that the quality and effectiveness of the measures taken according to paragraph 3 be demonstrated, and to suspend, prohibit or subject to condition the data flow.

97. Paragraph 4 enables parties to derogate, in a particular case, from the principle of an adequate level of protection and to allow data flows 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 legitimate interests protected by law) and subject to the competent supervisory authority's oversight.

98. Paragraph 5 provides another specific derogation, this time to the entire transborder data flows Chapter, when such a derogation is necessary in a democratic society to protect freedom of expression and information.

99. Data flows and the related necessary adequate 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 Cross-Border Privacy Rules.

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

100. 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 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.

101. 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, effective action in a person's favour.

102. 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, 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.

103. 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.

104. 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 of the file 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 himself/herself. 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, or to refer cases to national parliaments or other state institutions. The supervisory authority should have the power to inform the public through regular reports, the publication of opinions or any other means of communication.

105. 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. Moreover, every person should have the right to lodge a claim with the supervisory authority concerning his/her rights and liberties in respect of personal data processing. This lodging of a claim helps to guarantee people's right to an appropriate remedy, in keeping with Article 10 and Article 8 of the Convention. It is recalled that every person has 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.

106. 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.

107. 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 be entitled to carry out prior checks on the legitimacy of data processing operations and to keep a data processing register open to the public. The authority could also be asked to give its opinion when legislative, regulatory or administrative measures concerning personal data processing are in preparation, or on codes of conduct.

108. 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 could include the composition of the authority, the method for appointing its members, 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.

109. 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 when these decisions give rise to complaints.

110. 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.

111. 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 Consultative 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.

Chapter IV – Mutual assistance

Article 13 – Co-operation between Parties

112. The authorities will render each other general assistance for controls *a priori* (for example certifying whether terminals in one country, linked to a computer 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 computer centre). The information may be of a legal or factual character.

Article 14 (deleted)

Article 15 – Safeguards concerning assistance

113. 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.

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

Article 16 – Refusal of requests for assistance

115. 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.

116. These grounds are either that the request is incompatible with the powers of the authority or the terms of the convention and particularly with Article 3 regarding the extensions and exclusions every member State may have made to the scope of the convention or that it is at variance with overriding interests of the requested State or the data subject concerned.

117. 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 fundamental

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

Article 17 – Costs and procedures of assistance

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

119. "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 an automated data file.

120. 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 States 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 States 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

121. The purpose of Articles l8, 19 and 20 is to facilitate the smooth running of the convention and, where necessary, to perfect it.

122. 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.

123. 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).

124. In order to guarantee the implementation of the data protection principles set by the Convention, the Committee will prepare an assessment of the level of data protection provided by countries candidate for accession, will provide its opinion on the level of protection of a particular country in the context of transborder data flows and will periodically review the implementation of the Convention by the parties.

125. The committee may help to solve difficulties arising between Parties.

126. Where necessary, this committee will itself propose amendments to the convention or examine such proposals formulated by a Party or the Committee of Ministers in conformity with Article 21.

127. The nature of the 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.

Chapter VI – Amendments

Article 21 – Amendments

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

129. 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).

130. 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

131. 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

132. 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.

133. Considering the frontierless nature of data flows, accession by countries from all over the world is sought.

Article 24 – Territorial clause

134. 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

135. 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 27 - Notifications

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

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 1 June 2012

T-PD(2012)05

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

_____

Memorandum by the Secretariat on legal issues raised by the modernisation of Convention 108

_____

DG I – Human Rights and Rule of Law

_____

I. The form of the modernised instrument

1. The proposals for updating Convention CETS No. 108, as set out in document T-PD-BUR(2012)01Rev2 of 27 April 2012, are aimed at introducing significant changes to the existing text of the Convention, in particular, by incorporating into the Convention the amendments of 1999 and the provisions of the additional Protocol 2001 regarding supervisory authorities and transborder data flows (CETS No. 181) and by modifying the powers of the Convention Committee.

2. In view of the proposed changes, two types of instrument could be considered:
- a revised convention, or
- an amending protocol to Convention No. 108.

3. It should be pointed out that the main advantages and drawbacks of each type of instrument was described in document T-PD-BUR(2011)15, "Modalities for the amendment of Council of Europe treaties", prepared by the secretariat of the DG-HL.

Revised convention

4. In Council of Europe practice relating to conventions, it has been decided to draw up a revised convention in cases where the conditions which led to the drafting of the initial treaty have changed radically. This makes it possible to completely restructure the text of a former convention and bring it into force rapidly through a limited number of ratifications.

5. The drawback is that two treaty regimes, that of the former convention and that of the new convention, are applicable at one and the same time. The adoption of a revised convention does not automatically lead to the disappearance of the former convention, and it may take some time before all Parties to the former convention become Parties to the revised convention. Moreover, in keeping with the fundamental legal principle of free consent to treaties, no state can be forced to ratify the revised convention if it does not wish to. It cannot therefore be assumed that all of the Parties to Convention No. 108 will become Parties to the revised convention. Similarly, the final clauses of Convention No. 108 cannot guarantee that a member state of the Council of Europe (or a non-member State invited by the Committee of Ministers to accede to the Convention) will not decide to ratify Convention No. 108, as it is entitled to under Article 22 (or 23) of the Convention, rather than the revised convention. An example of this is the revised European Social Charter of 1996 (CETS No. 163): some member states of the Council of Europe have chosen to ratify the 1961 version of the European Social Charter 1961 and not the 1996 revised version.

6. A revised convention therefore entails the risk of setting up two treaty regimes, which means that the Convention Committee would have different functions and powers, depending on whether it was acting under Convention No. 108 or under the revised convention. It is believed that such a situation would make the functioning of the supervisory system set up under the Convention more complicated.

Amending protocol

7. The usual way to modify a Council of Europe convention is to draw up an amending protocol and there are many examples. The advantage of this method, compared to that of the revised convention, is that it ensures that there is only one version of the treaty in question and not several treaty regimes. Once Convention No. 108 has been amended, the Parties will all be bound by the same convention text. Similarly, in keeping with Article 40, paragraph 5 of the Vienna Convention on the Law of Treaties, states (irrespective of whether or not they are members of the Council of Europe) and the European Union wishing to become Parties to the Convention will only be able to express their consent to being bound by the convention in its amended version, which, once in force, will replace Convention No. 108.

8. It would be useful to consider including a clause concerning the effects of the amending protocol with regard to the amendments made to the Convention in 1999 and the Protocol drawn up in 2001. It could be stipulated in this clause that as from the entry into force of the amending protocol its provisions put an end to and replace the provisions of the amendments made in 1999 and the Protocol of 2001.

9. The possible effects of the amending protocol on State's declarations and reservations to the Convention and the additional Protocol should also be considered in greater detail. This refers in particular to the numerous declarations made to the current Article 3 of Convention CETS No. 108, in respect of which a change is envisaged. Questions as to whether existing declarations would continue to be valid and should therefore be retained should be addressed once progress has been made in preparing the draft updated instrument.

10. The main difficulty presented by an amending protocol is that it must be ratified by all Parties to the Convention before it can come into force. It was pointed out in the aforementioned document on "Modalities for the amendment of Council of Europe treaties that some so-called "hybrid" protocols, which contain both additional provisions and amending provisions, came into force after ratification by a limited number of states. Nevertheless, it should be pointed out that the implementation of these protocols depends on bilateral co-operation arrangements (for example, the protocol to the Convention on Mutual Administrative Assistance in Tax Matters or the protocols to the European Convention on Extradition) and that their ratification by a limited number of Parties does not therefore prevent them from functioning. On the other hand, the implementation of the changes envisaged in the present case, such as those concerning the functions and powers of the Convention Committee or the accession of the European Union or a number of states which are not members of the Council of Europe, means that they would have to be accepted by all Parties to the Convention.

11. To ensure that it does not take too long for the Protocol to come into force, due to the need for the 44 existing Parties to Convention No. 108 to ratify the amending protocol, it would be useful to include in the amending protocol a so-called "automatic" entry into force clause along the lines of the clause in Article 35 of the amending Protocol to the European Convention on Transfrontier Television (CETS No. 171), which reads as follows:

> "1. This Protocol shall enter into force on the first day of the month following the date on which the last of the Parties to the Convention has deposited its instrument of acceptance with the Secretary General of the Council of Europe.

2. However, this Protocol shall enter into force following the expiry of a period of two years after the date on which it has been opened to acceptance, unless a Party to the Convention has notified the Secretary General of the Council of Europe of an objection to its entry into force. The right to make an objection shall be reserved to those States or the European Community which expressed their consent to be bound by the Convention prior to the expiry of a period of three months after the opening for acceptance of this Protocol.

3. Should such an objection be notified, the Protocol shall enter into force on the first day of the month following the date on which the Party to the Convention which has notified the objection has deposited its instrument of acceptance with the Secretary General of the Council of Europe.(…)".

12. It will, of course, be possible to adjust the exact wording of this clause in the light of the discussions that take place and the specific needs identified during the negotiations. It should, however, be immediately pointed out that the presence of such a clause in no way prevents the Parties to the Convention who, under their domestic law, notably their constitutional law, are not able to accept the automatic entry into force of the amending Protocol, from following the procedures they normally use for the acceptance of the protocol, or if these cannot be completed within the time-limit set by the protocol, to object to the automatic entry into force (see the explanatory report to Protocol CETS No. 171, paragraphs 13-14 and 16).

II. Comments on the content of the draft modernised instrument

Title and preamble

13. Since 2004 conventions drawn up by the Council of Europe have borne the title "Council of Europe convention, with the exception of revised conventions, which, for reasons of consistency, have retained the title of the original convention. It would therefore be possible to consider adding the words "Council of Europe" to the amended title of the Convention.

14. The reference to Council of Europe member states in the opening line of the preamble should be retained. This is a set expression reflecting the fact that the convention in question was drawn up and adopted within the institutional structure of the Council of Europe. Moreover, the existing text of Convention No. 108 and the proposals for amendment provide that only member states of the Council of Europe may be Parties to the Convention. Non-member states of the Council of Europe and the European Union may only accede to it. If the aim of a reference to the "signatories" is to cover the situation of non-member states and the European Union, such a reference would be wrong if the instrument selected was an amending protocol to Convention No. 108.

15. The situation would be different if it was decided to revise the Convention. In that event, it would be possible to stipulate that not only Council of Europe member states but also non-member states which have participated in the preparation of the convention and the European Union can sign and ratify the revised convention. If this were the case, the wording used in the preamble to the Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No. 210) could be used, i.e.: "The member States of the Council of Europe and the other signatories hereto".

Article 4 – Duties of the Parties

16. Attention should be drawn to paragraph 2 of this article, which, according to you, presents difficulties with regard to its actual implementation. Pursuant to Article 22 of the Convention, Council of Europe member states are entitled to sign and ratify the Convention. The question is therefore what the consequences would be if a member state failed to take measures to give effect to the provisions of the Convention prior to depositing its instrument of ratification. This article would only have a genuine impact on non-member states as their request to be invited to accede to the Convention is closely examined. There is therefore a de facto inequality between States which ratify the Convention, depending on whether or not they are members of the Council of Europe. Similarly, if the authors of the proposals for updating the convention wish to give some non-member states the right to accede to the Convention without prior invitation from the Committee of Ministers, it would be advisable to first ensure that these states' legislation complies with the provisions set out in the amended Convention.

Article 18 – Composition of the Committee

17. With regard to paragraph 3 of Article 18, it would be useful to stipulate that it is the representatives "of the Parties" who vote. Moreover, the terminology used should be brought into line with that generally used at the Council of Europe, in particular in the Committee of Ministers. For example, it would be preferable to use the expressions "voix exprimées" in French (rather than "participant au vote") and "casting a vote" in English (rather than "voting"). For example the French text would read as follows:

> "Le comité conventionnel peut, par une décision prise [par les représentants *des Parties* à la majorité des deux-tiers *des voix exprimées*] OU [à la majorité des représentants *des Parties possédant* le droit de vote], inviter un observateur à se faire représenter à ses réunions".

In English:

> "The Convention Committee may, by a decision taken by a majority of two-thirds of *the* representatives *of the Parties* [*casting a vote*] [entitled to vote], invite an observer to be represented at its meetings".

Article 21 – Amendments

18. Insofar as the proposal for amending paragraph 2 of Article 21 is now addressed to the "Parties" to the Convention, the words "which has acceded to or" are redundant. The non-member States which have acceded to the Convention will be covered by the expression "Parties". Moreover, in view of the changes envisaged in respect of Articles 22 and 23, the European Union should also receive the proposals for amendment. If the EU is entitled to sign the revised convention or to accede to the amended convention, depending on which type of instrument is selected, it should be placed in the same situation as non-member States which have been invited to accede to the convention.

Article 23 – Accession by non-member States or the European Union

19. The procedure for inviting a non-member State to accede to the amended Convention could require the unanimous agreement of the Parties to the Convention, as is the case in recent Council of Europe conventions. Moreover, in order to avoid any ambiguity between the powers

of the Convention Committee and those of the Committee of Ministers in the invitation procedure, the full name of the Committee of Ministers should appear at the end of paragraph 1, which would read as follows:

> "After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may, *after consulting the Parties to the Convention and obtaining their unanimous agreement*" invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the *Committee of Ministers*."

20. The proposed changes should not be made to paragraph 2 of Article 23. A State only becomes Party to a convention once the convention has come into force in its respect. The reference to the "acceding State" should therefore be retained and a reference to the European Union should be added. Paragraph 2 of Article 23 would begins as follows: "In respect of any State or the European Union acceding to this Convention, in conformity with paragraph 1 above". The remainder of the article would be unchanged.

21. New paragraph 3 introduces a novel feature into Council of Europe practice relating to conventions. There is no objection to this from the legal standpoint. The non-member States concerned should, however, be clearly identified during the negotiation and adoption of the draft instrument by the Committee of Ministers and the list of these States should appear in the explanatory report. It should also be clearly stipulated that the right to accede without prior invitation from the Committee of Ministers only concerns the amended version of the convention. The word "amended" should therefore be added to "can accede to the Convention".

22. If the type of instrument selected is an amending protocol, this provision should be placed before the current paragraph 2 of Article 23. This provision on the manner of the entry into force would apply to both of the situations envisaged. It should, however, be pointed out that if it is decided to draft a revised convention, the situation referred to in paragraph 3 could be covered in Article 22, paragraph 1, which would read as follows: This Convention shall be open for signature by the member States of the Council of Europe, *the European Union and non-member states which have participated in its preparation"*. In this case, the reference to the European Union should be removed from the heading to Article 23.

Article 27 – Notifications

23. It should be recalled that the exact wording of this article will have to be altered to bring it into line with the wording of Articles 22 and 23 of the Convention.

Explanatory report

24. The proposals for updating the Convention envisage giving more importance to the explanatory report. It should, however, be pointed out that in the Council of Europe practice relating to conventions the explanatory report does not constitute an instrument providing an authoritative interpretation of the treaty to which it refers. Nevertheless, it is part of the "context" of a convention within the meaning of Article 31, paragraph 2, of the Vienna Convention on the Law of Treaties. It should also be pointed out that, in March 1991 the Committee of Ministers' Rapporteur Group on Legal Co-operation (GR-J) was asked to give an opinion on the interpretation of the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CETS No. 126). It is interesting to note that the Group "unanimously agreed that the explanatory report is of great value for the interpretation of the Convention but that it does not have the same value as the text of the Convention. The explanatory report therefore has to be taken into consideration when giving an opinion. However, as set out above, any such interpretation cannot be an authoritative and therefore binding interpretation, regardless of the weight of the arguments based on the explanatory report…". In view of the above, it does not seem appropriate to introduce a reference to the explanatory report in the text of the draft instrument for updating the Convention.

25. However, if it were decided to deal with a number of questions by a means other than a revised or amended convention, the possibility of drafting an appendix to the draft instrument could be envisaged. An example of this is provided by the European Social Charter (CETS No. 35) and the revised European Social Charter (CETS No. 163), both of which contain an appendix stipulating the scope and meaning of some of their provisions. It should be noted that this appendix would be an integral part of the text of the Convention (see Article 38 of the European Social Charter and Article N of the revised European Social Charter) and the Convention Committee could draw on this appendix with regard to its new powers of interpretation (Article 19.d of the draft text). An explanatory report could also be prepared but its value would be that usually given to explanatory reports of Council of Europe conventions.

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, le 1 juin 2012

T-PD (2012)05

LE COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL (T-PD)

_____

Mémorandum du Secrétariat sur les questions juridiques soulevées dans le cadre de la modernisation de la Convention 108.

_____

DG I – Droits de l'Homme et État de droit

_____

I. Sur la forme de l'instrument de modernisation

1. Les propositions de modernisation de la Convention n°108, telles qu'elles apparaissent dans le document T-PD-BUR(2012)01Rev2 du 27 avril 2012, visent à introduire d'importantes modifications au texte actuel de la Convention, en particulier, en intégrant dans la Convention les amendements de 1999 et les dispositions du Protocole additionnel de 2001 concernant les autorités de contrôle et les flux transfrontières de données (STE n°181) et en modifiant les compétences du comité de suivi.

2. Compte-tenu des modifications proposées, deux types d'instruments pourraient être envisagés :

- une convention révisée, ou
- un protocole d'amendement à la Convention n°108.

3. Il est rappelé que les avantages et inconvénients respectifs de chaque type d'instrument avaient été décrits dans leurs grandes lignes dans le document T-PD-BUR(2011)15, « Modalités d'amendement des traités du Conseil de l'Europe » préparé par le secrétariat de la DG-HL.

Convention révisée

4. Dans la pratique conventionnelle du Conseil de l'Europe, le choix d'une convention révisée a été fait lorsque les conditions qui avaient amené à conclure le traité initial avaient radicalement changé. Cette technique permet de refondre totalement le texte d'une convention ancienne et d'assurer une entrée en vigueur rapide par un nombre limité de ratifications.

5. Elle présente toutefois l'inconvénient de faire coexister deux régimes conventionnels, celui de l'ancienne convention et celui de la nouvelle convention. En effet, l'adoption d'une convention révisée ne fait pas disparaître l'ancienne convention, et un temps assez long peut s'avérer nécessaire pour que l'ensemble des Parties à l'ancienne convention deviennent Parties à la convention révisée. De plus, en vertu du principe fondamental en droit des traités de libre consentement, un Etat ne saurait être contraint de ratifier la convention révisée s'il ne le souhaite pas. Ainsi, il ne peut être acquis d'avance que l'ensemble des Parties à la Convention n°108 deviendront Parties à la convention révisée. De la même manière, les clauses finales de la Convention n°108 ne permettraient pas d'empêcher qu'un Etat membre du Conseil de l'Europe (ou un Etat non membre invité à adhérer par le Comité des Ministres) décide de ratifier la Convention n°108, comme il en a le droit en vertu de l'article 22 (ou 23) de cette Convention, plutôt que la convention révisée. Il peut être relevé à titre d'exemple que l'existence de la Charte sociale européenne révisée de 1996 (STE n°163) n'a pas empêché que des Etats membres du Conseil de l'Europe choisissent de ratifier la Charte sociale européenne dans sa version de 1961, et non celle de 1996.

6. Le choix d'une convention révisée comporte ainsi le risque d'instaurer deux régimes conventionnels. Ceci impliquerait notamment que le comité conventionnel aurait des compositions et des fonctions différentes selon qu'il agirait en vertu de la Convention n°108 ou de la convention révisée. Il nous semble qu'une telle situation compliquerait le fonctionnement du système de suivi mis en place par la Convention.

Protocole d'amendement

7. L'élaboration d'un protocole d'amendement constitue la manière habituelle de modifier des conventions du Conseil de l'Europe. Les exemples sont multiples. L'avantage de cette

technique, par contraste avec celle de la convention révisée, est qu'elle permet l'existence d'une seule version du traité concerné et évite la multiplicité de régimes conventionnels. Ainsi, une fois la Convention n° 108 amendée, les Parties seraient liées par le même texte conventionnel. De même, conformément à l'article 40, paragraphe 5, de la Convention de Vienne sur le droit des traités, les Etats (membres ou non du Conseil de l'Europe) et l'Union européenne qui souhaiteraient devenir Parties à la Convention ne pourraient exprimer leur consentement à être liés que par la convention dans sa version amendée qui, une fois en vigueur, se sera substituée à la Convention n° 108.

8. Pour ce qui est des amendements de 1999 et du Protocole de 2001, il serait utile d'envisager l'insertion d'une clause relative aux effets du protocole d'amendement sur ces deux instruments. Elle pourrait prévoir qu'à partir de l'entrée en vigueur du protocole d'amendement ses dispositions mettent fin et remplacent celles des amendements de 1999 et du Protocole de 2001.

9. Une réflexion plus approfondie sur les éventuels effets du protocole d'amendement sur les déclarations et réserves faites par les Etats à la Convention et au Protocole additionnel devrait également être menée. Il est fait en particulier référence aux nombreuses déclarations faites à l'actuel article 3 de la Convention STE n° 108 pour lequel une modification est envisagée. Les questions du maintien et de la validité des déclarations existantes devraient ainsi être abordées lorsque la rédaction du projet d'instrument de modernisation sera plus avancée.

10. La principale difficulté que présente un protocole d'amendement est qu'il doit être ratifié par toutes les Parties à la Convention pour qu'il puisse entrer en vigueur. Il a été indiqué, dans le document précité sur les « Modalités d'amendement des traités du Conseil de l'Europe » que certains protocoles dits « hybrides », c'est-à-dire contenant à la fois des dispositions additionnelles et des dispositions d'amendement, ont pu entrer en vigueur après un nombre limité de ratifications. Il convient toutefois de souligner que la mise en œuvre de ces protocoles reposent sur des mécanismes de coopération bilatérale (comme, par exemple, le protocole à la Convention sur l'assistance administrative mutuelle en matière fiscale ou les protocoles à la Convention européenne d'extradition) et, de ce fait, leur ratification par un nombre limité de Parties n'empêche pas leur fonctionnement effectif. En revanche, dans le cas présent, la mise en œuvre des modifications envisagées, telles que celles relatives aux fonctions du comité conventionnel ou à l'adhésion de l'Union européenne ou de certains Etats non membres du Conseil de l'Europe requiert qu'elles soient acceptées par l'ensemble des Parties à la Convention.

11. Pour éviter de trop longs délais d'entrée en vigueur, dus à la nécessité pour les 44 Parties actuelles à la Convention n° 108 de ratifier le protocole d'amendement, il serait souhaitable d'insérer dans le protocole d'amendement une clause d'entrée en vigueur dite « automatique » sur le modèle de celle contenue à l'article 35 du Protocole portant amendement à la Convention européenne sur la télévision transfrontière (STE n° 171). Cette clause se lit comme suit :

> « 1. Le présent Protocole entrera en vigueur le premier jour du mois suivant la date à laquelle la dernière des Parties à la Convention aura déposé son instrument d'acceptation auprès du Secrétaire Général du Conseil de l'Europe.
>
> 2. Néanmoins, le présent Protocole entrera en vigueur à l'expiration d'une période de deux ans à compter de la date à laquelle il aura été ouvert à l'acceptation, sauf si une Partie à la Convention a notifié au Secrétaire Général du Conseil de l'Europe une objection à son entrée en vigueur. Le droit de faire une objection est réservé aux Etats ou à la Communauté européenne qui ont exprimé leur consentement à être

liés par la Convention avant l'expiration d'une période de trois mois suivant l'ouverture à l'acceptation du présent Protocole.

3. Lorsqu'une telle objection a été notifiée, le Protocole entrera en vigueur le premier jour du mois suivant la date à laquelle la Partie à la Convention qui a notifié l'objection aura déposé son instrument d'acceptation auprès du Secrétaire Général du Conseil de l'Europe.(…) ».

12. Le libellé exact de cette clause pourra, bien entendu, être ajusté en fonction des discussions qui auront lieu lors des négociations et des besoins spécifiques qui en ressortiront. Il convient toutefois de préciser dès à présent que la présence d'une telle clause n'empêche nullement les Parties à la Convention qui, en application de leur droit national, et notamment de leur droit constitutionnel, ne sont pas en mesure d'accepter l'entrée en vigueur automatique du protocole d'amendement, de suivre les procédures qu'elles utilisent habituellement pour l'acceptation du protocole, voire, si cela ne peut être mené à bien dans le délai prévu par le protocole, de formuler une objection à l'encontre de l'entrée en vigueur automatique (voir le rapport explicatif du Protocole STE n°171, paragraphes 13-14 et 16).

II. Commentaires sur le contenu du projet d'instrument de modernisation

Titre et préambule

13. Depuis 2004, les conventions élaborées au sein du Conseil de l'Europe ont comme titre « convention du Conseil de l'Europe », à l'exception des conventions de révision qui, pour des raisons de concordance, ont conservé le titre de la convention d'origine. Il pourrait ainsi être envisagé d'ajouter les mots « du Conseil de l'Europe » au titre amendé de la Convention.

14. La référence aux Etats membres du Conseil de l'Europe dans la formule d'ouverture du préambule devrait être maintenue. Il s'agit d'une formule standard qui reflète le fait que la convention en question a été élaborée et adoptée dans le cadre institutionnel du Conseil de l'Europe. De plus, le texte actuel de la Convention n°108 et les propositions d'amendement prévoient que seuls les Etats membres du Conseil de l'Europe peuvent être signataires de la Convention. Les Etats non membres du Conseil de l'Europe et l'Union européenne peuvent seulement y adhérer. Si l'objectif d'une référence aux « signataires » est de couvrir la situation des Etats non membres et de l'Union européenne, une telle référence serait erronée si l'instrument retenu était un protocole d'amendement à la Convention n°108.

15. Il en irait autrement si le choix était fait d'une convention révisée. Il pourrait, dans ce cas, être prévu que les Etats non membres ayant participé à son élaboration et l'Union européenne signent et ratifient la convention révisée, au même titre que les Etats membres du Conseil de l'Europe. Dans cette hypothèse, la formule utilisée dans le préambule de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique (STCE n°210) pourrait être retenue, à savoir : « Les Etats membres du Conseil de l'Europe et les autres signataires de la présente Convention ».

Article 4 – Engagements des Parties

16. J'attire votre attention sur le paragraphe 2 de cette disposition qui présente, selon nous, des difficultés de mise en œuvre effective. En effet, en vertu de l'article 22 de la Convention, les Etats membres du Conseil de l'Europe bénéficient du droit de signer et ratifier la Convention. La question se pose ainsi de savoir quelles seraient les conséquences d'une absence de mesures

prises par un Etat membre pour donner effet aux dispositions de la Convention préalablement au dépôt de son instrument de ratification. Il nous semble que cette disposition ne pourrait avoir de véritables effets qu'à l'égard des Etats non membres dans la mesure où leur demande d'être invité à adhérer à la Convention est l'objet d'un examen. Il existe ainsi une inégalité de fait entre les Etats qui ratifient la Convention selon qu'ils sont membres ou pas du Conseil de l'Europe. De la même manière, si les rédacteurs des propositions de modernisation souhaitent donner à certains Etats non membres le droit d'adhérer à la Convention amendée sans invitation préalable du Comité des Ministres, il conviendra de s'assurer préalablement que ces Etats ont une législation conforme aux dispositions de la Convention amendée.

Article 18 – Composition du comité

17. S'agissant du paragraphe 3 de l'article 18, il serait utile de préciser que ce sont les représentants « des Parties » qui votent. De plus, la terminologie employée devrait être alignée sur celle généralement utilisée au Conseil de l'Europe, notamment au Comité des Ministres. Ainsi, les expressions « voix exprimées » (plutôt que « participant au vote ») et « casting a vote » (plutôt que « voting ») devraient être préférées. Le texte français se lirait, par exemple, comme suit :

> « Le comité conventionnel peut, par une décision prise [par les représentants *des Parties* à la majorité des deux-tiers *des voix exprimées*] OU [à la majorité des représentants *des Parties possédant* le droit de vote], inviter un observateur à se faire représenter à ses réunions ».

En anglais :

> "The Conventional Committee may, by a decision taken by a majority of two-thirds of *the* representatives *of the Parties* [*casting a vote*] [entitled to vote], invite an observer to be represented at its meetings".

Article 21 – Amendements

18. Dans la mesure où la proposition d'amendement au paragraphe 2 de l'article 21 vise désormais les « Parties » à la Convention, les termes « a adhéré ou » sont redondants. En effet, les Etats non membres qui auront adhéré à la Convention seront couverts par l'expression « Parties ». De plus, compte tenu des modifications envisagées aux articles 22 et 23, l'Union européenne devrait également recevoir les propositions d'amendement. En effet, si celle-ci bénéficie du droit de signer la convention révisée ou d'adhérer à la convention amendée, selon la formule choisie, elle devrait être placée dans la même situation que les Etats non membres qui ont été invités à adhérer.

Article 23 – Adhésion d'Etats membres ou de l'Union européenne

19. La procédure d'invitation d'un Etat non membre à adhérer à la Convention amendée pourrait prévoir l'accord unanime des Parties à la Convention, comme cela est le cas dans les conventions récentes du Conseil de l'Europe. De plus, afin d'éviter toute ambiguïté entre les compétences respectives du comité conventionnel et du Comité des Ministres dans la procédure d'invitation, le nom complet du Comité des Ministres devrait figurer à la fin du paragraphe 1. Ce paragraphe se lirait comme suit :

> « Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe pourra, *après consultation des Parties à la Convention et en*

avoir obtenu l'assentiment unanime, et à la lumière de l'avis formulé par le comité conventionnel conformément à l'article 19.e, inviter tout Etat non membre du Conseil de l'Europe à adhérer à la présente Convention par une décision prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe, et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité *des Ministres*. ».

20. Le paragraphe 2 de l'article 23 ne devrait pas être modifié comme envisagé. En effet, un Etat ne devient Partie à une convention qu'une fois celle-ci en vigueur à son égard. Il conviendrait ainsi de conserver la référence à « l'Etat adhérant » et d'ajouter une référence à l'Union européenne. Le paragraphe 2 de l'article 23 s'ouvrirait comme suit : « Pour tout Etat ou l'Union européenne adhérant à la présente Convention conformément au paragraphe 1 ci-dessus ». Le reste de la disposition serait inchangé.

21. Le nouveau paragraphe 3 introduit une nouveauté dans la pratique conventionnelle du Conseil de l'Europe. Nous n'y voyons pas d'objection d'un point de vue juridique. Les Etats non membres visés par cette disposition devraient toutefois être clairement identifiés lors de la négociation et de l'adoption du projet d'instrument par le Comité des Ministres, et la liste de ces Etats devrait figurer dans le rapport explicatif. De plus, il devrait être précisé que ce droit d'adhérer sans invitation préalable du Comité des Ministres ne concerne que la convention dans sa version amendée. Le mot « amendée » devrait ainsi être ajouté après « peuvent adhérer à la Convention ».

22. Par ailleurs, si la forme de l'instrument retenue est celle d'un protocole d'amendement, cette disposition devrait être placée avant l'actuel paragraphe 2 de l'article 23. Cette dernière disposition sur les modalités d'entrée en vigueur s'appliquera en effet aux deux situations envisagées. Il convient toutefois de préciser que si la forme de l'instrument retenue est celle d'une convention révisée, la situation visée au paragraphe 3 pourrait être couverte à l'article 22, paragraphe 1, qui se lirait comme suit : « La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe, *de l'Union européenne et des Etats non membres ayant participé à son élaboration* ». Dans ce cas, la référence à l'Union européenne devrait être enlevée du titre de l'article 23.

Article 27 – Notifications

23. Il est rappelé pour mémoire que le libellé exact de cette disposition devra être adapté en fonction de la rédaction des articles 22 et 23 de la Convention.

Rapport explicatif

24. Les propositions de modernisation envisagent de renforcer la valeur du rapport explicatif de la Convention. Il convient toutefois de rappeler que dans la pratique conventionnelle du Conseil de l'Europe le rapport explicatif n'est pas considéré comme un instrument authentique d'interprétation de la convention auquel il se rapporte. Toutefois, il fait partie du « contexte » d'une convention au sens de l'article 31, paragraphe 2, de la Convention de Vienne sur le droit des traités. Il est également rappelé qu'en mars 1991 le Groupe de rapporteurs sur la coopération juridique (GR-J) du Comité des Ministres avait eu à se prononcer sur l'interprétation de la Convention européenne pour la prévention de la torture et des peines ou traitements inhumains ou dégradants (STE n°126). Il est intéressant de relever que le Groupe avait « convenu à l'unanimité que le rapport explicatif est très utile pour l'interprétation de la Convention mais qu'il n'a pas la même valeur que le texte de la Convention. On doit donc le

prendre en considération lorsqu'on formule un avis. Toutefois, comme on l'a vu, une interprétation de cette sorte ne peut pas être authentique et donc contraignante, quel que soit le poids des arguments fondés sur le rapport explicatif. ». Compte-tenu de ce qui précède, il ne paraît pas approprié d'introduire une référence au rapport explicatif dans le texte du projet d'instrument de modernisation.

25. Toutefois, si un certain nombre de questions devaient être traitées en dehors du projet d'instrument conventionnel, il pourrait être envisagé de rédiger une annexe au projet. Un exemple sur lequel s'appuyer est fourni par la Charte sociale européenne (STE n°35) et la Charte sociale européenne révisée (STE n°163) qui contiennent toutes deux une annexe précisant la portée et le sens à donner à certaines de leurs dispositions. Il est à noter que cette annexe ferait partie intégrante du texte conventionnel (voir l'article 38 de la Charte sociale européenne et l'article N de la Charte sociale européenne révisée) et le comité conventionnel pourrait se fonder sur elle dans le cadre de ses nouvelles fonctions d'interprétation (article 19.d du projet). Un rapport explicatif pourrait également préparé, mais sa valeur serait celle habituellement reconnue aux rapports explicatifs des conventions du Conseil de l'Europe.

V. APPENDIX / *ANNEXE*

COMPILATION OF COMMENTS RECEIVED / *COMPILATION DES COMMENTAIRES REÇUS*

Delegations of the T-PD / *Délégations du T-PD*

AUSTRIA / *AUTRICHE*

ADDITIONAL COMMENTS OF THE REPUBLIC OF AUSTRIA ON THE MODERNISATION OF CONVENTION 108

1) General comments:

The following comments are made with reference to the proposals presented by the Bureau of the T-PD in document T-PD-BUR(2012)01Rev2_en of 27 April 2012.

2) Comments on Articles:

Article 2:
Art. 2 (a): It is proposed to return to the original remarks in the Explanatory Report, namely that an individual is not considered identifiable "*if identification requires unreasonable time or effort for a person who would be informed of it*". The current wording ("*if identification requires unreasonable time or effort for the controller or for any person from whom the controller could reasonably obtain the identification*") seems too narrow: a person could – for example – also be identified by any other person (see for that regard for example recital 26 of Directive 95/46/EC or Art. 4 para 1 of the proposed General Data Protection Regulation).

Art. 2 (c): Subparagraph 2 mentions no automated processing of data. On the other hand, Art. 3 para 2 (c) which provides for the possibility to apply Convention 108 also to personal data files which are not processed automatically will be deleted.

Prima facie this seems to be a contradiction which must be reconciled (see also comments on Art. 3 below).

If it is, however, intended to apply to Convention 108 to automated and no automated processing of data alike – which the Republic of Austria strongly supports –, it should be stated more clearly (for example in the Explanatory Report); the current structure of Art. 2 (c) is not very conclusive in that regard.

Article 3:
As already mentioned in former comments, the Republic of Austria strongly favours the applicability of Convention 108 to no automated data processing – either mandatory or if one party wishes to do so.

Just for the case that the proposed wording of Convention 108 – in particular Art. 2 (c) – does not cover automated and no automated processing of data alike, it is once again emphasised that by deleting Art. 3 para 2 (c) Convention 108 would fall behind the standard of current and future EU-law (see for that regard Art. 2 para 1 of the proposed EU General Data Protection Regulation).

The Republic of Austria also refers to her comments on Art. 2 (c) above.

Article 6:
For the sake of legal certainty it is once again proposed to define "*genetic data*" and "*biometric data*" in Art. 2 and not in the Explanatory Report (see also Art. 4 paras. 10 and 11 of the proposed General Data Protection Regulation).

Article 8:
The Republic of Austria again wishes to emphasise that Art. 8 (b) should be specified in a way to make it clear that a person cannot object to processing of personal data concerning him/her if there is a clear basis in law for data processing: it must be clear that if data are processed according to a law an individual cannot oppose the processing, not even for legitimate reasons (for example: data processing by the police or by courts).

Article 12bis:
It is proposed again that the wording "*explicitly agreed*" in para. 7 (a) should be replaced by "*given his/her consent*", because "*consent*" is a data protection term already used in the Convention.

Article 23:
Art. 23 in the version of 5 March 2012 provided for the accession by non-member States or international organisations. The current version provides only for the accession by non-member States or the European Union.

The Republic of Austria would like to know why the scope was narrowed down.

Generally, if it is the effort of the CoE to encourage as many actors as possible to join Convention 108 – which the Republic of Austria supports –, this treaty should be open for the accession by other international organisations (for example INTERPOL, OECD) as well.

BULGARIA / *BULGARIE*

COMMENTS OF THE COMMISSION FOR PERSONAL DATA PROTECTION ON THE PROPOSED AMENDMENTS TO THE CONVENTION 108/81/CE

In connection with the sent request for review and comments on the newly proposed texts of Convention 108/81/CE for the protection of individuals with regard to automatic processing of personal data, the Commission for Personal Data Protection would like to make the following comments:

1. On Art. 3 "Scope":

- **Paragraph 1 ter)**- about the application of the Convention's provisions with regard to the legal persons- it should be clarified to what extend the data of the legal persons will be protected. The Commission proposes this paragraph to be applied only with regard to these data, part of the legal persons' information, which disclose personal characteristics and can lead to personal identification of the data subject.

2. On Art. 5 "Legitimacy of data processing and quality of data":

- **para. 1** –the definition "fair balance" should be explained in details and if possible in the provision;

- **para. 2**- the explanation for "overriding legitimate interest" should be included in the provision, not in the Explanatory Report.

3. On Art. 6 "Processing of sensitive data":

- **para.1**- we support the classification of the different categories of sensitive data, which is foreseen in the text and the definitions mentioned in the Explanatory Report should be set in the provision.

- **para.2** – it should be clarified what is meant with "appropriate safeguards" and in which case can be performed sensitive data processing.

4. On Art. 7 "Data security":

- **para.2**- the Commission is of opinion that the right to inform the individuals should not be lost, but as exception, they could not be informed for data breaches if these breaches do not pose a treat to their privacy. It could be appropriate, to be explained in the provision in which cases the individuals should be informed and the requirement for mandatory notification of the individuals by serious data breaches, defined in the EC Regulation proposal should be considered.

5. On Art. 7 bis "Transparency of processing":

- **para.2** – it should be clarified what is meant with "impossible" and "involves disproportionate efforts". According to the Commission, the right to inform individuals about the processing of their personal data should not be restricted without the existence of serious ground and only in specific cases. Otherwise this could lead to wide interpretation of this provision with the purpose of avoiding the right of information and non application of paragraph 1 of the same article.

6. On Art. 9 "Exemptions and restrictions":

- **para.1, item b)**- the text with the explanations about the freedom of expression and information should be included in the provision.

7. On Chapter III "Transborder data flows":

- **Art. 12, para.3, item b**–in the provision should be clarified the following issues:

• What is meant with ad hoc measures?

• Will these measures be in force for the relevant transfer or for specific categories of data?

• If the measures are applied for defined period of time, for how long will they be applicable?

• What will happen with the personal data protection after the measures are no longer applied - will the relevant data processing be terminated?

CYPRUS / *CHYPRE*

Preamble – General Comments

Article 1 – Object and purpose

Cyprus has strong oppositions to the use of the term "j*urisdiction*" in the main body of the Convention instead of the word used in the Convention "territory". Please see the attached opinion of the Legal Service of the Cyprus Republic which reflects our concerns.

Article 2 – Definitions

We support the maintaining of definitions for genetic and biometric data in the explanatory memorandum.

We agree with the replacement of the term "consultative" with the term "conventional" which is better harmonized with the new role and functions of the Committee.

Text of the convention/proposals

Preamble:

For uniformity reasons we think that either the words "explanatory report" will be used or "explanatory memorandum".

Article 1: - object and purpose

Cyprus has strong reservations to the use of the term "jurisdiction" in the main body of the Convention instead of the word used in the Convention "territory". Please see the attached opinion of the Legal Service of the Cyprus Republic which reflects our concerns.

Article 2: - definitions

2(c) We are deeply concerned about the use of the term "*person concerned*", which may raise a lot of legal uncertainties. We consider the term "specific data subject" more suitable under the circumstances. The word "specified" should be replaced by the word "specific" and those criteria should be explained in the explanatory report.

Article 3 – Scope

1ter We strongly disagree to the prospect of applying the Convention to information on legal persons.

Arguments: Natural persons and legal persons do not face the same threats. If the Parties wish to extend the protection provided by the Convention to legal persons they should foremost identify the threats that legal persons face, which would justify this extension. So far we have not identified any threats to legal persons that need to be tackled by the Convention. The spirit of the modernization is to provide a more harmonizing legal instrument, which will facilitate the effective enforcement cooperation of the supervisory authorities. Such cooperation cannot be

endorsed if in some Parties the Convention applies to legal persons, whereas in others it does not.

Article 4 – Duties of the parties

4(3) We propose the following text: "*Each party undertakes to allow the Conventional Committee foreseen in Chapter V to observe (or monitor) and evaluate its engagements and to contribute actively to this evaluation"*.

Article 5 – Legitimacy of data processing and quality of data

5(3)(b) We propose the word "specific" instead of the word "specified" and before the word "processed" (second line) the word "further" to be added in order to give the correct meaning.

Article 6 – Processing of personal data

Cyprus has a general reservation for the wording of this article, which changes radically the rational for the protection of special categories of data. We would like to hear the rationale behind the proposed wording before we provide our final comments. This new wording creates legal uncertainty and interpretation issues.

Article 7- Data Security

7 (1) We propose instead of the word "modification" the word "alteration" to be used.
7(2) The new wording "fundamental rights and freedoms of the data subject" is rather general since the interference specifically refers to the personal data of the data subject which has been put at risk. We propose amendment of the current text accordingly.

Article 8 - Rights of the data subject

8(a) the word "significantly" needs to be clarified in the explanatory report.

Article 8bis – Additional Obligations

8bis (1) in relation with the other paragraphs creates legal uncertainties as to whether is the controller responsible for applying the domestic legal provisions or where a processor is delegated if only the latter is responsible for applying the domestic legal provisions.

8bis(5) We suggest the following wording instead of the wording "of data protection" "on the right to the protection of personal data" which is in line with the wording of Article 8bis(1).

Article 12 – Transborder data flows

Article 12(2) The wording "The Conventional Committee may nevertheless conclude that the level of protection is not adequate" needs to be clarified in the explanatory report explaining the reasons which lead the Committee to the aforementioned conclusion.

Article 12(3)(a) By the wording “agreements” do we mean multilateral and bilateral agreements?

Article 12(3)(b) second paragraph the word “shall” should not be replaced by the word “may” because the supervisory Authority should have a more active and binding role in this procedure.

Article 12(4) the words “data subjects” (6th line) should be replaced by the words “personal data” since speaking about adequate level we mean adequate level of protection of personal data.

Article 12bis - Supervisory authorities

12bis(2)(c) We believe the choice of the word “seized” is inappropriate and may be confused with confiscation. We would prefer to see another wording that would avoid legal uncertainties.

12bis(4) Substitute the word “accomplish” with the word “perform”.

12bis(9) From the positions expressed at the November meeting we have understood that this exception would apply to the processing carried out by judicial authorities only when acting in their judicial capacity. The proposed text seems to extend to other judicial services such as the Chief Registrar and other institutions incorporated in Parties' judicial systems. We propose to use another, more clear text.

Article 19 – Functions of the committee

Article 19(i) refers to article 12 paragraph (3) this reference is not correct since paragraph (3) of article 12 does not provide for an opinion of the Conventional Committee.

Article 20 – Procedure

Article 20(3) With regard to this article we would like to hear the rationale behind the proposed wording before we provide our final comments, we retain our reservation.

Article 21 – Amendments, Article 23 Accession by non - member states or the European Union and Article 24 Territorial clause

Republic concluding that articles 21(8), 23 and 24 do not seem to be problematic we withdraw our reservations regarding the aforementioned articles.

New Proposals by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Data (ETS No.108)
Executive Summary

(Comments on Consultative Committee document T-PD-BUR(2012)01 Rev-en re Modernization of Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data)

1. The Consultative Committee's major proposals to amend the Convention of 28 January 1981 and its Additional Protocol of 8 November 2001 are analysed, concentrating (as requested by MFA) on the impact of amending the Convention by referring to the concept of "jurisdiction" instead of to "territory" to define the geographical scope of the Convention's protection of personal data.

2. Ambiguity, due to different meanings of "jurisdiction," is pointed out. Depending upon what meaning is adopted regarding "jurisdiction," the scope of application of the Convention and State responsibility could be considerably extended so as to bind each ratifying State to protecting data, subject however to a larger discretion, while also permitting data disclosure within and across its national frontiers.

3. It is suggested that, by introducing the multi-faceted concept of "jurisdiction," major problems concerning the interpretation and the application of the Convention could arise.

4. This could be especially problematic regarding action by Turkey in relation to the "TRNC".

5. Extending the scope of application of the Convention involves policy considerations for ROC, not only because of the potential impact of extended application of the Convention in relation to the "TRNC", but also because, in light of ECHR jurisprudence on the restriction of rights, States (including ROC) will have very extensive competence to restrict the rights involved by way of the large margin of appreciation accorded them by the Court. In a litigious society, there are unnecessary dangers and uncertainties in amending the Convention, especially when it has not been clearly established that this is necessary.

New Proposals by the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Data (ETS No.108)

1. The Law Office was requested by letter, dated 2 April 2012 from the MFA, to comment on the Consultative Committee's new proposals to amend the Convention of 28 January 1981. Advice was only requested in relation to references to the concept of "jurisdiction". That multifaceted concept is reflected (at p.3) in the explanatory introductory Memorandum in relation to Article 1 (governing the "object and purpose" of the Treaty); and in relation to Article 3 (governing the "Scope" of the Convention). It is also reflected in the proposed amendment of Article 1 (at p.9 of the Memorandum) and in Article 12 (governing trans-border flows of personal data and domestic law) both in a first and in an alternative proposal. Currently, the only reference to "jurisdiction" is in Article 2 of the Additional Protocol of 8 November 2001. In the context of the Additional Protocol, it is obvious that "jurisdiction" is being used in a sense that is different from the sense given it under the proposed amendment to Article 1 of the Convention. "Jurisdiction," when referred to in the Additional Protocol of 8 November 2001, is there used a meaning "the legal

power (competence/authority) of a State to regulate conduct either legislatively, judicially or administratively or executively," with the extent of the State's jurisdiction possibly differing in each context and depending upon whether prescription or also enforcement is in issue.

2. "Jurisdiction" has several meanings. "Jurisdiction" is sometimes used as a synonym for "sovereignty". Because it is an aspect of sovereignty and springs from the concept of sovereignty, which originally implied exclusive power as against all other international persons over all territorial affairs,2 jurisdiction is equated to sovereignty. It is arguable, for example, that in the Ottawa Convention (on Anti-Personnel Mines) the term "jurisdiction," used together with "jurisdiction or control," refers to State Parties having either sovereignty or control as the basis for duties under the Convention.

3. "Jurisdiction" has also acquired an expanded meaning so as to apply to State conduct (entailing correlative State responsibility) both within a State's territory and extra-territorially if certain conditions are met. Regrettably, especially in a Council of Europe context, the criteria for "jurisdiction" (and consequential correlative State responsibility) are unclear because of conflicting and uncertain jurisprudence of the European Court of Human Rights (the judicial organ of the Council of Europe).3 The principle laid down in Loizidou v. Turkey (1995) and confirmed in Cyprus v. Turkey (2001) of effective overall control of any territory (whether national or inside a third State) leading to jurisdiction has been whittled down in Bankovic´ v. Belgium (2007) 44 E.H.R.R. SE5. The Court held that the Convention was not designed to be applied throughout the world, even in respect of conduct of Contracting States, and operates in an essentially regional context, notably in the legal space (espace juridique) of the Contracting States. On Bankovic's reasoning, there is not Contracting State liability outside such space. Other judgments, however, impose liability and hold that there is jurisdiction when States exercise authority and control through operating agents and perform acts of a kind prohibited in their own territory (Issa v. Turkey (2005) 41 E.H. R.R. 27). As of today, the scope of extra-territorial jurisdiction has not decisively been settled even by the principles set out in Al-Skeini v. UK (55721/07) (2011) 53 E.H.R.R.18. That case, and Sargsyan v. Azerbaijan, Decision, [GC]. 14 December 2011, treated "jurisdictional competence" as "primarily territorial," while accepting (following Ilascu and Others v. Moldova and Russia [GC] no 48787/99, 4 July 2001) that there were exceptional situations where a State might be prevented from exercising its territorial jurisdiction and thus not incur responsibility subject to any positive obligations it may have undertaken.

4. The situation resulting from the various judgments is that there can be uncertainty as to whether there is jurisdictional responsibility in case even of territory of the sovereign State, as well as uncertainty whether a State has jurisdiction when it acts territorially outside the Convention legal space.

5. The explanation proffered at p.3 of the Memorandum regarding Article 1 declares that the reference in the new proposals

"to the concept of "jurisdiction" instead of "territory" to define the Convention's geographical scope of application is in line with general public international law".

Several points need making:

(a) International law is by no means clear as to the scope of the concept "jurisdiction". Using that term will introduce uncertainties as to whether or not, and on what principles, a State enjoys "jurisdiction" and whether the Convention applies – as opposed to the existing position where it clearly applies "in the territory of each Party".

(b) Is it desired that States be obliged to protect data extraterritorially? And to what extent? Does the amendment go so far as requiring this universally?

(c) Is it desired that States be obliged to permit the free flow of data, ignoring national borders (by virtue of the proposals that they shall ensure this) ?

(d) Is it also desired, that States be incapable of restricting data flows within their own territory where a third State has temporarily usurped "jurisdiction" or "effective overall control"? It appears from the ECHR case law on declarations, reservations and the territorial clause that the ECHR will not interpret a declaration respecting restriction of a State's obligations within its territory.4 Accordingly, Article 24 of the Convention may not assist the ROC in restricting data flows to the "TRNC", should it wish to do so. Indeed, ROC will incur State responsibility for performing to Convention standards in the "TRNC", especially as the Court's jurisprudence on exempting occupied States from responsibility is uncertain in scope (cp. Ilascu, supra). In addition, Article 25 provides that no reservations may be made.

(e) Is it desirable that the complexities of the concept of "jurisdiction" be adopted (instead of the criterion being "territory"), thereby introducing uncertainties as to the fact of jurisdiction and the principles according to which this is to be assessed?

(f) Is it desirable to complicate the applicability of the Convention with issues arising out of modern developments regarding "jurisdiction" (i.e. competence is accompanied by correlative State responsibility)? This point is made having regard, inter alia, to:

(a) The existence of conflicting authorities as to whether there must be a genuine link (sufficiently close connection) to justify a State in regulating the matter and possibly overriding any competing claim to jurisdiction by another State.

(b) The fact that some States, particularly the USA, seek to apply their laws extra-territorially and protectively wherever conduct outside their borders has consequences within these which the State reprehends, although that "effects" doctrine has been modified by a need to take into account a balancing, but only through diplomatic negotiations, of other States´ interests and the nature of the relationship between the actors concerned and the State purporting to exercise extra-territorial jurisdiction;

(c) Some jurists argue that criminal jurisdiction can be universal – quite apart from cases involving piracy and war crimes etc;

(d) The matter can be further complicated by the fact that, where foreign elements are involved, the grounds for exercise of jurisdiction are not identical in the cases of public international law and of conflict of laws (private international law); and

(e) National constitutions of federal States may also result in disputes about jurisdictional competence.

6. Thus, introducing the concept of "jurisdiction," unless carefully defined and limited, into the Convention as respects its object and purposes could cause:

(a) major problems of interpretation and application;
(b) potentially enlarge the scope of its application (and consequential State responsibility) far beyond that of the existing
Convention and Additional Protocol; and
(c) lead to possibly unwanted complications regarding applicability of the Convention in the "TRNC" and as regards its inhabitants. If "jurisdiction" is substituted and should Turkey ratify any Additional Protocol (or modernized Convention), she will have "jurisdiction" and will be vested with Convention rights and duties vis-à-vis the "TRNC".

7. Another complexity: there is ambiguity in the phrasing of the proposed draft amendments

There are indications in the Memorandum in relation to Article 3 (Scope) that the introduction of the concept of "jurisdiction" is

"to apply the Convention to any processing … subject to the jurisdiction of a Party",

leaving still to be examined the question of processing carried out by controllers who are not subject to the jurisdiction of a Party (comments on Article 3 Scope, at p.4). The relevance of the term "jurisdiction" would thus initially be to bind all State Parties to apply the Convention

"to data processing carried out by any controller subject to its
jurisdiction".

In that context, "jurisdiction" is being used (in accordance with ECHR post-Loizidou jurisprudence) to cover cases where, in territory of the regulating State and in territory of a third State the regulating State has sovereign competence or effective overall control. The jurisdictional linkage is the ratio for applicability of the Convention. That concept of "jurisdiction", extending State obligation to regulate conduct beyond its national borders, is indeed consistent with the explanation in the Memorandum as to the Convention's "geographical scope of application" (p.3 dealing with the replacement for Article 1 on "Object and purpose). Obviously, the concept of "jurisdiction" in those contexts is that developed by the ECHR in the line of cases from Loizidou v. Turkey (1995) to Sargsyan v. Azerbaijan (December 2011), especially as the Convention is proposed to protect rights to protection of personal data and to privacy. Accordingly, the Convention as a whole (having regard to Article 1 on "Object and purpose") will apply not only in the territory of each Party, but also in relation to any area (whether of a Contracting or non-Contracting Party) where any Party has effective overall control (thereby incorporating all the interpretation and application problems of the ECHR's jurisprudence on "jurisdiction").

8. Nonetheless, some ambiguity remains because of the way the new Article 1 (Object and purpose) is phrased. In that Article, the focus is on securing for every individual the right to protection of personal data and particularly their right to privacy. As the Article is worded, the phrase "subject to the jurisdiction of the Parties" immediately follows on "every individual," being however bounded on either side by commas. Does this phrase qualify the words "every individual"? If "yes" then it is only individuals subject to the Parties´ geographical or personal or possibly "effects" jurisdiction who are to be protected. If "no," then the protection covers all

individuals, but subjects them to the jurisdiction (competence) of the Parties, possibly collectively. That the latter meaning applies is indicated by the fact that in Article 2 of the Additional Protocol (dealing with when transborder i.e. international, flows of personal data are permissible to a recipient not subject to the jurisdiction of a High Contracting Party and providing for safeguards) the term "jurisdiction" was used (and is still retained) in the sense of "legal competence" to prescribe or enforce legislative, judicial and executive regulation coupled with provision that, in the event of absence of such competence, there is to be strict provision for safeguards. In the proposed amendments (new Article 12 for which alternative proposals are made) "jurisdiction" continues to be used, but the effectiveness of the safeguards appears to be reduced (cp. Details of new Article 12 with old Article 12 and Additional Protocol Article 2).

9. It is suggested that the new Article 1 needs clarification as to whether it covers:

(a) every individual subject to the jurisdiction of the parties; or
(b) every individual, and all such individuals are subject to the jurisdiction of all, or each, of the Parties, or subject to both.

10. Such clarification involves significant policy decisions because, while the Convention is intended to extend data and privacy protection, it also provides for States to limit such protection. The language of the European Convention on Human Rights and ECHR jurisprudence is used in new proposed Article 9 (Exceptions and restrictions), but such language has been very extensively interpreted by the Court to allow States a broad margin of appreciation to restrict rights. Their discretion to restrict rights of data protection and privacy or, conversely to apply them extensively, is thus very considerable e.g. when national authorities contend there is a "pressing social need", and they adduce reasons which appear "relevant and sufficient" to justify exceptions to the Convention Articles governing legitimacy of personal data processing (especially sensitive data), data security and transparency of processing (see text of new Article 9.).

Conclusions

11. The MFA should cautiously consider whether the benefits of extending the protection of the Convention (assuming the scope of the extension is clarified by some rephrasing of the proposals) is in ROC's interest. The Convention now applies "in the territory" of ROC and of other State Parties (old Article 1). The 1960 Constitution (in particular Articles 15, 16 and 17) ensure privacy to all persons in ROC and the ROC's data protection Laws also give protection.

12. If the Convention is amended, there will be potential problems as to

(i) the competing jurisdiction of Turkey, the Occupying Power, in the "TRNC", where Turkey has overall effective control;

(ii) difficulties in applying the ECHR concept of "jurisdiction", itself uncertain in scope and application due to conflicting judgments by the ECHR;

(iii) encouragement to lawyers to mine a broad golden seam by litigation, which does not appear to be in the public interest, especially in relation to data protection and data flows to the occupied area.

13. This appears to be a case where the relevant Council of Europe Consultative Committee, pursuing the policy of modernization, has transgressed the practical rule: "If it isn't broke, don't fix it". The Committee should tactfully be encouraged to continue examining the subject – especially as there has been extensive public consultation (probably much of the response being by computer interests and nerds) – but ROC faces more than enough legal problems without involving itself in a "modernized" Convention which will increase uncertainty in the spheres of data protection, privacy, freedom of information and freedom of expression. All these concepts are doubleedged: they accord rights to individuals, but they can also impact adversely on the rights of other individuals.

C. Palley
10 May 2012

CZECH REPUBLIC / *REPUBLIC TCHEQUE*

Generally

Although the Czech Republic has already presented some proposals for amendments at the T-PD meetings, for the sake of clarity they are included in this text. The proposals follow Guideline 18 of the Joint Practical Guide of the European Parliament, the Council and the Commission for persons involved in the drafting of legislation within the Community institutions[5] and also Chapter II.IV of the Manual of Precedents for acts established within the Council of the European Union.[6]

Proposals for amendments

In Article 2 letter c shall be replaced by the following:
"c. "data processing" means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction; if personal data are generated either through automated means or by intellectual effort, then such operation means processing;"

Explanatory note:
The term "collection" undoubtedly covers the beginning of the processing of personal data and the very moment from which the regulation should apply—for processing based on collection of personal data from data subjects or receiving already existing data from another controller or someone else. Such a situation—as far the applicability of the regulation is concerned—is clear. Unclear is the starting moment for the applicability when personal data are created by whom is carrying out the further processing, especially by technical means' performance—such as video surveillance systems, smart devices systems using sensing applications, geolocation, usage-based billing, access control and advance monitoring in general.
Clear reference to, and absolute clarity of, the concept of processing is crucial for the implementation of the Convention, especially supervision. It is of the same importance for subjects responsible pro processing or taking part in it.
In Article 5(2)(a) the word "explicit" shall be replaced by "provable".

Implicit consents shall be also considered as valid. Almost every contract includes a lot of personal data; it is of no usefulness to enumerate them explicitly. Instead, the capability of being demonstrated or logically proved is essential; the form which it takes may vary depending on technology or means of processing. This change also provides for technological neutrality and addresses another key characteristics of the data subject's consent—that the consent must be proved later.

In Article 5(2)(a), the words "specific and" shall be deleted.
See above.

[5] http://eur-lex.europa.eu/en/techleg/index.htm
[6] http://ec.europa.eu/translation/documents/council/manual_precedents_acts_en.pdf

In Article 5(2)(b), the words “or contractual obligations binding the data subject” shall be deleted.

The Convention 108 distinguishes between “consent” and “contract”. But every bilateral contract consists basically of two parties’ consents together. So does a “consent” which is within the meaning of the Convention 108 bilateral legal negotiation between a data subject who gives consent and a data controller who accepts it. Therefore this artificial difference should be abandoned.
The following words shall be added to Article 5(3) (d): “personal data established as inaccurate shall not be disclosed unless rectified or marked appropriately”.

The provision is inadequate. There is a need to provide for the quality in situations when personal data are to be transferred, more precisely to prevent controllers and processors from transferring personal data of the known inaccuracy.
The following letter shall be added to Article 5(3):
“(f) lawfully published personal data”.

Republishing is legitimate purpose of data processing. Art. 5(1) has no meaning there. Although Art. 5(2) (b) puts a space for domestic legislation, it is better to put it there expressly.
The following paragraph shall be added to Article 6:
“3. Processing of data relating to criminal convictions or related security measures may be carried out either under the control of the public authority or when processing is necessary for compliance with a legal or regulatory obligation to which a controller is subject, or for the performance of a task carried out for important public interest reasons, and in so far as authorised by the Member State law providing for adequate safeguards. A complete register of criminal convictions shall be kept only by the public authority.”

Sensitive data processing nature is relative. Some sensitive data in some context are not sensitive at all and vice versa.

The following paragraph shall be added to Article 6:
“4. Conditions set up in paragraph 1 shall apply for processing of any set of personal data including unique identification data together with any data concerning private life of data subject.”

Sets or combinations of personal data generally perceived as directed at data subject’s vulnerability are made subject to stricter rules.
Article 9(1)(a) shall be replaced by the following:
“a. protect national security, public order, the national economic and financial interest or the suppression of criminal offences”.

Standard preventive measures consist of national security and public order. Since this wording is traditional, specification: “when such derogation is provided for by law” has no meaning there.
It could not be agreed on the prevention of criminal offences inclusion, since this is misused for lowering of human rights, especially privacy an human dignity by CCTV, exploring DNA etc.
Article 25 is **under question**:

Is Art.19–23 of the Vienna Convention on the Law of Treaties applicable to the Convention 108? The important decision concerning the mentioned problem should be taken. In case the Vienna Convention on the Law Treaties is applicable, Art. 25 of the Convention 108 should be deleted.

ESTONIA / *ESTONIE*

In general Estonian Data Protection Inspectorate agrees with the proposals for modernisation of the Convention for the protection of individuals with regard to automatic processing of personal data. Here follows the opinion of the inspectorate.

Article 1
Fully support the new wording of Article 1.

Article 2
We support the decision not to change/amend the definition of "personal data". Article 2.e introduces a new definition "recipient"; according to our opinion there is no need for it.

Article 6
Article 6.1.b and c are partly overlapping, there seem to be examples of discrimination in Article 6.1.b, while Article 6.1.c also refers to discrimination.

Article 7
We support the amendments to Article 7.2, which present a clear criteria to the circumstance of obligation to notify ("... violation ... which may seriously interfere with the fundamental rights and freedoms of the data subject").

Article 8bis
Inspectorate does not support adding this article to the Convention. It is our opinion that it creates considerable amount of administrative burden. Therefore, we suggest that the parties to the Convention should have full power of decision how to regulate it in national law.

Kaja Puusepp
Supervision Director
Estonian Data Protection Inspectorate

FINLAND / *FINLANDE*

30.5.2012

COMMENTS OF THE FINNISH T-PD DELEGATION ON THE PROPOSAL CONCERNING MODERNISATION OF CONVENTION 108 T-PD BUR(2012)01 Rev2

Data protection is under a major review in Europe. In addition to the modernisation of Convention 108 also the Regulation on Data Protection, which aims to modify the Directive 95/46/EC, is under way within the European Union. On that account Finland considers that it is difficult to make specific comments about the proposal prepared by the bureau of T-PD so far as this proposal raises a question of its compatibility with the current European legislation in force as well as with the work in progress within the European Union.

Taking into account this situation Finland will pay attention to some general aspects.

1. Right of access to official documents

The principle of open government is one of the most fundamental societal principles in Finland. Moreover, the right to have access to official documents held by public authorities has also been confirmed in the Council of Europe Convention on Access to Official Documents. Consequently we feel that the proposed amendments to the convention should be developed so that it safeguards the principle of open government and national legislation relating to public access to documents. This ought to be done through the introduction of an operative article on the matter which would empower national authorities to take account of their national legislation on public access, if such rules exist, and the said convention on Access to Official Documents.

2. Processing of sensitive data (Article 6)

The structure of paragraph 1 of article 6 needs to be revised. Sub-paragraph c, when read in conjunction with the first part of paragraph 1, does not form a comprehensible provision. Finland would like to know what data the word “their” refers to in sub-paragraph 6.1c. Does it refer to certain categories of personal data? If so, what are these categories?

The risk of discrimination is mentioned in sub-paragraph 6.1c as an example of a serious risk to the interests, rights and fundamental freedoms of the data subject. Finland would like to get more information about the other risks covered by this sub-paragraph.

3. Supervisory authorities (Article 12bis)

What kind of administrative offences does article 12bis 2c.refer to?

FRANCE

30 05 2012

FRANCE

Remarques générales

Le travail de modernisation de la Convention 108 doit être salué tout particulièrement en raison de l'approche qui consiste à maintenir le caractère général et technologiquement neutre de la Convention et son ouverture.

A cet égard, il parait important que le projet de texte mette clairement en avant dans ses visas notamment, sa volonté d'ouverture à d'autres Etats, la volonté de coopération internationale sur laquelle il repose, de conciliation avec d'autres droits qui est un point fondamental ainsi que sa volonté d'assurer et de favoriser la libre circulation des informations.

Remarques particulières

Préambule

Les objectifs poursuivis par la modernisation de la Convention 108 visent à permettre l' adaptation de la protection des données aux évolutions technologiques , sa conciliation avec la liberté d'expression ainsi que l'ouverture de la Convention elle-même aux Etats non membres. A cet égard, les aspects de coopération internationale, de conciliation avec d'autres droits, de volonté de favoriser la libre circulation des informations doivent être mis en valeur dans les visas. C'est pourquoi nous proposons une réécriture des visas ci-dessous.

Propositions : les éléments nouveaux figurent en gras

Les signataires de la présente Convention,

Considérant que le but du Conseil de l'Europe est de réaliser une union (inchangé) …….

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention ;

Convaincus de la nécessité de promouvoir les valeurs fondamentales du respect de la vie privée et de la protection des données par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale ;

Convaincus qu'il est nécessaire eu égard à l'intensification et à la diversification des traitements et des échanges de données à caractère personnel , de garantir la dignité **humaine** ainsi que la protection des droits et des libertés fondamentales de chacun, notamment au moyen du droit de contrôler ses propres données et les usages qui en sont faits ;

Reconnaissant que le droit à la protection des données doit être concilié avec les autres droits de l'homme et les libertés fondamentales dont la liberté d'expression ;

Estimant que le respect de la protection des données et des libertés fondamentales favorise la libre circulation de l'information entre les peuples et requiert une législation appropriée et une coopération internationale ;

Rappelant que la présente convention est à interpréter en prenant dument en considération le rapport explicatif y relatif.

Article 2 a .Définitions.
Le rapport explicatif devrait être renforcé sur la notion de personne identifiée ou identifiable. Nous proposons de rajouter la précision suivante : « une personne peut être rendue identifiable par exemple, par référence à l'utilisation d'un numéro identifiant, de données de localisation, d'un identifiant internet comme par des caractéristiques physiques, physiologiques génétiques, mentales, économiques, culturelles ou sociales ».

Article 3 Champ d'application
Le rapport explicatif devra expliciter clairement que le nombre de personnes auxquelles les données sont divulguées ne permet pas nécessairement de déterminer si le traitement relève ou non d'une activité personnelle ou domestique. Il devra ainsi expliciter le fait que la Convention ne recouvre pas des activités « hybrides » dans lesquelles l'objectif principal est une activité personnelle (par exemple les individus qui vendent des objets en ligne), si tel est l'objectif poursuivi par la Convention.

Article 4 Engagement des parties.
Du fait des dernières modifications apportées à cet article, il trouverait mieux sa place dans le chapitre 1 « dispositions générales ». Il prévoit en effet que les Etats doivent prendre les mesures nécessaires en interne pour donner effet aux dispositions de la Convention dans son ensemble et non pas aux seules dispositions relatives aux principes de base de la protection des données définis au chapitre II.

Article 5- Qualité des données.
Le rapport explicatif devra préciser si les finalités statistiques, historiques ou de recherche scientifique visées sont les seules finalités considérées comme compatibles. Certains traitements peuvent en effet avoir des finalités « secondes » compatibles qui ne sont pas pour autant des finalités historiques, statistiques ou de recherche.
Il devrait aussi rappeler que les traitements ne peuvent être compatibles avec la finalité initiale que s'ils sont effectués en respectant les principes posés par la Convention.

Article 7 Sécurité des données.
L'obligation qui pèse sur le responsable de traitement est plus large que celle prévue par l'intitulé de l'article. Elle couvre aussi la sécurité des traitements afin d'éviter tout traitement illicite des données.
Il conviendrait donc de compléter le titre de l'article en ce sens pour le mettre en adéquation avec le contenu de l'article. Enfin, nous proposons de rajouter la divulgation qui se distingue de la diffusion des données.

Propositions de modification (en gras dans le texte):
Article 7 **Sécurité des traitements et des données.**

Rajouter dans la fin de la dernière phrase du I : «…. ainsi que contre l'accès, la diffusion **ou la divulgation** non autorisés des données à caractère personnel traitées ».

Le rapport explicatif devra aussi préciser que seront définies les conditions dans lesquelles un responsable de traitement est tenu de notifier la violation de données à caractère personnel.

Article 7 bis
Le principe de transparence est un principe nouveau dans la Convention. Aussi il serait utile d'une part de faire apparaître clairement dans la rédaction de l'article que la transparence repose sur l'obligation d'information par le responsable de traitement et d'autre part que cette obligation nécessite qu'un certain nombre d'informations listées dans l'article soient fournies.

Nous proposons donc de modifier la rédaction de l'article pour le rendre plus impératif, en remplaçant « et en particulier fournit » par « en informant les personnes concernées de … ».

En complément nous proposons que soient insérés directement dans l'article, et non pas dans le seul rapport explicatif, l'information relative aux transferts de données afin d'être cohérent avec le fait que l'on intègre dans la Convention les aspects « transferts de données ».

Le texte serait alors: « Chaque partie prévoit que le responsable de traitement **assure** ~~garantit~~ la transparence du traitement des données ~~et en particulier fournit~~ en **informant** les personnes concernées de…… les moyens d'exercer les droits énoncés à l'article 8, **sur les transferts vers des Etats** (préciser lesquels)…… » .

Enfin il serait utile que le rapport explicatif prévoit des cas de limitation de cette obligation d' information par exemple pour les traitements de sécurité publique ou de recherche et poursuite d'infractions pénales ou pour des traitements spécifiques tels que ceux qui prévoient une anonymisation des données très rapidement ou pour les traitements de lutte contre la fraude pour lesquels l'information peut être générale et ne pas comporter l'ensemble des informations listées.

Article 9- Exceptions et restrictions.
Nous proposons dans la première phrase de supprimer « de base » qui semble introduire un distingo entre plusieurs catégories de principe.

Proposition de rédaction :
« 1. Aucune exception aux principes ~~de base~~ énoncés au-… »

Article 12. 2 Proposition rédactionnelle. Nous proposons de couper la phrase en deux et de modifier la fin du paragraphe.

« Lorsque le destinataire relève de la juridiction d'une Partie de la Convention, le droit applicable à ce destinataire est présumé assurer un niveau de protection adéquat**.** Une partie ne peut (….) mise à disposition des données, **sous réserve des pouvoirs du Comité conventionnel prévus à l'article 19**. »

Article 12 3 dernier paragraphe.
Nous proposons de modifier la dernière phrase. La rédaction pourrait être « L'autorité peut le cas échéant suspendre, interdire ou soumettre à condition **ces mesures juridiques encadrant** la communication des données et leur mise à disposition ».

Article 12 bis 2 c : Le rapport explicatif devra préciser le sens de « et notamment sanctionner les infractions administratives ».

Article 12 bis 5 : Remplacer dans le texte français «autonome » par « indépendante »

GERMANY / *ALLEMAGNE*

30 May 2012

Comments of the Federal Government regarding the planned overhaul of Council of Europe Convention 108

I.

The Federal Government is convinced that Convention 108 and its principles have proved satisfactory in the 30 years of their application and have contributed significantly to ensuring data privacy in Europe and in non-European countries.

In an increasingly globalized world and highly complex information societies, data protection requirements have changed over the years. Therefore, the Federal Government welcomes the initiative to revise Convention 108 and to identify parts that may require modernization and adjustments to meet new challenges and needs.

The Federal Government expressly welcomes the objective of the reform project which is to create a universal set of data protection rules setting global standards; it also welcomes the efforts to dovetail the reform process with the one regarding the new data protection framework in the EU.

II.

The Federal Government finds it important to drive the reform efforts at the level of the Council of Europe forward while the negotiations in the EU are ongoing. Germany and the other Member States share the responsibility for making sure that the two new sets of rules are compatible. Therefore, the Federal Government is prepared to make an active and constructive contribution to the envisaged further negotiations of the proposals to reform Convention 108 in an Ad Hoc Committee. This Committee needs enough time to also discuss - in sufficient depth - questions of a general nature. Further negotiations should however aim to put the reformed Convention 108 into effect as soon as possible, while dovetailing the CoE Convention reform process with the one regarding the new data protection framework of the EU. It does not seem necessary, though, to wait until the considerably more complex and more detailed reform plans of the EU have been finalized.

III.

Negotiations regarding the European Commission's proposals for a General Data Protection Regulation and a Directive Governing the Law Enforcement Area have already begun. Against this backdrop, the following issues are of particular importance to the Federal Government:

1. We should stick to our approach which is to keep up the general character of Convention 108. This is the only way to enforce the universal standard the Convention pursues and to ensure that it has a comprehensive scope (public and private sector).

2. The Contracting Parties of the new Convention should be entitled, as they are under the existing one, to regulate data protection for the public sector and that for the private sector in different manners. Also, the Council of Europe should consider whether it would make sense to make a distinction to this effect in the Convention itself, especially because the constitutional situation for these two sectors differ.

3. Against this backdrop we will have to look at the new regulations in greater depth to see whether they meet the particular requirements of specific public sectors such as the processing of data in criminal investigations and criminal court proceedings, in other court proceedings or in administrative social security proceedings.

4. The Federal Government expressly welcomes the current approach pursued by the reform proposals which is to identify further fundamental rights to be balanced against the right to data protection.

5. Ultimately, all new provisions must therefore be measured against their ability to cater for Internet applications or other technical framework conditions, including new developments and services such as cloud computing. Also, they need to be evolutionary and capable of accommodating all sorts of technologies.

6. We should consider including a catalogue of Internet-related user rights, what with the capabilities of the Internet and users' particular need of protection vis-à-vis providers which frequently act internationally. These user rights could add to the principles already contained in the Convention and flesh out the relationship between providers and users in the private sector.

7. We should look at whether a distinction could be made between data processing entailing a smaller threat to privacy and processes generally representing a greater threat, a basic approach already contained in Article 6 (1) and Article 8 bis (4) of the Draft Convention.

8. A sound balance needs to be struck between the basic rights of freedom of expression, freedom of the press and freedom of information on the one hand and the particular threats to the privacy of data subjects on the other. It is not least against this background that we should consider including a separate provision governing the disclosure of data.

9. We should check to what extent anonymized data may suffice to achieve certain objectives, and whether data may be categorized according to their degree of de-identification, so that pseudonymized data may be put to a greater use than direct personal data, for instance.

10. Article 6 bis (6) of the Draft Convention seeks to avoid excessive burdens on smaller and medium-sized enterprises. That said, the entire Convention should be checked once again for whether it balances, adequately, the privacy interests of data subjects and the administrative burdens arising especially for smaller and medium-sized enterprises.

11. The scope of the exception in Article 3 bis (exception for purely personal or household activities) needs to be discussed further, as it is of general importance and has far-reaching effects.

12. The provisions governing data transfers to third countries also need to be discussed in depth. This is also applicable to the role of data protection supervisory authorities. As regards data transfers by private bodes, i.e. in particular by internationally active enterprises, we should consider creating adequate safeguards, through a yet to be concretized process of regulated self-regulation, making sure that the regulations are actually enforceable. The Council of Europe - together with other international organizations such as OECD or APEC - should look at how to ensure such effective enforcement.

IV.

The Federal Government wishes to submit the following initial comments with regard to Draft T-PD-Bur(2012)01Rev2_en dated 27 April 2012, and reserves the right to submit further proposals following closer scrutiny:

Preamble
We welcome the fact that Recital 3 is no longer restricted to the reconciliation of privacy and the right to freedom of expression and freedom of information, but **also** refers **to further fundamental rights**. The Federal Government suggests to flesh out the Recital in the Explanatory Memorandum by stating cases where the right to data protection or right to privacy needs to be balanced against other fundamental rights (e.g. data processing on the Internet).
Generally speaking, the Federal Government recommends giving the Explanatory Memorandum more weight, for instance by mentioning, in the Preamble, that the Explanatory Memorandum offers the Contracting Parties help in interpreting Convention 108 through, among other things, concrete examples.

Article 1 – Object and purpose
Generally, the Federal Government holds no objections against using the term "**jurisdiction**" in Article 1, it being more appropriate than "territory" in the Internet age. However, we have not yet been able to assess the concrete legal implications the change in terms might have. The Federal Government recommends including, in the Explanatory Memorandum, particularly diligent explanations of the legal term chosen in this respect, both with regard to Article 1 and the chapter on trans-border data flows (currently Article 12 or 12ter) - a stance already voiced at the T-PD General Assembly.

„Right to data protection“
The newly included reference to the "right to data protection" as opposed to the "right to privacy" in the current Convention is not designed to bring about any substantial changes, but aims to clarify the objectives. However, the Federal Government fears that the new wording (“the right to the protection of personal data, thus ensuring the respect for their rights and fundamental freedoms, and in particular their right to privacy“) might actually make matters unclearer: Firstly, the Federal Government finds it difficult to draw the line between the "right to data protection” and the “right to privacy“. We will not be able to resolve, in the framework of Convention 108, the uncertainties existing in this context. In the German understanding, the right to data protection is derived from the right to privacy: Data protection is based on the right of the individual to determine the use of their personal data, which is one dimension of the general right to privacy.

Furthermore, Article 1 refers to the - more general - "rights and fundamental freedoms, after mentioning the "right to data protection", which seems slightly unsystematic. As we see it, it would make more sense to first mention the general rights to be followed by the more specific ones. Against this background the wording used in the existing Convention seems preferable. Alternatively, the phrase “thus ensuring their fundamental rights and freedoms“ could be deleted, as its added value is not quite clear and as it complicates Article 1.

Gender-neutral language
The Federal Government welcomes the gender-neutral language used throughout the Draft Convention.

Article 2 - Definitions
The definitions still need to be discussed in depth. It might be expedient to copy definitions from EU Data Protection Directive 95/46, as these are currently discussed thoroughly at EU level. We therefore suggest postponing the definition issue for the time being.

Article 3 - Scope
Provisions to cover public and private-sector bodies:
It is true that, also from the Federal Government's point of view, general data protection principles apply to private- and public-sector bodies alike. At the more specific level, though, the German law distinguishes between private-sector and public-sector bodies, as laid down in the Federal Data Protection Act ("Bundesdaten-schutzgesetz"). A great number of sector-specific regulations apply only to public bodies. Against this background, the Convention should only drop the distinction between private and public bodies if and when it upholds a sufficiently abstract nature and continues to give the Contracting Parties enough leeway to make the necessary distinctions at national level. A distinction within the Convention seems preferable for all fields which are to be spelled out in more detail.

In this context we need to take into account that, in the private sector, other basic rights may tend to clash with the right to data protection, as the general situation here differs from that in the public sector: It is in the nature of things that data processing in the private sector needs to be reconciled with various other fundamental rights.

Some individual provisions such as the ones governing the rights of data subjects in the public sector also need to be put more precisely, in particular with regard to criminal prosecution, crime suppression and social security administration.

Manual data processing
The drafters have dropped the restriction of the Convention's scope to **automated data processing**. The aim is to also cover manual data processing in the future, where the personal data are organized in a structured manner according to specified criteria and allow the search for individual persons. The Federal Government does not hold general objections against widening the scope to non-automated data processing on certain conditions. We should take care, though, to avoid a wording which is out of line with the standard definitions used at EU level.

Also, care should be taken to include adequate special regulations for (paper-based) files coming under the scope of the Convention. This concerns retention periods, the rights of data subjects, and assignments to the archives, for instance.

Exempting “purely personal or household activities“
The Federal Government welcomes the aim of excluding purely personal data processing from the data protection regime imposed on major enterprises, for instance. It is increasingly hard to distinguish "purely personal or household activities“, though, a term which is geared to Directive 95/46. This is especially true in connection with the Internet. We should once again look in depth at the extent to which purely private activities should be subject to other legal consequences.

Article 5 – Legitimacy of data processing and quality of data
The Federal Government welcomes the explicit inclusion of **further** data processing **principles**. This includes the principle of **proportionality** (Article 5 (1)).

Conditions for the lawfulness of data processing are mentioned for the first time in Article 5 (2) - another approach which has the Federal Government's express backing. Nevertheless, distinctions should here be made between the public and the private sector.
As for the rest, we might consider adding further conditions for the lawfulness of data processing. Great care should be taken here, however, that the newly introduced conditions for the lawfulness of data processing do not collide with the regulations that will probably be adopted at EU level (Article 6 of the Draft Regulation).

The new wording in Article 5 (3) lit. c "and limited to a strict minimum“ is striking and needs further scrutiny.

Article 6 – Special categories of data
The Federal Government welcomes the fact that the Council of Europe is looking at ways to make the protection of sensitive data more flexible and effective.
Article 6 does not contain a strict catalogue of sensitive data the processing of which is generally prohibited; instead, it refers to three basic situations where it can safely be assumed, as a general rule, that the data is sensitive ("by their nature“, "by the use made of them“, "where their processing presents a serious risk“). What is new is the Convention's context-based approach, which, from Germany's point of view, could be emphasized even more strongly. Furthermore we doubt that it makes sense to relate individual data categories to the three case categories referred to in Article 6 (1) lit. a to c. For this reason the Federal Government holds the view that there is further need for discussion here.
Finally we will have to look at how the current flexible approach pursued by the Council of Europe can be dovetailed with **future EU regulations** regarding sensitive data.

Article 7 - Data security
The Draft Convention requires data controllers to report **severe data breaches**. The Federal Government supports provisions requiring controllers to notify data breaches as introduced at European level by Article 4 (3) of Directive 2002/58/EC. The Federal Data Protection Act ("Bundesdatenschutzgesetz"), in its Section 42a, already requires private bodies to inform the competent supervisory authority and the data subject(s) immediately if and when personal data have been unlawfully revealed to third parties. A similar provision is contained in Section 93 (3) of the Telecommunications Act ("Telekommunikationsgesetz") and Section 15a of the Telemedia Act ("Telemediengesetz").

Reporting requirements do not come under data security, but begin to bite once data security has been breached. For this reason, reporting requirements do not necessarily have to be included in Article 7.

It might be helpful if Article 7 contained not only reporting requirements vis-à-vis the data protection supervisory authorities but also vis-à-vis the **data subjects** affected by the data breach, possibly under stricter prerequisites.

The purpose of such a regulation is first and foremost to inform data subjects of data breaches they would not otherwise have learnt of. This is the only way for them to avert further damage and to invoke their data protection rights as data subjects and claim for damages, where appropriate. Article 32 of the EU Draft General Data Protection Regulation also requires data controllers to inform data subjects of any personal data breach.

Article 7 bis – Transparency of processing
The new provision seeks to ensure the **transparency of data processing** from the data subjects' view - an objective we expressly welcome. We should look at whether and to what extent this provision could be supplemented and put in a more concrete manner in line with the general character of Convention 108.

Article 8 – Rights of the data subject
Right of access, Article 8 lit. d
Improving access rights generally increases transparency - a stance which has our general support. However, Article 8 extends the right of access to the source of the data and the "reasoning underlying the data processing". This needs to be discussed in more detail. The same holds good for the wording with regard to the overhaul process at EU level.

Right to object to data processing, Article 8 lit. b
From the Federal Government's point of view, the current design of the general right to object to the processing of personal data needs to be looked at thoroughly. The legitimate interests of the data subjects, of the controller of the files, and, where appropriate, of third parties, need to be reconciled adequately with basic rights such as freedom of expression, freedom of research, or the freedom to conduct a business. Furthermore, we need to discuss how data subjects can actually implement or exercise their right to object to the processing of personal data concerning them.

Article 8 bis – Additional obligations
This Article contains a number of innovative elements which generally have the Federal Government's backing. This applies in particular to the risk analysis in paragraph 2 and the privacy-by design principle laid down in paragraphs 3 and 5. That said, the details still need to be discussed thoroughly.

In Germany, the privacy-by-design principle is contained in Section 3a of the Federal Data Protection Act. The Telemedia Act, in its Section 13 (4) and (6), contains legal regulations governing the technical and organizational design of Internet offers.

We should consider including specific privacy-by-design options in Convention 108 itself. This includes above all **anonymization, pseudonymization, early erasure** and **privacy by default**. We should also look in how far software developers and suppliers should be addressed by the Convention.

Risk analysis could be restricted to certain types of data processing which are of a highly invasive nature. The requirements to be met for prior checkings in line with Article 18 of Directive 95/46/EC could serve as a criterion here. Generally, however, it would be useful to distinguish between the public and the private sector. Risks or disadvantages for the data subject tend to be high where sovereign action is concerned, which is why most of them are already governed by sector-specific regulations. This applies in particular to the police and justice fields.

With regard to the **accountability principle**, the Article 29 Working Party has already done a valuable job (e.g. WP 173 of 13 July 2010). The principle is already contained in the 1980 OECD guidelines and has most recently been included in the Madrid Resolution and Draft ISO 29100. Nevertheless, it has turned out that not all measures are equally appropriate to ensure compliance with data protection provisions. Therefore, the Convention should not go into the accountability measures in detail, but leave the Contracting States enough leeway for their own ideas.

Great care needs to be taken to dovetail the proposals regarding 8 bis with the process at EU level to overhaul the European Union's data protection law.

Article 9 – Exceptions and restrictions
The Draft Convention upholds the possibility to allow exceptions from certain regulations contained therein in order to protect **public or state security**, the **prevention and suppression of criminal offences**, and with regard to data processing for statistical purposes or for the purposes of scientific research. The Federal Government welcomes the fact that another provision has been added to the list of regulations from which Contracting States may deviate (Article 7 (2), reporting requirement in data breach cases), because such a requirement would cause problems when it comes to criminal proceedings and the work of intelligence agencies. It might be useful to provide exceptions also for the obligations arising from Article 8 bis.
As regards Article 9 (2) we should look at whether the phrase "obviously no risk of an infringement“ is still adequate for the amended provisions to which the catalogue of exceptions now refers (e.g. new Article 6 (1)). Would it not be more useful to relate to cases "where domestic law provides for appropriate safeguards”, as laid down in Article 6 (2)? How is Article 9 (2) supposed to relate to Article 6 (2)?

Article 12 - Transborder data flows
The Federal Government shares the view that Article 12 of the Convention and Article 2 of the Additional Protocol need to be overhauled. Designing modern regulations governing transborder data flows is particularly challenging.
The issues arising from the regulation of transborder data flows and its practical implementation need to be discussed thoroughly, namely where this concerns data transfers by Internet services.

For instance, the Draft provides, on the one hand, that data may only be communicated if the receiving state has an adequate data protection level in place. On the other hand, it provides for far-reaching exceptions. This mechanism needs to be looked at thoroughly. The provision itself may prove to be too detailed.

We need to explore whether and to what extent the role of data protection supervisory authorities can be strengthened when it comes to international data transfers. This is particularly true for the public sector, and especially for the police and justice fields.
How are the provisions of Article 12 (3), third sentence, and 12 (5) supposed to relate to one another, as the competences of the supervisory authorities mentioned therein overlap? Furthermore, we would have to clarify how the supervisory authorities could enforce the obligations mentioned in Article 12 (3) third sentence ("demonstrate the quality and effectiveness of actions taken“) vis-à-vis recipients in a third country.

We welcome the accountability principle on the part of the recipient as laid down in Article 12 (3). This principle would be difficult to enforce in practice, though, if and when transborder movements of personal data within the meaning of Article 2 of the Additional Protocol are concerned to a recipient not subject to the jurisdiction of a State Party to the Convention. We should therefore explore ways to improve the practical implementation of this regulation.

The German law distinguishes between public and private bodies, both as senders and recipients of personal data - a distinction we find expedient also in this context.

Chapter 4 (Articles 13, 14, 15, 16 and 17) – Mutual Assistance

Chapter 4 has so far undergone just one major change: The Contracting Parties should now designate **supervisory authorities** as the competent bodies for consultations among the Contracting Parties or as the point of contact for data subjects - a proposal which needs to be looked at in depth.

We generally welcome the idea of improving the coordination among the supervisory authorities. The general issue that needs to be resolved, though, is reconciling coherence and a uniform enforcement with the independence of the data protection supervisory authorities

Chapter 5 (Articles 18, 19 and 20) – Consultative Committee

Chapter 5 provides for the establishment of a Consultative Committee. We welcome the proposal to develop further its standard-setting functions. However, the Contracting Parties themselves should also play a key role here. It does not seem useful for the Committee to take on a dispute resolution role - a task better left to the existing Council of Europe bodies, notably the European Court of Human Rights. The valid version of the Convention already gives the Committee a monitoring function (Article 20 (3) "a report ... on the functioning of the Convention").

IRELAND / *IRLANDE*

Modernisation of Convention 108

Comments on T-PD-BUR(2012)01Rev2 dated 27 April 2012

Overall Comment
There is a risk that the Convention text is becoming excessively detailed and prescriptive and thus increasing the potential for conflict with EU data protection instruments.

Preamble
Recital 2
It is suggested that 'them' should be replaced with 'such data'.

Recital 3
The meaning of 'be considered in respect of its role in society' is not clear.

It is suggested that 'the' before 'freedom of expression' should be deleted.

Recital 4
Most data flows take place between enterprises. We would therefore suggest that 'thereby contributing to …. between peoples' should be replaced with 'thereby facilitating the free flow of personal data'.

Article 1
It is suggested that
- the comma after 'individual'; and
- the word 'the' before 'respect'

should be deleted.

It is suggested that the Explanatory Report might include an explanation in relation to the use and meaning of the word 'jurisdiction' in the text.

Article 2
In order to ensure consistency in the drafting of the definitions, it is suggested that 'shall mean' in the definitions of 'recipient' and 'processor' should be replaced with 'means'.

Article 3
We consider that 1ter is not necessary and would therefore suggest that it should be deleted.

Article 4
An EU Regulation, as proposed by the European Commission in January last, would be directly applicable in Member States without the requirement for domestic law to give effect to it. This needs to be accommodated in the Convention.

Replace 'foreseen' in paragraph 3 with 'provided for'.

Article 5

Article 5.2

We have reservations about the requirement for 'explicit' consent in all cases.

It is suggested that paragraph b should be replaced with the following text:

b. it is necessary for the performance of a contract to which the data subject is a party or prior to entering into such a contract, or

c. it is necessary to comply with legal obligations binding the data controller, or

d. it is necessary for the purpose of an overriding legitimate interest.

Article 5.3

It is suggested that paragraphs a and b should be amended to provide as follows:

a collected for explicit, specified and legitimate purposes;

b processed fairly and lawfully and not processed in a way incompatible with those purposes unless the data subject has given his/her explicit consent or it is provided for by domestic law;

Article 6

We would suggest that 'whether' should be replaced with 'where'.

It is not clear what 'security measures' in paragraph 1a means.

Article 7

Article 7.1

It is suggested that:

- the comma after 'destruction', and
- the word 'processed' at the end of paragraph 1

should be deleted as they are not necessary.

Article 7.2

What does 'violation' mean in this context?

Article 7bis

Article 7bis 1

It is suggested that:

- the word 'forth' should be replaced with 'out';
- the 'a' before 'fair' should be deleted; and
- 'and lawful' should be added after 'fair'.

Article 8

Paragraph a

We would suggest that 'the grounds of' should be deleted as it does not add anything to the text.

Paragraph d

It is suggested that 'in' after 'underlying' should be deleted.

Paragraph f
The scope of the assistance to be provided by a supervisory authority needs to be clearly defined.

Article 8bis

Article 8bis.2
It is suggested that 'foreseen' should be replaced with 'intended'.

Article 8bis.5
It is suggested that –

(i) 'allowing the' should be replaced with 'which facilitate'; and
(ii) 'to be ensured' should be deleted.

Article 9

Article 9.1, paragraph a
It is suggested that 'and suppression' should be replaced with ', detection, investigation and prosecution'.

Article 12

Article 12.4 c
We presume that 'meeting the criteria of Article 9' means that to protect State security, etc. If this is correct it should be spelled out in this Article.

Article 12.4 d
We support the point made by the United Kingdom in document T-PD-BUR(2012)03Mos.

Article 12.6
We would suggest the following changes to the wording of Article 12.6

(i) replace 'foresee' with 'provide'; and
(ii) replace 'to protection' with 'for the purpose of the protection'.

Article 12bis

Article 12bis.2
The meaning of point c needs to be clarified before we could comment on it.

We would also suggest the following amendments:

(i) add 'shall' after 'authorities';
(ii) replace 'are' with 'be' in point a;
(iii) delete 'in particular' in point b;
(iv) replace 'are able to' with 'have power to' in point d.

Article 12bis.3
It is suggested that this Article should be amended as follows:

> Each supervisory authority shall have power to investigate, or cause to be investigated, complaints from an individual concerning the protection of his or her rights or personal freedoms with regard to the processing of personal data within its competence and shall inform the data subject of the outcome of the investigation.

Article 12bis.4 and 5
It is suggested that 'accomplish' should be replaced with 'perform' in both paragraphs 4 and5.

Article 12bis.6
It is suggested that this paragraph should be replaced with the following text:

Decisions of the supervisory authorities may be appealed against through the courts.

Article 12bis.8
It is suggested that ‘forth’ should be replaced with ‘out’.

The meaning of ‘conference’ is not clear.

Article 18
Article 18.3
We would prefer ‘entitled to vote’ rather than ‘voting’.

Article 18.4
Insert ‘a’ before ‘member’.

Article 19
It is suggested that paragraphs e, h and j should state that the Committee
‘shall prepare…’, ‘shall periodically review ..’ and ‘shall do all that is needed’ respectively.

Article 20.3
Is this a standard provision?

Who would vote on behalf of the European Union?

Article 27
Insert ‘of’ after ‘Convention’.

NORWAY / *NORVÈGE*

Modernisation of Convention nr.108

Norway welcomes the proposal for a modernised Convention nr. 108, and we are thankful for the work both the Secretariat and the Bureau have invested in order to present the draft proposal. Please find below the Norwegian comments on the latest draft of a modernised Convention nr. 108.

The protection of data relating to children is of utmost importance, and we believe that the Convention should go further than the current draft when it comes to protecting children's personal data. We propose to include a general provision stating that personal data relating to children cannot be processed in an irresponsible manner contrary to the child's best interest. Such a provision gives the supervisory authorities a possibility to intervene if for example adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child. We have proposed that a provision of the same nature should be included in the EU-rules on personal data protection, and we believe that including such a provision also in Convention nr. 108 will ensure a consistent protection of children's personal data in Europe.

In our view, it is of importance that Convention nr. 108 ensures that the right to access public information at national level can be maintained. We therefore propose that the following sentence is included in the preamble of the Convention, as it was before the latest amendments to the draft: "*Considering that this Convention allows account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to public documents".*

We support a household exemption, cf. article 3 number 1bis. We are, however, concerned that the current wording is unclear. We would therefore welcome a wording that draws a more precise line between private and public use of information, for example by stating explicitly how information has to be used in order for it to be regarded as made accessible to persons outside of the household sphere.

In order to clarify that the legal grounds of processing under the convention are not narrower than under EU-law, we believe that the draft article 5 of the Convention should reflect the legal grounds for processing listed in the proposed General Data Protection Regulation article 6 number 1.

As regards the provision in article 8 a and d, relating to decisions made based on processing of personal data, we believe that this concerns the administrative decisions based on personal data more than the processing of the personal data in itself. We would therefore propose that the T-PD considers whether these provisions should be included in the Convention, also taking the provisions of the proposed EU-regulation into account. We do however support the underlying intention, that data subjects should have the right to be informed of, and have the right to object to, decisions that affect them, which are based solely on the processing of personal data. To clarify the scope of the proposed rules, an alternative could therefore be to draft a separate provision concerning automated decisions based on personal data.

Lise Lehrmann
Acting Legal Adviser

Anne Sofie Hippe
Higher Executive Officer

PORTUGAL

Modernisation of Convention 108

Please find below the Portuguese drafting suggestions:

TITLE
The first drafting suggestion regards the title of the Convention. We suggest that the title should read as follows: **Convention of the Protection of Individuals with Regards to Processing of Personal Data**. The reason is that the limitation of the application of the Convention to automatic data has been suppressed. Therefore from now the convention will be equally applicable to the processing of personal data either by automatic or manual means, meaning that word "automatic" should be suppressed.

Articles

Article 2 – c)
In litter c) of article 2, we are adding the following sentence: "where no automated processing is used, data processing means the operations carried out on personal data organized in a structured manner according to specified criteria allowing search by person concerned."

We strongly advise to, at least, explain this. "Organized in a structured manner" means that the "structure" given to the organization of data may be any, at all. In what "specified" criteria is concerned, the same consideration applies.
Present draft:
"where no automated processing is used, data processing means the operations carried out on personal data organised in a structured manner according to specified criteria allowing search by person concerned;"
Our suggestion:
"Where no automated processing is used, data processing means the operations carried out on personal data organized **in any structured manner** according to **any** criteria allowing search by **the** person concerned."

Article 3 - 1bis)
We suggest for the sake of clarity to add at the end of the sentence: "…namely but not exclusively through social networks offered in the Internet or other kind of networks such as an Intranet."
Present draft:
"1bis This Convention shall not apply to data processing carried out by a natural person for the exercise of purely personal or household activities, unless the data are made accessible to persons outside the personal or household sphere."
Our suggestion:
"1bis This Convention shall not apply to data processing carried out by a natural person for the exercise of purely personal or household activities, unless the data are made accessible to persons outside the personal or household sphere, **namely but not exclusively through social networks offered in the Internet or other kind of networks such as an Intranet.**"

Article 6
For the sake of better clarity and economy of the text, maybe we could redraft it by transferring the safeguards set to in paragraph 2 directly to the existing paragraph 1 and referring to them firstly.
Existing draft:
"1 The processing of certain categories of personal data shall be prohibited, whether such data are sensitive:

by their nature, namely genetic data, data related to health or sexual life, data related to criminal offences or convictions, or security measures;

by the use made of them, namely biometric data, data whose processing reveals racial origin, political opinions [or trade-union membership], religious or other beliefs, or;

where their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

2 Such data may nevertheless be processed where domestic law provides appropriate safeguards."
Our suggestion:
""The processing of certain categories of personal data shall be prohibited, **unless such processing is permitted by law within strict appropriated safeguards**, whether such data sensitive:"
(Litter of paragraph 1 a) to c) remain with its proposed draft, paragraph 2 is eliminated).

Article 8
We suggest including in the Explanatory Report the interpretation of the T-PD of what is to be understood by the word "significantly/significant" used in **paragraph a**).

We start this article by correctly using the word person. All the paragraphs from a) to f) refer to a person (any person being affect by the situations referred to in those paragraphs, without any kind of discrimination) therefore the drafting could be reformulated in order to avoid keep repeating "his/her". We also think it is redundant to say "producing legal effects". If we don't say that, are illegal effects to become acceptable?
Present draft:
"a) not to be subject to a decision significantly affecting him/her or producing legal effects relating to him/her, based solely on the grounds of an automatic processing of data without having the right to express his/her views;"
Our suggestion:
"**a) not to be subject to a significant decision based solely on the grounds of an automatic processing of data without having the right to express his or her views;**"

In **paragraph c**), the words "or not" are not necessary. In fact the logical, necessary, answer to the question "can you confirm?" is "yes" or "no".

The "confirmation", within the draft as we suggest it, means not only the factuality of the existence of the processing but also the justification for such processing to exist.
Present draft:
"c) to obtain at reasonable intervals and without excessive delay or expense confirmation or not of the existence of data processing relating to him/her, the communication in an intelligible

form of the data processed, **all available information on their origin as well as any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7bis;"**
Our suggestion:
"c) to obtain at reasonable intervals, and without excessive delay or expense, **confirmation of the processing of personal data relating to him or her, in an intelligible manner**, all available information on their origin, as well as any other information that the controller is required to provide to ensure the transparency of processing in accordance with article 7bis."

In light of what is proposed to paragraph c), **paragraph d) should be deleted**.

Article (?)
We fully agree with the idea of creation of data protection officers by the parties. However it is not to the Explanatory Report to create the data protection officer.

We propose to add a new paragraph to this article for that effect.
Our suggestion:
"**Parties may, if they so which, provide for the possibility of the existence of data protection officers in Administrations and business, to assist them to implement this Convention and national data protection laws. Those officers may be hierarchically submitted to the heads of administrative bodies and business responsible but should have their independence of judgment respected and should submit reports to national data protection authorities on a regularly basis.**"

Article 12
In **paragraph 1**, we think that the exception should be integrated in the principle. By making that option we are saying, as part of our main statement that though in principle personal data is not to be transferred if an adequate protection is not given. We acknowledge, as normal in democratic law obeying societies, that in very exceptional situations determined by law, either to protect public or private interests, it can nevertheless happen. We think it is very important to make this absolutely clear.
Present draft:
"1 Each Party shall ensure that personal data will only be disclosed or made available to a recipient who is not subject to its jurisdiction on condition that an adequate level of data protection is ensured."
Our suggestion:
"Each Party shall ensure that personal data will only be disclosed or made available to a recipient who is not subject to its jurisdiction on condition that an adequate level of data protection is ensured, **except as provided by law either for private or public reasons, to ensure the protection of human rights or fundamental interests as referred in subparagraph a) of paragraph 2) of article 9).**"

Paragraph 2)
In paragraph 2, we agree that the T-PD is entitled, even now in its nature of consultative committee, to express itself about the compliance of a Party do the Convention with the Convention and, or, additional Protocols. We also agree that the T-PD should be accorded monitoring powers, may be similar, for instance, to those of the OECD in relation to its own Conventions, namely the one against Corruption. However we cannot accept, as members of the European Union, that such a judgment of the T-PD conflict with the jurisdiction of the Institutions of European Union regarding the application of EU legislation. We therefore recommend that an understanding between the Council of Europe and de European Union be

reached in light to have a common understanding about the adequacy of EU members and to avoid treating 108 Convention Parties in an unfair discriminating way.

Present draft

"2 When the recipient is subject to the jurisdiction of a Party to the Convention, the law applicable to this recipient is presumed to provide an adequate level of protection and a Party shall not, for the sole purpose of data protection, prohibit or subject to special authorisation the disclosure or making available of data. The Conventional Committee may nevertheless conclude that the level of protection is not adequate."

Our suggestion:

"2 When the recipient is subject to the jurisdiction of a Party to the Convention, the law applicable to this recipient is presumed to provide an adequate level of protection and a Party shall not, for the sole purpose of data protection, prohibit or subject to special authorisation the disclosure or making available of data."

Second paragraph of subparagraph b) of paragraph 3 of article 12

The use of the word "prohibit" must be clarified in order to made clear that the power of prohibit relates only to illegal acts. In any situation a national data protection authority can prohibit legal a decision made by a public authority. Decisions made by the Administration according to the law, can only be challenged at Administrative Courts, and only on the ground of illegality and, if found illegal, annulled.

We propose the word "may" be adopted instead of "shall".

Present draft:

"The competent supervisory authority within the meaning of Article 12 bis of the Convention [shall] [may] be informed of the ad hoc measures implemented and may request that the person who discloses or makes data available, or the recipient, demonstrate the quality and effectiveness of actions taken. This authority may suspend, prohibit or subject to condition the disclosure or making available of data."

Our suggestion:

"The competent supervisory authority within the meaning of Article 12 bis of the Convention may be informed of the ad hoc measures implemented and may request that the person who discloses or makes data available, or the recipient, demonstrate the quality and effectiveness of actions taken. **This authority may suspend, prohibit or subject to condition the illegal disclosure or making available of data.**"

Article 12, paragraph 5

We have the same objections as explained above in subparagraph b) of paragraph 3 of article 12.

Present draft:

"5. The competent supervisory authority within the meaning of Article 12 bis of the Convention, may suspend, prohibit or subject to condition the disclosure or making available of data within the meaning of Articles 12.3.b and 12.4."

Our suggestion:

"**The competent supervisory authority within the meaning of Article 12 bis of the Convention, may suspend, prohibit or subject to condition the illegal disclosure or making available of data within the meaning of Articles 12.3.b and 12.4.**"

Article 18, paragraph 3

We prefer the option "entitled to vote", taking into attention the difficulties encountered in past decisions considered to be more sensitive.

Just for the sake of clarity, a majority of parties entitled to vote means, at this date (May 2012), 23 Countries. If we were to adopt the option "voting", it would mean any majority formed by those who have voted.
Present draft:
"3 The Conventional Committee may, by a decision taken by a majority of two-thirds of its representatives [voting] [entitled to vote], invite an observer to be represented at its meetings."
Our suggestion:
The text would be: **"The Conventional Committee may, by a decision taken by a majority of two-thirds of its representatives entitled to vote, invite an observer to be represented at its meetings."**

New article - Bureau
We suggest the existence of the Bureau to be "acknowledged" within the Convention. We believe it to be more than justified not only within the present situation.
The T-PD would not do any productive work if it wasn't for the preparatory drafting made by the Bureau, not to mention other tasks entrusted to the Bureau, but also having in mind that we want to entrust the new "conventional committee" with new competences, namely the one, extremely important, of a monitoring body.

In light of those changes the T-PD will have to reconsider its work, namely the role entrusted with the Bureau. In addition, we believe the existence of the Bureau should be acknowledged within the text of the Convention, and eventually its composition. All regulatory aspects concerning the Bureau would be left to the internal regulation of the Committee as well as, if applicable, to other Council of Europe regulations.
It is also to be reminded that the Bureau has been functioning uninterruptedly since its creation becoming, *de facto*, a permanent structure. Not to mention that the former CG-PD or "initial" T-PD had also their own Bureaux (respectively the CG-PD-GC and the T-PD-GR).

Our suggestion:
"**Article (?)**
The Conventional Committee shall be assisted by a permanent group of representatives called the Bureau. The Bureau shall have the competences entrusted to it by the Committee."

Article 20, paragraph 3
We believe there is a drafting error in the beginning of this paragraph. It should begin by "each party", whether the party is a country or, for instance, the European Union.
Present draft:
"3 Every Party has a right to vote. Each State which is a Party to the Convention shall have one vote. On questions related to its competence, the European Union exercises its right to vote and casts a number of votes equal to the number of its member States that are Parties to the Convention and have transferred competencies to the European Union in the field concerned. In this case, those member States of the European Union do not vote. When the Committee acts according to provisions of litera h), i) and j) of Article 19, however, both the European Union and its Member States vote. The European Union does not vote when a question which does not fall within its competence is examined."
Our suggestion:
"**Each Party to the Convention shall have one vote. On questions related to its competence, the European Union exercises its right to vote and casts a number of votes equal to the number of its member States that are Parties to the Convention and have transferred competencies to the European Union in the field concerned. In this case,**

those member States of the European Union do not vote. When the Committee acts according to provisions of litera (h), (i) and (j) of Article 19, however, both the European Union and its Member States vote. The European Union does not vote when a question which does not fall within its competence is examined."

Article 20, paragraph 5
We are not comfortable with the reference to a procedure "for the examination of the adequate level of protection" till the special situation of the EU countries be clarified. We would like therefore this reference to be placed in square brackets for further consideration.
Our suggestion:
"Subject to the provisions of this Convention, the Conventional Committee shall draw up its own Rules of Procedure [and establish the procedure for the examination of the adequate level of protection]."

Thank you.

The Portuguese delegation.

May, 2012

SLOVENIA / *SLOVÉNIE*

TEXT OF THE CONVENTION – PROPOSALS
TITLE : CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

CURRENT TEXT OF THE CONVENTION	PROPOSALS
Preamble	Preamble
The member States of the Council of Europe, signatory hereto,	The signatories of this Convention,
Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;	unchanged
Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;	Considering that it is necessary, given the increase in and diversification of processing and exchanges of personal data, to guarantee the dignity and protection of fundamental rights and freedoms of every person, in particular through the right to control one's own data and the use made of them. *Explanatory report will underline that human dignity implies that individuals can not be treated as objects and be submitted to machines, and consequently that decisions based solely on the grounds of an automated processing of data can not be made without individuals having the right to express their views.*

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;	Recognising that the right to data protection is to be considered in respect of its ever increasing role in society and that it has to be balanced with the other human rights and fundamental freedoms, notably the freedom of expression and the right of access to official documents; Explanation: We find the expression »balance« more convenient than »reconcile« since the latter seems rather vigorous in this context. In addition to the »freedom of expression«, we propose also stressing the right of access to official documents being singled out as a special modern right by the Council of Europe Convention on Access to Official Documents.
Article 6 – Special categories of data	Article 6 – Processing of sensitive data
Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.	1 The processing of certain categories of personal data shall be prohibited, whether such data are sensitive: by their nature, namely genetic data, data related to health or sexual life, data related to criminal offences or convictions, or security measures; by the use made of them, namely biometric data, data whose processing reveals racial origin, political opinions [or trade-union membership], religious or other beliefs, or; where their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination, injury to dignity or to physical integrity 2 Such data may nevertheless be processed where domestic law provides appropriate safeguards.

Comment [m1]:

Comment [m2]: We prefer including the wording in this paragraph to merely mentioning this kind of risk in explanatory memorandum.

	The Explanatory Report will explain that “serious risk” includes injury to dignity or to physical integrity, "genetic data” means all data concerning the hereditary characteristics of an individual or characteristics acquired during early prenatal development, "biometric data” means all data concerning the physical, biological of physiological characteristics of an individual that allow his/her unique identification. Since it is sometimes impossible to separate sensitive from the non-sensitive personal data, we propose alternatively to include an additional paragraph in this Article,or to include the following text in the Explanatory report: »In the event that sensitive personal data cannot be separated from other categories of personal data, these data may exceptionally be processed in accordance with appropriate safeguards under domestic law, but prohibited criteria from the first paragraph shall not be the primary purpose for their processing.« For explanation the following could be indicated: paying with a credit card issued by a trade union saving bank, processing of a colour photography, etc.

Comment [m3]: The definition of genetic data seems rather questionable, therefore we propose whether omitting the definition of genetic data or verifying scientific credibility of this definition

SWEDEN / *SUÈDE*

TEXT OF THE CONVENTION – PROPOSALS
TITLE : CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

CURRENT TEXT OF THE CONVENTION	**PROPOSALS**
Preamble	Preamble
The member States of the Council of Europe, signatory hereto,	The signatories of this Convention,
Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;	Unchanged
Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;	Considering that it is necessary, given the increase in and diversification of processing and exchanges of personal data, to guarantee the dignity and protection of fundamental rights and freedoms of every person, in particular the right to privacy ~~through the right to control one's own data and the use made of them~~. Comment: We believe that the current reference to the right to privacy should be kept. This reference clarifies the connection between Convention 108 and art. 8 ECHR. Such a reference would also keep the recital in line with art. 1 of the Convention where explicit mention is made of the right to privacy. Further, a "right to control one's own data and the use made of them" does not appear in the text of the convention and it is unclear what it means. It may be argued that the mentioning of such a right can be considered as misleading since it can be perceived as a right to veto the processing of one's own personal data. *Explanatory report will underline that human dignity implies that individuals can not be treated as objects and be submitted to machines, and consequently that decisions based solely on the grounds of an automated processing of data can not be made without individuals having the right to express their views.*

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;	Recognising that the right to ~~data~~ protection of personal data is to be considered in respect of its role in society and that it has to be reconciled with ~~the~~ other human rights and fundamental freedoms, including the freedom of expression, and other public and private interests; Comment: "Data protection" should be changed to "protection of personal data" in order to keep the recital in line with article 1. Further, an amendment is proposed in order to clarify that the right to privacy has to be reconciled not only with other human rights and freedoms but also with other public and private interests (for example those mentioned in article 9). This would also bring the recital in line with the wording of art. 5.1.
Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,	Recognising that it is necessary to promote at the global level the fundamental values of respect for privacy and ~~data~~ protection of personal data, thereby contributing to the free flow of information between peoples; Comment: To keep wording in line with article 1.
	Recognising that this Convention is to be interpreted with due regard to its explanatory report, Considering that this Convention allows account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to public documents, Comment: The relationship between data protection and the right of access to public documents is of central importance. The previous drafts have included a recital on this issue. We believe that this recital should be reintroduced. *The Explanatory Report will refer to the Madrid Resolution.*
Have agreed as follows:	Unchanged
Chapter I – General provisions	Chapter I – General provisions
Article 1 – Object and purpose	Article 1 – Object and purpose

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").	The purpose of this Convention is to secure for every individual, subject to the jurisdiction of the Parties, whatever their nationality or residence, the right to the protection of personal data, thus ensuring the respect for their rights and fundamental freedoms, and in particular their right to privacy, with regard to the processing of their personal data.
Article 2 – Definitions	Article 2 – Definitions
For the purposes of this Convention:	Unchanged
a "personal data" means any information relating to an identified or identifiable individual ("data subject");	Unchanged *Make an addition to the Explanatory Report, specifying in particular that an individual is not considered "identifiable" if identification requires unreasonable time or effort for the controller or for any person from whom the controller could reasonably obtain the identification.* *Also specify that "identifiable" does not only refer to the individual's civil identity but also to what allows to "individualise" one person amongst others.* *Comment: It should be clarified in the Explanatory Report that the Convention does not apply to deceased persons.*
b "automated data file" means any set of data undergoing automatic processing;	Deleted – see 3.1 below
"automatic processing" includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;	c "data processing" means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data;
	where no automated processing is used, data processing means the operations carried out on personal data organised in a structured manner according to specified criteria allowing search by person concerned;

d “controller of the file” means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.	d “controller” means the natural or legal person, public authority, agency or any other body which alone or jointly with others has the decision-making power with respect to data processing. *In the explanatory report, specify that ‘decision-making power’ covers the purposes and conditions of processing, the means used for the data processing, as well as the reasons justifying the processing and the choice of data to be processed.*
	e “recipient” shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed or made available; f “processor“ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; *In the Explanatory Memorandum indicate that this does not apply to the employees of the controller.*
Article 3 – Scope	Article 3 – Scope

1 The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.	1 Each Party undertakes to apply this Convention to data processing carried out by any controller subject to its jurisdiction. 1bis This Convention shall not apply to data processing carried out by a natural person for the exercise of ~~purely~~ personal or household activities, ~~unless the data are made accessible to persons outside the personal or household sphere~~. Comment: As a consequence of the rapid technological development, the use of ICTs for processing sound and image data and continuous text has become widespread. Processing of large amounts of personal data by automatic means has thus become a natural part of everyday life for almost everyone. The traditional rules on the actual processing of personal data often appear too comprehensive and complicated for such ordinary processing that is in most cases completely harmless. Sweden believes that if data protection rules are to gain public acceptance and have a real effect in practical application, necessary exemptions and adaptations should be introduced for ordinary processing such as the use of e-mail programs and individuals' use of social media. The aim should be to concentrate the rules governing everyday processing on the essentials, namely, protection against harmful misuse. An important part of everyday processing is carried out by natural persons. The above-mentioned problems could therefore be partially resolved by providing for a wider exemption in art 3.1bis. 1ter Any Party may decide to apply this Convention to information on legal persons.

	In the explanatory report, specify what is meant by the exercise of ~~purely~~ personal or household activities, ~~and making accessible to persons outside the personal or household sphere (to be illustrated according to several criteria, including notably the indefinite number of persons of the CJUE judgement in the Lindqvist case).~~ Also cover services and products offered in the context of domestic activities (if the service provider acts for his/herself or for a third party with respect for data which has been provided to him/her, in other wordsif it goes beyond what is necessary in terms of the service offered, he/she begins a processing of data. If he/she is within the jurisdiction of a Party to the Convention, he/she will be subject to the data protection law of that Party). *Specify that while the processing concerns data of natural persons, the Parties nevertheless have the possibility to extend the protection to legal persons.*
2 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:	Delete
a that it will not apply this Convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law; b that it will also apply this Convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;	Delete Delete
c that it will also apply this Convention to personal data files which are not processed automatically.	Delete

3 Any State which has extended the scope of this Convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.	Delete
4 Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this Convention to such categories by a Party which has not excluded them.	Delete
5 Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2b and c above may not claim the application of this Convention on these points with respect to a Party which has made such extensions.	Delete
6 The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the Convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.	Delete
Chapter II – Basic principles for data protection	Chapter II – Basic principles for data protection
Article 4 – Duties of the Parties	Article 4 – Duties of the Parties

1 Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.	1 Each Party shall take the necessary measures in its domestic law to give effect to the provisions set out in this Convention. Comment: Article 4 makes it clear that the parties shall implement the provisions of the Convention in their national legislation. It would appear that this provision makes wordings like “Each party shall provide….” (see for example art. 8bis) unnecessary. It may be noted that the current provisions of Chapter II don’t contain such wordings.
2 These measures shall be taken at the latest at the time of entry into force of this Convention in respect of that Party.	2 These measures shall be taken by each Party prior to ratification or accession to this Convention.
	3 Each Party undertakes to allow the Conventional Committee foreseen in Chapter V to evaluate the observance of its engagements and to contribute actively to this evaluation.
Article 5 – Quality of data	Article 5 – Legitimacy of data processing and quality of data
	1 Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect a fair balance between the protection of personal data and other ~~the~~ public or private interests, rights and freedoms at stake. Comment: Editorial changes aiming at clarifying the two sides that shall be balanced. *The Explanatory Report will underline that data processing must be proportionate, that is to say, appropriate in relation to the legitimate aims pursued, necessary in the sense that there are no other appropriate and less intrusive measures with regard to the interests, rights and freedoms of data subjects or society, and it should not lead to a disproportionate interference with these interests, rights and freedoms in relation to the benefits expected from the controller.*

	2 ~~Each Party shall provide that~~ Data processing can be carried out only if: a. the data subject has freely given his/her ~~explicit~~, specific and informed consent, or Comment: As regards "Each Party..", see comment under article 4. Further, we are not convinced that consent always should be explicit. A thorough impact assessment would be necessary in order to evaluate this proposal. b. this processing is provided by domestic law for a~~n overriding~~ legitimate interest ~~or is necessary to comply with legal obligations or contractual obligations binding the data subject~~; Comment: It would appear that the specific legal bases mentioned in litera b - "is necessary to comply with legal obligations or contractual obligations binding the data subject" – are examples of legitimate interests. It is unclear why these examples need to be mentioned in the article. The mentioning of these examples may lead to questions why other examples of legitimate legal interests are not mentioned. An alternative solution would be to bring the wording more in line with article 8.2 of the EU Charter on Fundamental Rights. The Charter does not explicitly require the legitimate bases for processing to be overriding. The requirement for the interest to be overriding would follow from the principle of proportionality. Under the Convention all processing will need to comply with the principle of proportionality as formulated in art. 5.1. It may be argued that this makes the "overriding criterion" unnecessary in article 5.2 b. T*he Explanatory Report will explain the meaning of ~~overriding~~ legitimate interest (including by taking the examples of Section 7 of the Directive 95/46/CE) and that consent may be withdrawn.*
Personal data undergoing automatic processing shall be:	3 Personal data undergoing ~~automatic~~ processing shall be :
a obtained and processed fairly and lawfully;	a ~~obtained and~~ processed lawfully and fairly.

b stored for specified and legitimate purposes and not used in a way incompatible with those purposes;	b collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes; The *Explanatory Report will give examples of compatible purposes (statistics, historical or scientific research purposes that are a priori compatible provided that other safeguards exist and that the processing is not the ground for a decision to be taken concerning the data subject).*
c adequate, relevant and not excessive in relation to the purposes for which they are stored;	c adequate, relevant and not excessive ~~and limited to the strict minimum~~ in relation to the purposes for which they are processed; Comment: The Convention is applicable to widely differing categories of processing, ranging from processing in police databases to the use of e-mail programs and word processors for everyday purposes. The provisions must therefore provide sufficient flexibility in order to be relevant for the different kinds of processing. A requirement for strict minimisation of personal data may be appropriate for certain kinds of processing. This is, however, not the case as regards such everyday processing described in our comments under article 3. It may be considered unreasonable to require data minimisation during the course of an IP telephony conversation or when e-mailing. The current wording provides for the necessary flexibility and should therefore not be changed.
d accurate and, where necessary, kept up to date;	d accurate and, where necessary, kept up to date;
e preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.	e preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.
Article 6 – Special categories of data	Article 6 – Processing of sensitive data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.	1 The processing of certain categories of personal data shall be prohibited, whether such data are sensitive: by their nature, namely genetic data, data related to health or sexual life, data related to criminal offences or convictions, or security measures; by the use made of them, namely biometric data, data whose processing reveals racial origin, political opinions [or trade-union membership], religious or other beliefs, or; where their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination. 2 Such data may nevertheless be processed where domestic law provides appropriate safeguards or where the processing is not likely to adversely affect the interests, rights and fundamental freedoms of the data subject. Comment: The context and purposes are often important in order to establish the sensitivity of the processing. This is clearly the case as regards certain data related to health. For example, if it is mentioned in an email that a colleague is absent with a cold, this would in most peoples' view not be considered as sensitive processing. In order not to prohibit such ordinary and harmless processing a new exemption should be introduced in art. 6.2 b.
	The *Explanatory Report will explain that "serious risk" includes injury to dignity or to physical integrity, "genetic data" means all data concerning the hereditary characteristics of an individual or characteristics acquired during early prenatal development, "biometric data" means all data concerning the physical, biological of physiological characteristics of an individual that allow his/her unique identification.*
Article 7 – Data security	Article 7 – Data security

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.	1 ~~Every Party shall provide that~~ The controller, and, where applicable the processor, shall take~~s~~ the appropriate security measures against accidental or unauthorised modification, loss or destruction of personal data ~~accidental~~, as well as against unauthorised access or dissemination ~~of personal data processed~~. Comment: As regards "Every Party…", see comment under article 4. The other amendments are editorial. 2 ~~Each Party shall provide that~~ The controller shall notify, without delay, at least the supervisory authorities within the meaning of Article 12 bis of this Convention of any ~~violation of data~~ data security breach/personal data breach which may seriously interfere with the fundamental rights and freedoms of the data subject. Comment: As regards "Each Party…", see comment under article 4. We are not convinced that "violation of data" is the appropriate term to use in this context. Alternatives could be "data security breach" or "personal data breach". *The Explanatory Report will specify that the controller should be encouraged to also notify, where necessary, the data subjects.*
	Article 7bis – Transparency of processing

	1. ~~Each Party shall provide that e~~The controller must ensure the transparency of data processing and in particular provide data subjects with information concerning at least his/her identity and habitual residence or establishment, the purposes of the processing carried out by him/her, the data processed, the recipients or the categories of recipients of the personal data[, the preservation period] and the means of exercising the rights set forth in Article 8, as well as any other information necessary to ensure a fair data processing. Comment: As regards “Every Party…”, see comment under article 4. Further, the inclusion of “the categories of recipients” would bring the Convention in line with directive 95/46. We believe that this issue should be dealt with in the Convention and not only in the Explanatory Report. Further, Sweden is not convinced that information on "preservation period” should be obligatory. Maybe it can, instead, be elaborated in the Explanatory Report in which cases such information is necessary to ensure fair data processing.

	2. The controller shall nonetheless not be required to provide such information where a. this proves to be impossible or involves disproportionate efforts, b. the processing is expressly laid down by law, or c. the data subject already has the information. Comment: The controller should not be required to provide information where the processing is expressly laid down by law or where the data subject already has the information. This would bring the provision in line with articles 10-11 of directive 95/46. The *Explanatory Report will specify when the information should be given, that the information should be direct, readable etc, and that "any other information necessary to ensure a fair data processing" notably includes information on transfers to other countries.* *The information should also include measures taken to guarantee data protection in the context of transfers to countries which do not have an adequate system of data protection.* *The collection of personal data includes both direct and indirect collection. The information regarding the recipients may also refer to categories of recipients.*
Article 8 – Additional safeguards for the data subject	Article 8 – Rights of the data subject
Any person shall be enabled:	Any person shall be entitled on request:
a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;	a not to be subject to a decision significantly affecting him/her or producing legal effects relating to him/her, based solely on the grounds of an automatic processing of data without having the right to express his/her views;
	b to object at any time for legitimate reasons to the processing of personal data concerning him/her;

b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;	c to obtain at reasonable intervals and without excessive delay or expense confirmation ~~or not~~ of the existence of data processing relating to him/her, the communication in an intelligible form of the data processed, all available information on their origin as well as any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7bis; ~~d to obtain knowledge of the reasoning underlying in the data processing, the results of which are applied to him/her ;~~ Comment: The information set out in litera d is only relevant in certain situations, for example in cases dealt with in litera a. It is therefore more appropriate to apply the provision in litera c ("any other information that the controller is required to provide to ensure the transparency of processing") to such information. This issue could be elaborated in the Explanatory Report.
	Explanatory Report: this right can, in accordance with Article 9, be limited where this is necessary in a democratic society, in order to protect "legally protected secrets".
c to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;	Unchanged
d to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.	See e below
	e to have a remedy if no response is given to a request for confirmation, communication, rectification, erasure or to an objection, as referred to in this Article;

	f to benefit, whatever his/her residence, from the assistance of a supervisory authority within the meaning of Article 12 bis, in exercising the rights provided by this Convention. *Explanatory report: 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.*
	Article 8bis – Additional obligations

	1- ~~Each Party shall provide that~~ The controller is responsible ~~for ensuring respect for the right to the protection of personal data at all stages of the processing and~~ for taking all appropriate measures to ~~implement~~ ensure respect for the domestic legal provisions giving effect to the principles and obligations of this Convention. Comment: As regards “Each Party…”, see comment under article 4. The other changes aim at simplifying the provision. 2- The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the foreseen data processing on the rights and fundamental freedoms of the data subject. 3- The controller, or where applicable the processor, shall design data processing operations in such a way as to prevent or at least minimise the risk of interference with the right to the protection of personal data. 4- The controller shall establish internal mechanisms to verify and demonstrate to the data subjects and to the supervisory authorities provided for in Article 12 bis of this Convention the compliance of the data processing for which he/she is responsible with the applicable law.

	[5- ~~Each Party shall provide that~~ The products and services intended for the data processing shall take into account the implications of data protection from the stage of their design and include easy-to-use functionalities allowing the compliance of the processing with the applicable law to be ensured.] Comment: It is difficult to foresee the consequences of this provision. It may first be noted that the addressees of the requirements are not set out in the provision, which would cause legal uncertainty. Further, this provision would introduce new technical requirements for a wide range of products and services. We are therefore not convinced that it is appropriate to include this provision in the convention. It may be noted that the wording of paragraph 6 ("the size of the controller, or where applicable, the processor") is not adapted to the possible addressees in paragraph 5, i.e. manufacturers etc. 6- The obligations included in the domestic law on the basis of the provisions of the previous paragraphs may be adapted according to the size of the controller, or where applicable the processor, the volume of data processed and the risks for the interests, rights and fundamental freedoms of the data subjects. Comment: Certain categories of processing may require exemptions from most of the obligations in this article. This is the case for ordinary and normally harmless processing described in the comments under art. 3. It appears unclear whether the current wording of paragraph 6 – which allows for the *adaptation* of the obligations – also allows for certain categories of processing to be *excluded* from the obligations. This needs to be clarified. *The Explanatory Report will specify that one of the possible measures could consist of the designation of a 'data protection officers' entrusted with the means necessary to fulfil its mission independently and of whose designation the supervisory authority has been informed. They can be internal or external to the controller.*
Article 9 – Exceptions and restrictions	Article 9 – Exceptions and restrictions

1 No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.	1 No exception to the basic principles expressed in this Chapter shall be allowed, except to the provisions of Articles 5.3 , 6, 7.2, 7bis and 8 when such derogation is provided for by law and constitutes a necessary measure in a democratic society to: *Explanatory Report: a measure shall be considered as "necessary in a democratic society" to pursue a legitimate aim if it meets a "pressing social need" which cannot be achieved by less intrusive means and, especially, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it appear "relevant and sufficient".*
2 Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:	Delete
a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;	a protect State security, public security, the economic and financial interests of the State or the prevention and suppression of criminal offences; *The Explanatory Report will clarify by means of examples the scope of the provision, referring to the confidentiality of communications and business or commercial secrecy and other legally protected secrets.*
b protecting the data subject or the rights and freedoms of others.	b protect the data subject or the rights and freedoms of others, notably freedom of expression and information. ~~*The Explanatory Report will specify that this provision concerns data processing carried out solely for communicating information to the public, ideas or opinions of general interest, or for literary or artistic expression.*~~ *The Explanatory Report should clarify that the parties may apply litera b in relation to the right of access to official documents.*

3 Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.	2 Restrictions on the exercise of the provisions specified in Articles 6, 7bis and 8 may be provided by law with respect to ~~personal~~ data processing for statistical purposes or for the purposes of scientific research, when there is obviously no risk of an infringement of the rights and freedoms of the data subjects.
Article 10 – Sanctions and remedies	Article 10 – Sanctions and remedies
Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter	Each Party undertakes to establish appropriate judicial and non-judicial sanctions and remedies for violations of domestic law giving effect to the provisions of this Convention.
Article 11 Extended protection	Article 11 Extended protection
None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this Convention.	unchanged
Chapter III – Transborder data flows	Chapter III – Transborder data flows
Article 12 – Transborder flows of personal data and domestic law	Article 12
1 The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.	1 Each Party shall ensure that personal data will only be disclosed or made available to a recipient who is not subject to its jurisdiction on condition that an adequate level of data protection is ensured. *Explanatory report: It should be reminded, in accordance with the judgement in the Lindqvist case, that internet publishing is not per se considered as a transborder data flow.*
2 A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.	2 When the recipient is subject to the jurisdiction of a Party to the Convention, the law applicable to this recipient is presumed to provide an adequate level of protection and a Party shall not, for the sole purpose of data protection, prohibit or subject to special authorisation the disclosure or making available of data. The Conventional Committee may nevertheless conclude that the level of protection is not adequate.

3 Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:	3 When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to the Convention, an adequate level of protection can be ensured by: a) the law of that State or organisation, in particular by applicable international treaties or agreements, or b) standardised or ad hoc legal measures, such as contract clauses, internal rules or similar measures that are binding, effective and capable of effective remedies, implemented by the person who discloses or makes personal data accessible and by the recipient. The competent supervisory authority within the meaning of Article 12 bis of the Convention [shall] [may] be informed of the ad hoc measures implemented and may request that the person who discloses or makes data available, or the recipient, demonstrate the quality and effectiveness of actions taken. ~~This authority may suspend, prohibit or subject to condition the disclosure or making available of data.~~ Comment: The suspension etc. of transfers is dealt with in art. 12.5.
a insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;	4. Notwithstanding paragraphs 2 and 3 , each Party may provide that the disclosure or making available of data may take place without the law applicable to the recipient ensuring, for the purposes of this Convention, an adequate level of protection of data subjects, if in a particular case: a) the data subject has given his/her specific, free and explicit consent, after being informed of risks arising in the absence of appropriate safeguards, or b) the specific interests of the data subject require it in the particular case, or c) legitimate interests protected by law and meeting the criteria of Article 9, prevail.

	5. The competent supervisory authority within the meaning of Article 12 bis of the Convention, may suspend, prohibit or subject to condition ~~the~~ such disclosure or making available of data that is not in compliance with ~~within the meaning of~~ Articles 12.3~~.b~~ and 12.4. Comment: The supervisory authority should only be allowed to suspend or otherwise hinder transborder data flows that are not in compliance with the relevant provisions.
b when the transfer is made from its territory to the territory of a non Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph. and a Party shall not, for the sole purpose of data protection, prohibit or subject to special authorisation the disclosure or making available	6. Each Party may foresee in its domestic law derogations to the provisions set out in this Chapter, providing they constitute a measure necessary in a democratic society to protection of freedom of expression and information.
Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention (Additional Protocol)	*(Article 12 above replaces the old Article 12 and Article 2 of the Additional Protocol)*
1 Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer	
2 By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data :	
a if domestic law provides for it because of :	
– specific interests of the data subject, or	
– legitimate prevailing interests, especially important public interests, or	
b if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.	

	Chapter III bis Supervisory authorities
	Article 12bis Supervisory authorities
1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.	1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles of this Convention.
2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.	2 To this end, such authorities: a. are responsible for raising awareness of and providing information on ~~data~~ the protection of personal data; b. have, in particular, powers of investigation and intervention; c. may pronounce decisions necessary with respect to domestic law ~~measures~~ giving effect to the provisions of this Convention and in particular to sanction administrative offences; d. are able to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the provisions of this Convention. *The Explanatory report will note that the powers of intervention should notably concern data processing which presents particular risks for rights and fundamental freedoms.*
b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.	3 Each supervisory authority can be seized by any person concerning the protection of his/her rights and fundamental freedoms with regard to the data processing ~~of personal data~~ within its competence and shall inform the data subject of the follow-up given to such a claim.
3. The supervisory authorities shall exercise their functions in complete independence.	4 The supervisory authorities shall accomplish their duties and exercise their powers in complete independence. They shall in their supervision neither seek nor accept instructions from anyone. Comment: It needs to be clarified that the prohibition on taking instructions only covers the performance of the duties as a supervisory authority, and not when the authority acts as an employer etc. It should be clarified in the Explanatory Report that it is never allowed to give instructions or guidelines on the interpretation or application of law, neither in a specific case nor in general.

	5 Each Party shall ensure that the supervisory authorities have adequate human, technical and financial resources and infrastructure necessary to accomplish their mission and exercise their powers autonomously and effectively.
4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.	6 Decisions of the supervisory authorities which give rise to complaints shall be subject to judicial remedies. Comment: The French language version of this provision has not been changed compared with the Additional Protocol and is the same as the corresponding provision in directive 95/46 (art. 28.3). However, the English language version has been changed compared with the Additional Protocol (e.g. “may” has been changed to “shall be” which seems do differ from the French version: “peuvent faire”). The proposed changes would further mean that the English language version would differ from the corresponding provision (art. 28.3) in directive 95/46, which is identical to the current provision in the Additional protocol. Against this background we are not convinced that this provision should be changed.
5. In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the Convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.	7. In accordance with the provisions of Chapter IV, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by:
	a exchanging all useful information, in particular by taking, under their domestic law and solely for the protection of personal data, all appropriate measures to provide factual information relating to specific processing carried out on its territory, with the exception of personal data undergoing this processing, unless such data is essential for co-operation or that the data subject has previously explicitly agreed to;
	b coordinating their investigations or interventions or conducting joint actions;
	c providing information on their law and administrative practice in data protection.

	8 In order to organise their co-operation and to perform the duties set forth in the preceding paragraph, the supervisory authorities of the Parties ~~shall~~ may form a conference. Comment: We are not convinced that it should be obligatory to form a conference.
	9. The supervisory authorities shall not be competent with respect to processing carried out by judicial bodies in the exercise of their judicial functions.

Federal Office of Justice - Switzerland / *Office fédéral de la justice - Suisse*

Berne, le 25 mai 2012

Art. 3 :

Proposition de modification :
1quater nouveau : **Toute partie peut décider de ne pas appliquer la présente Convention aux traitements de données effectués dans le cadre d'une procédure pendante pénale ou d'entraide judiciaire internationale en matière pénale**.

Motivation :
La convention n'est pour partie, en particulier en ce qui concerne les art. 3 al. 1, 5, 6 al. 1, 7 al. 2, 7bis, 8 et 8bis, pas adaptée aux spécificités et impératifs du traitement des données dans le cadre de procédures pénales en cours. Dans ce contexte les données sont en effet partie intégrante du dossier pénal et suivent le sort de celui-ci; ce traitement est en outre effectué par des autorités judiciaires et un contrôle de celui-ci doit avoir lieu d'une manière compatible avec les intérêts, en particulier de procédure, d'organisation, de flexibilité, de praticabilité et d'efficacité, de la procédure pénale, ce qu'il appartient aux dispositions de procédure pénale de garantir.

Art. 6 :

Proposition de modification:
1 Les données à caractère personnel ne peuvent pas être traitées pour l'origine, les opinions politiques, les convictions religieuses ou autres convictions qu'elles révèlent. Les données génétiques, les données à caractère personnel relatives à la santé ou à la vie sexuelle, les données biométriques, les condamnations pénales ne peuvent pas non plus être traitées.
2 Ces données peuvent toutefois faire l'objet d'un traitement si le droit interne prévoit des garanties appropriées.

Motivation:
Nous sommes d'avis que les « données sensibles » doivent être définies de par leur nature, et non par les critères de l'usage qui en est fait et du risque que leur traitement présente pour les droits de la personne concernée. En effet, la nouvelle conception de la notion de données sensibles prévue aux let. b et c laisse trop de zones d'ombre. En pratique, il sera très difficile de savoir dans quels cas une donnée, qui constitue au moment de sa collecte une donnée « simple », se transforme en donnée « sensible ». Cette insécurité juridique donnera lieu à de nombreuses incertitudes, ce qui est préjudiciable pour la protection des données. Nous proposons par conséquent d'élargir la notion de « données sensibles » aux données génétiques et aux données biométriques.

Art. 7bis, par. 2 :

Proposition de modification:
2. Le responsable du traitement n'est néanmoins pas tenu de fournir ces informations lorsque cela lui est impossible, **que cela** implique des efforts disproportionnés **ou lorsque le traitement de données est expressément prévu par le droit interne.**

Motivation:
La transparence des traitements de données est garantie si ceux-ci reposent sur une base légale expresse.

Art. 12, par. 4, let. c :

Proposition de modification:
4. Par dérogation aux paragraphes 2 et 3, chaque Partie peut prévoir que la communication ou la mise à disposition peut avoir lieu sans que le droit applicable au destinataire assure, au regard de la Convention, un niveau de protection adéquat des personnes concernées par ces données, si dans un cas particulier :
a) la personne concernée a donné son consentement spécifique, libre et explicite, après avoir été informée des risques dus à l'absence de garanties appropriées ; ou
b) des intérêts spécifiques de la personne concernée le nécessitent ; ou
c) des intérêts légitimes protégés par la loi en particulier des intérêts publics importants ~~**et répondant aux critères de l'article 9**~~, prévalent.

Motivation:
La disposition selon laquelle des données ne peuvent être communiquées que lorsqu'il s'agit de la sécurité de l'Etat, de la sécurité publique, d'intérêts économiques et financiers importants ou de la prévention et de la répression des infractions pénales est trop restrictive et trop absolue. D'autres intérêts publics prépondérants peuvent en effet prévaloir, par exemple dans le domaine de l'asile ou des assurances sociales. Nous demandons par conséquent d'élargir l'art. 12 par. 4 let. c.

Art. 12, par. 5 :

Proposition de supprimer cette disposition.

Motivation :
Il est contradictoire de conférer à chaque Etat partie la possibilité de prévoir des exceptions et d'accorder la faculté à l'autorité de contrôle de rendre inapplicables les exceptions décidées par le législateur national.

Art. 12bis, par. 2 :

Proposition de modification :
2 A cet effet, ces autorités :
a. sont chargées de sensibiliser et d'éduquer à la protection des données ;
b. disposent notamment de pouvoirs d'investigation et d'intervention ;
c. ;

d.peuvent ester en justice ou porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux dispositions de la présente Convention.

Motivation :
Nous sommes d'avis que les Etats parties doivent garder toute latitude de conférer le pouvoir de prononcer des décisions et/ou des sanctions à d'autres autorités, en particulier à des instances judiciaires, d'autant plus que ces compétences ne sont pas forcément compatibles avec des tâches de sensibilisation et d'éducation à la protection des données. Autrement dit l'autorité de contrôle ne saurait nécessairement cumuler les rôles de prévention et de répression en matière de protection des données.

Art. 12bis, par. 9 :
Proposition de modification:
9 Les autorités de contrôle ne sont pas compétentes en matière de traitement effectués par les autorités compétentes dans le cadre d'une procédure judiciaire. Le contrôle de ces traitements est régi par le droit national de procédure.

Motivation:
Pour fixer clairement le cadre dans lequel les données seront traitées dans le cadre d'une procédure judiciaire en dehors de tout contrôle de l'autorité de contrôle, nous proposons la modification mentionnée ci-dessus. En effet, la notion de « fonctions juridictionnelles » (soit la fonction « de dire le droit ») ne correspond pas à la notion anglaise de « judicial functions » qui est plus appropriée aux fins de la présente Convention.

T-PD observers / *T-PD observateurs*

AUSTRALIA / *AUSTRALIE*

EDPS

EDPS comments on revision of Convention 108, version 27 April 2012-05-25

Preamble
"Considering that it is necessary, given the increase in and diversification of processing and exchanges of personal data, to guarantee the dignity and protection of fundamental rights and freedoms of every person, in particular through the right to control one's own data and the use made of them."

Facilitating user's control on their personal data is one of consequences of the main principles of the Convention but there is not, literally speaking, a right to control one's data in the text: this only results to some extent from the rights of information, access, objection, rectification. We suggest replacing the final part of the text by "in particular through the recognition of basic principles for data protection, including the rights of individuals and the responsibilities of controllers".

Article 2 - Definitions
"Make an addition to the Explanatory Report, specifying in particular that an individual is not considered "identifiable" if identification requires unreasonable time or effort for the controller or for any person from whom the controller could reasonably obtain the identification.
Also specify that "identifiable" does not only refer to the individual's civil identity but also to what allows to "individualise" one person amongst others."

We suggest simplifying the part of the sentence highlighted in grey in order to provide for consistency with the EU regulatory framework, as follows: "for any other person involved".
The new wording makes "identifiability" subject to complex requirements, including a connection between the controller and other parties and an additional reasonability test in the obtaining of information by the controller from that party.
In our view this unduly narrows the concept and makes it difficult to apply. Besides, it is not in line with the way "identifiability" is understood by EU DPAs (see WP29 opinion of 20 June 2007 (WP136)

Article 2.c
"Where no automated processing is used, data processing means the operations carried out on personal data organised in a structured manner according to specified criteria allowing search by person concerned;"

This paragraph mixes the definition of non automated files with the definition of data processing.
We suggest leaving the definition of data processing as is (2.c. first par.), and defining non automated files as 'organised in a structured manner according to specific criteria' but deleting the requirement of search by person concerned as this unduly limits the scope of application: structured files may for instance be accessible through criteria such as age, nationality, etc, which would then lead to a list of names. This should not be excluded from the definition.

Article 3.1 - Scope
"In the explanatory report, specify what is meant by the exercise of purely personal or household activities, and making accessible to persons outside the personal or household sphere (to be illustrated according to several criteria, including notably the indefinite number of persons of the CJUE judgement in the Lindqvist case).
Also cover services and products offered in the context of domestic activities (if the service provider acts for his/herself or for a third party with respect for data which has been provided to him/her, in other words if it goes beyond what is necessary in terms of the service offered, he/she begins a processing of data. (…)"

This part may need redrafting as the situation intended to be covered (by domestic processing?) and the desired outcomes are not fully clear.

Article 5 - Legitimacy
"2. Each Party shall provide that data processing can be carried out only if:
a. the data subject has freely given his/her explicit, specific and informed consent, or
b. this processing is provided by domestic law for an overriding legitimate interest or is necessary to comply with legal obligations or contractual obligations binding the data subject;"

Unlike the EU Directive and draft EU regulation, the convention does not include as a basis for processing the legitimate interests of the data controller, subject to a balance with possible overriding interests of the data subject. Consider adding this provision.

Article 6 - Sensitive data
"1. The processing of certain categories of personal data shall be prohibited, whether such data are sensitive:
a. by their nature, namely genetic data, data related to health or sexual life, data related to criminal offences or convictions, or security measures;
b. by the use made of them, namely biometric data, data whose processing reveals racial origin, political opinions [or trade-union membership], religious or other beliefs, or;
c. where their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."

This has been intensively discussed during the last T-PD. We still wonder however whether the last category should be maintained as such, or rather withdrawn from the definition of sensitive data, and subjected to specific safeguards (such as prior-check, authorisation by DPA, PIA...).

Article 9 - Exceptions and restrictions
"1. No exception to the basic principles expressed in this Chapter shall be allowed, except to the provisions of Articles 5.3 , 6, 7.2, 7bis and 8 when such derogation is provided for by law and constitutes a necessary measure in a democratic society to:
a. protect State security, public security, the economic and financial interests of the State or the prevention and suppression of criminal offences;
b protect the data subject or the rights and freedoms of others, notably freedom of expression and information. (...)"

The Articled referred to concern respectively the obligation of fair and lawful processing, conditions for processing sensitive data, notification of data breaches, transparency and rights of

data subjects. While exceptions to transparency and exercise of rights can be justified in specific cases, we do not see any convincing reason to allow for unfair processing, limiting safeguards for sensitive data or not notifying data breaches. We suggest deleting the reference to Articles 5.3., 6 and 7.2.

Transborder data flows

In general, we support the new wording of Article 12 which foresees a presumption of adequacy for Parties to the Convention, which can be reversed by the Conventional Committee.
The addition in Article 4 ("Each Party undertakes to allow the Conventional Committee foreseen in Chapter V to evaluate the observance of its engagements and to contribute actively to this evaluation") is another step to ensure effective implementation of the requirements of the Convention.
The new wording with regard to adequacy requirements is also more in line with the wording of the EU draft Regulation. This should facilitate the assessment of situations where a country is Party to the Convention without being member of the EU.

Article 12.3.
"When the recipient is subject to a jurisdiction (...) which is not party to the Convention, an adequate level of protection can be ensured by:
a) the law (...)
b) standardised or ad hoc legal measures (...)
The competent supervisory authority within the meaning of Article 12 bis of the Convention [shall] [may] be informed of the ad hoc measures implemented and may request that the person who discloses or makes data available, or the recipient, demonstrate the quality and effectiveness of actions taken. This authority may suspend, prohibit or subject to condition the disclosure or making available of data."

We suggest ensuring consistency with the EU draft Regulation and providing as a minimum for information of the supervisory authority ("shall be informed"), considering that the EU framework goes even further in providing for prior authorisation in specific cases.
We suggest replacing the second part in grey by "demonstrate effective compliance with these measures".

Article 12.4.
"4. Notwithstanding paragraphs 2 and 3, each Party may provide that the disclosure or making available of data may take place without the law applicable to the recipient ensuring, for the purposes of this Convention, an adequate level of protection of data subjects, if in a particular case:
a) the data subject has given his/her specific, free and explicit consent, after being informed of risks arising in the absence of appropriate safeguards, or
b) the specific interests of the data subject require it in the particular case, or
c) legitimate interests protected by law and meeting the criteria of Article 9, prevail."

This last sentence has been discussed during the last T-PD meeting. The text is improved compared to the previous version, which mentioned prevailing legitimate interests, in particular important public interests, without any additional safeguards. To strengthen the main adequacy principle in relation to exceptions, we suggest adding at the end of this provision or as a minimum in the explanatory memorandum that exceptions cannot be used to allow massive and repetitive transfers of personal data.

ICC

Comments of the ICC Commission on the Digital Economy on the Council of Europe's April 2012 revision draft to Convention 108

ICC has appreciated the opportunity to participate as an observer in the work of the T-PD that is considering amendments to Council of Europe Convention 108, and has the following comments on the April 2012 draft:

Preamble page 8. The removal of the reference to information flows eliminates the parallelism with OECD and EU Directive/Regulation. Global information flows are an important societal objective and should be declared so in the recitals, especially since human rights law mandates that various fundamental rights be balanced. It is through those information flows that rights of association, expression, choice and prosperity/pursuit of happiness are often exercised. Thus a preamble reference to the importance of information flows to today's digital economy and information society should be reinserted.

Article 2 definitions – personal data. A question arises from the term to individualize one person amongst others – does this require persistence of that ability? At any point in time one might be able to identify two dynamically generate IP addresses as different, but it may not be possible to individualise a person beyond that point in time. This should be expressed more as a factor which, depending upon circumstances could tend to identify a person in the particular context.

Definitions – data controller. One must be careful in how "means" are discussed. Processors may also make numerous determinations related to means in order to execute the instruction (purposes) of the controller, so that the power to determine means alone should not be sufficient to implicate control.

Definitions – recipient. In definitions, recipient is defined in between the two major roles (controller/processor) – explanatory memo should explain the nature of the term, and how it relates to these two other ones.

Article 5 Para 1 – explanatory memo reference. "In relation to the benefits expected from the controller" is too subjective and impossible to quantify as it may change with every user.

Article 5 Para 2. We do not believe that a requirement of consent should override the legitimate interests' test, as stated in the Explanatory Memorandum (p 4). We also believe that it needs to be clarified in the memorandum that other possibility of legitimizing processing are possible (eg to fulfill a contract) as foreseen in Article of the EU Directive.

Article 6 Para 2. It is unclear what "appropriate safeguards" might be. Is a general privacy regulation an appropriate safeguard? Could that be a code of conduct or research protocol? Health data must be processed to treat patients; there is no option not to process. We should better define appropriate safeguards and better consider the real-world implications of this provision.

Article 7 Para 1. While there is no question that data processors need to provide adequate security for data processing, independent obligations in relation to the security of specific information may require the processor to have greater knowledge of the information – defeating

the principle of data minimization. Thus, this requirement should be derivative of the controller's obligation ("controller should require processor to….") rather than an independent obligation.

Article 7 Para 2. Question arises as to how "seriously interfere with the right to the protection of personal data" will be interpreted. Is this the same as reasonably likely to cause harm or adverse effect?

Article 7 Bis Para 1. We should consider the granularity and the utility of the documentation. In some cases categories of recipients may be sufficient. Some of this information may also vary across types of data elements. We thus suggest adding a qualifier such as: "as appropriate under the circumstances".

Article 8 Para b. Clarification of scope and application of "legitimate" reasons would be welcome.

Article 8 Para c. "All available information" seems overbroad. Perhaps "information relevant to". May also wish to have the ability to scope the request to address issues of scale, reasonableness, cost and potential for abuse.

Article 8 Para d. A clarification that the reasoning does not include information about algorithms or proprietary methods would be welcome.

Article 8 Bis. We question whether it is realistic to expect data controllers to "carry out a risk analysis of the potential impact of the foreseen data processing on the rights and fundamental freedoms of the data subject". This sort of requirement will be unintelligible to the majority of data controllers, and it is important to clarify in the explanatory memorandum that in many cases this may mean only that data protection needs to be taken into account based on the potential risks of the processing and the costs and benefits of protective measures, in accordance with the principle of proportionality. There is also a continued issue of independent obligations on the processor for the reasons outlined above.

Article 12 overall. "Supervisory authority" does not seem to include concepts of accountability agents (regarding APEC, Safe Harbour etc); they have a growing role.

Article 12 overall and 12 Bis 7 et seq. The EU draft regulation has recognized the benefits of more harmonized application of rules and decisions, perhaps some emphasis on that topic could be introduced.

Article 12 Para 3. We have a strong preference for "may", as this better takes into account the fact that states vary greatly on whether there is a duty to notify the regulators about transborder data flows.

Article 12 Bis Para 4. It could be clarified in the explanatory memorandum that the requirement of independence should not preclude the ability to consult technical and other experts, which should be encouraged, or to hold external consultations. This clarification could be useful in particular in states that do not have a lot of experience with data protection laws.

USA / *ETATS-UNIS D'AMERIQUE*

Comments of the United States of America on the Modernization of Convention 108: New Proposals

Introduction

The United States of America welcomes the opportunity to submit comments on the proposals for the Modernization of Convention 108 contained in Document T-PD-BUR (2012)01Rev2_en, circulated on 27 April 2012. The United States applauds the crucial work of the Consultative Committee for Convention 108, and shares the Council of Europe's commitment to developing new mechanisms to promote interoperability in order to protect privacy in an age of global data flows. The following comments incorporate by reference the United States' previous submission of March 10, 2011.[1]

As the United States notes in its February 2012 report Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,

> [C]ross-border data flows are a vital component of the domestic and global economies. Differences in national privacy laws create challenges for companies wishing to transfer personal data across national borders. Complying with different privacy laws is burdensome for companies that transfer personal data as part of well-defined, discrete data processing operations because legal standards may vary among jurisdictions, and companies may need to obtain multiple regulatory approvals to conduct even routine operations. Though governments may take different approaches to meeting these challenges, it is critical to the continued growth of the digital economy that they strive to create interoperability between privacy regimes.[2]

The United States, despite not having joined Convention 108, respects the approach to privacy and trans-border data flows that was pioneered by the Council of Europe with the creation of Convention 108 in 1981, and takes note of the common ancestry shared between Convention 108 and the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. In 2005, the OECD Guidelines' Basic Principles of National Application were adapted for use within the Asia-Pacific Economic Cooperation (APEC) to form the basis for the APEC Privacy Framework. Between 2005 and 2011, a dedicated group of APEC member economies—including but not limited to Australia, Canada, Chile, Chinese Taipei, Hong Kong, Japan, Korea, Mexico, New Zealand, Peru, the Philippines, the United States and Vietnam—developed the APEC Cross-Border Privacy Rules (CBPR), which were finalized and publicly announced during the APEC Leaders' Summit in November 2011.

[1] The March 10, 2011 comments are available at page 444 of the Consultation concerning the modernisation of Convention 108: results, T-PD-BUR(2011) 01 MOS rev 6, June 2011, available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2011_01_%20MOS6%20Results.pdf. We also refer you to comments submitted to the Council of Europe by the U.S. Federal Trade Commission. *See* U.S. Federal Trade Commission Staff Comments to the Council of Europe's Consultative Committee on the Modernization of Convention 108 (March 9, 2011), *available at* http://www.ftc.gov/os/2011/03/110309staffcommentconvention.pdf.

[2] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (hereinafter "Privacy and Innovation Blueprint"), February 23, 2012, p. 31, available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

The United States sees a number of advantages to the APEC approach, which does not at all contradict the Convention 108 approach; indeed, the two approaches could complement each other. The APEC approach is not one of treaty obligations between nation-states. It is an arrangement between member *economies* (which gives certain economies a unique opportunity to participate) that is agnostic as to what sorts of domestic privacy legislation each economy must have in place. It does not seek to harmonize or homogenize domestic privacy legislation; rather, it focuses more narrowly on the issue of how to ensure a basic consistency of consumer privacy protections as data moves from one member economy to the other. It does so by encouraging each member economy to implement the APEC Privacy Principles[3] using any combination of domestic legal authority and private oversight mechanisms that is available and effective.

The APEC CBPRs are a system for businesses to transfer their data across borders within the APEC region. To participate, a member economy must have a Privacy Enforcement Authority with "the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR program requirements."[4] A "Privacy Enforcement Authority" is defined as "any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings."[5] The emphasis is not on the form of the privacy law or the nature of the enforcement authority, but on the practical effect. While the decision to participate in the system is voluntary, once an organization has committed to participate, the rules are binding and enforceable.

Private multinational organizations that choose to participate in the APEC CBPR system ("Participants") must submit to a rigorous certification process conducted by an Accountability Agent.[6] An Accountability Agent can be either a public or private enforcement body. However, in order to be certified by APEC, the Accountability Agent must "be free of actual or potential conflicts of interest," and be capable of (1) evaluating applicants to become Participants against the Intake Questionnaire; (2) providing ongoing monitoring and compliance review of its Participants; (3) conducting re-certification and annual attestation; and (4) providing a mechanism to receive and investigate complaints about Participants and to resolve disputes between complainants and Participants in relation to non-compliance with its program requirements, as well as a mechanism for cooperation on dispute resolution with other Accountability Agents recognized by APEC economies when appropriate and where possible.[7]

The APEC CBPR's complaint resolution mechanisms are intended to work seamlessly and in trans-border fashion based on two aspects of the system: (1) the Accountability Agents, whose enforcement authority over the Participants arises from their contractual relationship with the Participants and without regard to national jurisdiction; and (2) the Cross Border Privacy Enforcement Arrangement (CPEA), which provides a framework for trans-border cooperation between Privacy Enforcement Authorities. Privacy Enforcement Authorities can also rely on

[3] The APEC Privacy Principles are available at http://www.apec.org/Groups/Committee-on-Trade-and Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

[4] *See* attached APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines, para. 44.

[5] *Id.*, para. 42.

[6] *See* attached Intake Questionnaire.

[7] See attached Accountability Agent Application for APEC Recognition, Annex A: Accountability Agent Recognition Criteria

Accountability Agents to extend their own jurisdictional reach and limited resources by allowing the Accountability Agents to provide at least a preliminary dispute resolution mechanism; consumer disputes or instances of non-compliance with the program requirements by participating businesses that are not satisfactorily resolved by the Accountability Agents can then also be addressed through dispute resolution mechanisms or law enforcement measures that exist in domestic legislation.

In order to participate in the APEC CBPR, an APEC Member Economy must meet the following conditions, which are to be conveyed to the APEC CBPR Joint Oversight Panel:

(1) It must have at least one Privacy Enforcement Authority in that Economy that is a participant in the CPEA;
(2) It must make use of at least one APEC recognized Accountability Agent; and
(3) It must explain to the APEC CBPR Joint Oversight Panel how the CBPR System program requirements may be enforced in that Economy.

The Joint Oversight Panel then must formally approve the Member Economy's participation and notify the Chair of APEC's Electronic Commerce Steering Group.[8]

An analysis of the APEC Privacy Principles and CBPR raises several issues that are useful to highlight with respect to the Council of Europe's proposed modernization of Convention 108. First, in light of the stringent requirements with respect to privacy compliance in the APEC system, the Council of Europe may wish to consider whether a member economy's participation in the APEC CBPR project is sufficient to satisfy the requirements of Convention 108, as to transfers made using that framework. Second, we suggest a few substantive edits to the Council of Europe's proposal that would make it more interoperable with APEC and other such systems. Third, we suggest that the Council of Europe consider the advisability of incorporating codes of conduct, like the APEC model, as a basis for cross-border data transfers.

Overlap Between APEC CBPR and Convention 108 Compliance; Suggestions for Explanatory Memorandum

Considerable overlap between the APEC CBPR and Convention 108 suggests that participation in the former could be taken as evidence of compliance with the latter; whether and to what extent Member Economy participation in the APEC CBPR would suffice as evidence of compliance with Convention 108 is of course for the Council of Europe to decide. The Charter of the APEC CBPR Joint Oversight Panel makes clear that nothing in the charter is intended to "[c]reate any binding obligations on APEC Economies and/or their government agencies, or affect their existing rights and obligations under international or domestic law." However, the United States respectfully submits that a decision by a Member Economy to participate in APEC expresses a serious commitment to privacy, and should be given significant weight in makingany determination as to whether most or all of the requirements of Convention 108 have also been met. Specifically, the following proposals contained in T-PD-BUR(2012)01Rev2_en, if implemented and adopted as revisions to Convention 108, suggest considerable overlap with the APEC CBPR requirements, and the CoE may wish to specifically acknowledge this overlap in an Explanatory Memorandum.

[8] APEC CBPR Privacy Rules and Guidelines, Annex A: Charter of the APEC CBPR Joint Oversight Panel.

- Proposed Article 8bis "Each Party shall provide that the controller is responsible for ensuring respect for the right to the protection of personal data at all stages of the processing….The controller shall establish internal mechanisms to verify and demonstrate to the data subjects and to the supervisory authorities provided for in Article 12 bis of this Convention the compliance of the data processing for which he/she is responsible with the applicable law." Any data controller that is certified for participation in the APEC CBPR program would appear to easily satisfy this criteria.

- Proposed Article 12 paragraph 3(b) reference to "standardized or ad hoc legal measures, such as contract clauses, internal rules or similar measures that are binding, effective and capable of effective remedies, implemented by the person who discloses or makes personal data accessible and by the recipient." Any data controller that is an APEC CBPR Participant is legally bound to comply with the APEC CBPR program requirements and could therefore be considered as having met this criteria.

- Proposed Article 12bis, paragraph 5 requirement that "Each party shall ensure that the supervisory authorities have adequate human, technical and financial resources and infrastructure necessary to accomplish their mission and exercise their powers autonomously and effectively." The certification that a Member Economy must make to the APEC CBPR Joint Oversight Panel, as to the existence of a Privacy Enforcement Authority that participates in the CPEA, and the Member Economy's willingness to rely upon at least one Accountability Agent (which, as noted above, effectively extends the resources of the Privacy Enforcement Authority, particularly with regard to trans-border complaints), should satisfy this requirement.

- Proposed Article 13 paragraph a ("each party shall designate one or more supervisory authorities within the meaning of Article 12bis of this Convention, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe"). This aligns with the APEC requirement that

APEC Economies will establish a publicly accessible directory of organizations that

> have been certified by Accountability Agents as compliant with the CBPR System. The directory will include contact point information that consumers can use to contact participating organizations. Each organization's listing will include the contact point information for the APEC-recognized Accountability Agent that certified the organization and the relevant Privacy Enforcement Authority. Contact point information allows consumers or other interested parties to direct questions and complaints to the appropriate contact point in an organization or to the relevant Accountability Agent, or if necessary, to contact the relevant Privacy Enforcement Authority.[9]

Moreover, given that the APEC directory will be publicly accessible, this should suffice as communication to the Secretary General of the Council of Europe.

In addition, the proposed Article 19 paragraph h, which assigns the Consultative Committee the task of "review[ing] the implementation of this Convention by the Parties in accordance with the provisions of Article 4.3," appears to be a new obligation for which the Consultative Committee might wish or need to leverage existing outside resources. Under the APEC CBPR Joint Oversight Panel Charter, the Joint Oversight Panel will, inter alia:

[9] APEC CBPR Policies, Rules and Guidelines, para. 22.

Collect complaint statistics from recognized Accountability Agents as required under the Accountability Agent Recognition Criteria and circulate to APEC Economies;

Review any reported material change by the recognized Accountability Agent (e.g. ownership, structure or policies) as required under the Accountability Agent Recognition Criteria and report to APEC Economies its recommendation as to whether such change impacts the appropriateness of recognizing the Accountability Agent as compliant with the requirements of the CBPR System; and

Consider and recommend suspension of the recognition of an Accountability Agent at any time;

In addition, under the Charter,

Participation by an APEC Economy in the CBPR System may be suspended or terminated by a consensus determination by the other APEC Economies that one or more of the following conditions have been met:

i. Revocation, repeal or amendment of any domestic laws and/or regulations having the effect of making participation in the APEC CBPR System impossible;

ii. The CBPR Participant's Privacy Enforcement Authority as defined in paragraph 4.1 of the CPEA ceases participation pursuant to paragraph 8.2 of the CPEA; or

iii. Dissolution or disqualification of a previously recognized Accountability Agent where this function is provided exclusively in the CBPR Participant's Economy by that entity.

If there is any participating APEC Member Economy that is also party to Convention 108, all of this information would appear to be quite pertinent to the work of the CoE's Consultative Committee.

Suggestions on Proposed Changes to Convention 108

The United States also takes note of a degree of overlap between the underlying APEC Privacy Principles and Convention 108's key terms and definitions. However, a few key changes to the CoE's proposals, as described below, could greatly increase interoperability between the two.

Article 5 Legitimacy of Data Processing and Quality of Data, Article 12(4)(a) Trans-Border Data Transfers

Proposed Article 5 (Legitimacy of data processing and quality of data), paragraph 2, suggests that data processing may only be carried out on two bases: (a) the data subject's consent, or (b) "as provided for under domestic law for an overriding legitimate interest or is necessary to comply with legal obligations or contractual obligations binding the data subject." Proposed Article 12(4) contains similar restrictions on the trans-border transfer of data. The United States has some suggestions for both (a) and (b) and suggests an additional ground for both processing and transfer.

Article 5(2)(a) Consent

Under the proposed Article 5(2)(a), consent may only serve as a basis for processing if it is "freely given," "explicit," "specific," and "informed" (proposed Article 12(4) (a) references "specific, free, and explicit consent" within the context of trans-border transfers). Similarly, the U.S. Federal Trade Commission (FTC), has concluded that *affirmative express* consent is appropriate before companies (1) use consumer data in a materially different manner than claimed when the data was collected; or (2) collect sensitive data for certain purposes.[10]
Although the concept of consent has been explored in detail in domestic contexts, reaching a global consensus on these issues could be difficult, as the application of this concept has varied widely in the EU and elsewhere...[11] In the APEC Privacy Framework, "consent" is referred to under the Principle entitled "Uses of Personal Information," but the term is not defined in the principles. In the U.S. Privacy and Innovation Blueprint, consent is generally treated as highly contextual.[12]

Given that Convention 108 is designed to apply in a wide variety of both public and private contexts, the United States suggests that the proposed Article 5(2)(a) be shortened to "the data subject has given his/her consent." The concepts of "freely given," "explicit," "specific" and "informed," which are all important to meaningful consent, should then be explained in greater detail in an Explanatory Memorandum and perhaps compared and contrasted with the permissible uses of the "legitimate interest" exception in proposed Article 5(2)(b). It is entirely possible that what some countries and/or APEC member economies would justify on the basis of "consent," others would justify on the basis of "legitimate interest," but they would ultimately reach the same conclusion as to the legitimacy of the processing.

Article 5(2)(b) Legitimate Interests

The proposed phrasing of Convention 108 Article 5(2)(b), "provided for by domestic law for an overriding legitimate interest," might reflect underlying assumptions that are somewhat unique to European law. The laws of non-European countries sometimes operate under the presumption that processing is legal under domestic law unless deemed illegal, whereas the proposed Article 5(2)(b) presumes that all processing will be illegal unless deemed legal. This appears to be a far more restrictive formulation of the "legitimate interest" exception than exists in the EU's proposed Regulation Article 6(1)(f), which does not require that the "legitimate interest" be set forth in domestic law (see below). The United States suggests that the phrase "provided for by domestic law" be omitted and that the term "overriding" either be explained in the Explanatory Memorandum or also omitted.

[10] *See* FTC Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers ("FTC Report"), March 2012, p. 60, available at http://ftc.gov/os/2012/03/120326privacyreport.pdf (emphasis added).

[11] Even within the European Union, which is governed by the 2002 e-Privacy Directive (as amended in 2009 to address personal data collection and use on a user's computer or other device), some member states are implementing the so-called 2009 "Cookie Directive" by requiring express consent in all instances, while others allow for implied consent or take a contextual approach.

[12] *See generally* Privacy and Innovation Blueprint, pp. 11-19 (in particular, the principle of "Respect for Context").

Article 5(2) Other Bases for Processing

> The EU's proposed Regulation, Article 6(1), lists a number of bases for lawful processing of personal data, including where:
>
> (a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject;
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

The CoE's formulation, by contrast, does not reflect the legitimacy of processing in order to protect the vital interests of data subjects, nor does it reflect the legitimacy of processing "when necessary to provide a service or product requested by the individual," as articulated in Principle 4 of the APEC Privacy Principles (Uses of Personal Information).

Article 6 Processing of Sensitive Data

The United States supports the proposed change to Article 6 (Processing of sensitive data, formerly "special categories of data") in that the proposal suggests that the sensitivity of data should be considered in light of whether "their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination." The U.S. FTC regards certain categories of data as per se sensitive; namely, data pertaining to children, health data, financial data, Social Security numbers, and precise geolocation data.[13]The EU has also recognized that certain types of data are inherently sensitive. In the global context, the APEC Privacy Framework does not delineate categories of data deemed per se "sensitive" as, again, there would most likely be no consensus on this issue among a broad array of economies.

[13] *See* FTC Report, pp. 5-8 and 47-48.

Presumably, the underlying idea behind the CoE's delineation of "sensitive" categories of data, and the idea more conducive to global consensus, is that special precautions should be undertaken with regard to the types of data that are more likely to directly impact the legitimate rights or interests of data subjects. In some countries or APEC Member Economies, one's religious or other beliefs or trade union membership, for example, might place a data subject in danger of discrimination or even physical harm, whereas in other countries such data might be considered less troubling. Thus, to reach global consensus, it might be best not to create a comprehensive list of categories of sensitive data, which would allow national authorities to continue to address these issues based on their own analysis of the risk, cultural norms, and national interests.

An alternative articulation of Article 6 might read:

> The [processing] of certain categories of personal data shall be subject to special restrictions or safeguards where such processing presents a serious risk to the interests, rights, and fundamental freedoms of the data subject. The designation of certain categories of personal data as sensitive under domestic law shall be made in light of the nature, likelihood and severity of the harm threatened by the [processing] of such data.

An explanatory memorandum could then set forth a number of examples of how particular categories of data (such as criminal convictions, trade union memberships, etc.) have the capacity to cause serious harm in particular contexts.

Article 7 Data Security / Article 12bis Supervisory Authorities

The proposal for amending Article 7 contains a new requirement that the controller "shall notify, without delay, at least the supervisory authorities within the meaning of Article 12bis of this Convention of any violation of data which may seriously interference with the fundamental rights and freedoms of the data subject." The proposed Article 12bis sets forth a number of requirements for supervisory authorities, including that supervisory authorities "shall accomplish their duties and exercise their powers in complete independence. They shall neither seek nor accept instructions from anyone."

The United States is a strong supporter of data breach notification requirements and is generally supportive of such a requirement being added to Convention 108. The problematic aspect of this proposal, from the U.S. perspective (and possibly the perspective of other APEC Member Economies), is that data breaches often both have cyber security and privacy aspects, and accordingly, different types of reporting requirements and obligations for different sectors of activity that should not be set into conflict with one another. For example, in the U.S. Department of State and in many other U.S. federal agencies, internal regulations generally require that all data breaches be reported promptly to the designated Information Systems Security Officer (ISSO) and/or the Computer Emergency Response Team (CERT); if the data breach involves personal data, there are additional requirements and oversight bodies that become involved. The Article 7 proposal, particular when read in light of the Article 12bis proposal, appears to place sole responsibility for responding to both the cyber security and privacy-related aspects of data breaches on a single privacy enforcement authority. Moreover, the two proposed articles, respectively, use the terms "fundamental rights" and "complete independence," terms which may have resonance within Europe but which seem to foreclose non-European approaches to the management of data breaches, as well as alternative privacy oversight mechanisms. Moreover,

the United States has difficulty understanding how a supervisory authority could work with a multi-disciplinary group in a way necessary to investigate and respond to a complex data breach scenario while “neither seek[ing] nor accept[ing] instructions from anyone.”

Codes of Conduct

Finally, we note that the APEC CBPR framework, described above, is an example of an enforceable code of conduct or certification scheme that effectively facilitates cross-border data transfers while ensuring privacy protections for consumers’ personal data between jurisdictions with different privacy frameworks. We believe that the APEC system has tremendous potential to facilitate accountable and efficient data transfers within the APEC region. All stakeholders in such a system could benefit significantly—consumers because they are dealing with accountable organizations who have opted into an efficient privacy management system that includes effective complaint resolution procedures; companies because the system creates greater efficiency, uniformity and predictability with respect to their privacy and data security requirements; and privacy enforcement authorities, such as the FTC, because an efficient self-regulatory system, coupled with effective backstop enforcement contingencies, improves the effectiveness of their privacy enforcement missions.

This framework, and other similar models, significantly enhances global interoperability, which has become increasingly important to ensure the free flow of information. We think it would be useful for the COE to consider the ability to acknowledge such codes of conduct and certification schemes as a proper basis for cross-border transfers.

Conclusion

The United States again thanks the Council of Europe for the opportunity to comment on its revisions to Convention 108 and looks forward to the future work of rediscovering our shared privacy heritage.

Delegations of the CDCJ / *Délégations du CDCJ*

BELGIUM / *BELGIQUE*

(English verson)

Comments of the Belgian delegation of the CDCJ concerning the proposal of modernisation of Convention 108 – May 2012

The Belgian delegation of the CDCJ considers that it is not appropriate to make specific comments about the text which has been submitted by the T-PD for an opinion to the CDCJ in so far as this text raises a the question of its compatibility with the current European legislation in force as well as with the work in progress within the European Union.

Indeed, the field of data protection is the subject of a major review.
On one hand, the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data has made a text proposal to modernize the Convention 108.

On the other hand within the European Union, a proposal for a Regulation on « data protection » is being negotiated within the Council. This regulation aims to modify the Directive 95/46/EC.

Two problems arise:

- with regard to existing legislation : certain dispositions of the draft modernized Convention 108 are incompatible with existing Union law – notably the Directive 95/46/EC – and with internal legislation of Member States of the Union, in particular as regards the definition of sensitive data as well as cross-border data flows towards third countries.

- with regard to future legislation : these same dispositions are also incompatible with the proposal for a “General Data Protection Regulation” of the European Union, as the proposal currently stands.

Taking this situation into account, the Belgian authorities are currently in the process of determining their position in view of the T-PD.

In this delicate context, it is therefore not appropriate to formulate specific comments on the content of the draft text.

(Version française)

Observations de la délégation belge au CDCJ au sujet de la proposition de modernisation de la Convention 108 – mai 2012

La délégation belge au CDCJ estime inopportun de formuler des commentaires spécifiques au sujet du texte transmis pour avis au CDCJ par le T-PD dans la mesure où ce texte pose la question de principe de sa compatibilité avec le droit communautaire actuel ainsi qu'avec les travaux en cours à l'Union européenne.

La matière de la protection des données fait en effet l'objet d'une profonde révision.
D'une part, le Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel propose un texte afin de moderniser la Convention 108.

D'autre part au sein de l'Union Européenne, une proposition de Règlement "protection de données" est en cours de négociation au Conseil. Ce règlement vise la révision de l'actuelle Directive 95/46/CE.

Deux problèmes se posent :

- par rapport au droit existant : certaines dispositions du projet de modernisation de la Convention 108 sont incompatibles avec le droit existant de l'Union Européenne– la Directive 95/46/CE – ainsi qu'avec les législations des Etats membres transposant la directive notamment en ce qui concerne la définition des données sensibles ainsi que les flux transfrontières de données vers des pays tiers.

- par rapport au droit futur : Ces mêmes dispositions sont également incompatibles avec la proposition de Règlement « vie privée » de l'Union Européenne, dans l'état actuel du projet de texte.

C'est en tenant compte de cet état de fait que les autorités belges définissent actuellement la position qui sera défendue au T-PD.

Dans ce contexte délicat, il ne paraît pas souhaitable de formuler des observations ponctuelles sur le contenu du texte en projet.

AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA
Zagreb, Martićeva 14

Klasa: 018-05/12-01/01
Ur.broj: 567/04-03-12-02
Zagreb, 15. svibnja 2012.

MINISTARSTVO PRAVOSUĐA
Uprava za EU i međunarodnu suradnju
n/p gđa. Helena Husnjak

PREDMET: Modernizacija Konvencije 108 – novi prijedlozi
- mišljenje, daje se

Poštovana gospođo Husnjak,

Obzirom na nove prijedloge Savjetodavnog odbora Konvencije 108 (T-PD-a) u vezi modernizacije Konvencije za zaštitu osoba glede automatizirane obrade osobnih podataka (Konvencija 108) u privitku se dostavlja mišljenje Agencije za zaštitu osobnih podataka.

S poštovanjem

RAVNATELJ
Dubravko Bilić, mag.philol.croat

REPUBLIKA HRVATSKA - AGENCIJA ZA ZAŠTITU OSOBNIH PODATAKA - ZAGREB

Dostaviti:

1. Naslov
2. Pismohrana (1x)

Modernizacija Konvencije 108 nužna je uslijed razvoja informacijsko-komunikacijskih tehnologija u suvremenom društvu te posljedično dolazi i do razvoja brojnih mogućnosti obrade osobnih podataka, odnosno obrade velikog broja (opsega) osobnih podataka, sredstava obrade, učestalog prekograničnog prijenosa osobnih podataka u države (teritorije) koji u svom domaćem pravu ne osiguravaju adekvatnu zaštitu osobnih podataka.

U tom smislu potrebno je primijeniti dodatna jamstva kako bi se osigurala adekvatna zaštita i povjerljivost osobnih podataka koji se obrađuju i prenose u inozemstvo.

Kako proizlazi iz novih prijedloga za modernizaciju Konvencije 108 (koja datira iz 1981. godine) novi prijedlozi prate odredbe Direktive 95/46/EZ kao temeljnog standarda zaštite osobnih podataka EU koji je implementiran u nacionalne zakone država članica EU a koji su obvezne implementirati i sve buduće države članice EU.

Novi prijedlozi tako uključuju prilagođavanje definicija (termina) koji se koriste odnosno na obradu osobnih podataka, navode se kriteriji za zakonitu obradu osobnih podataka, **naglašavaju se obveze svih subjekata – sudionika u sustavu obrade osobnih podataka i to voditelja zbirke osobnih podataka ali i izvršitelja obrade osobnih podataka i primatelja osobnih podataka u inozemstvu, koji su dužni pridržavati se pravila i načela zaštite osobnih podataka u svim fazama obrade osobnih podataka (počevši od njihovog prikupljanja).**

Vrlo je važno da je u novim prijedlozima modernizacije Konvencije navedeno kako obrada osobnih podataka mora biti zakonita, opravdana, poštena i transparentna.

S druge strane detaljno su razrađena **prava ispitanika (pri čemu je jedno od temeljnih i najznačajnijih pravo na informaciju)** odnosno na obradu njegovih osobnih podataka, ali i **prava prigovora na obradu osobnih podataka, prava uvida u podatke koji se obrađuju** i sl.

Obzirom na gore navedeno, Agencija za zaštitu osobnih podataka RH u potpunosti podržava nove prijedloge za modernizaciju Konvencije 108 iznesene u podnesenom draftu.

Prijevod mišljenja na engleski jezik:

Modernization of Convention 108 is necessary due to the development of information and communication technologies in contemporary society, and consequently leads to the development of many possibilities personal data processing, and processing of a large number (range) of personal data, also development of processing resources, frequent cross-border transfer of personal data in the countries (territories) which in its domestic law does not provide adequate protection of personal data.

In this sense, it is necessary to implement additional safeguards to ensure adequate protection and confidentiality of personal data which are processed and transferred abroad.

Following on from the new proposals for the modernization of the Convention 108 (which dates from 1981.) the new proposals follow the provisions of Directive 95/46/EC as a basic

standard of protection of personal data which has been implemented into national laws of EU Member States and this standard are required to implement all future EU member states.

The new proposals include the adjustment of definitions (terms) used regarding to the personal data processing, the criteria for lawful processing of personal data, underline the obligations of all actors in the processing of personal data – data controller, data processor and the recipient of personal data abroad, who are obliged to abide by the rules and principles of protection of personal data in all stages of processing of personal data (starting from their collection).

It is very important that the new proposals for the modernization of the Convention states that processing of personal data must be lawful, reasonable, fair and transparent.

On the other hand, the rights of the data subjects are worked out in detail (one of the most important and fundamental right is right to information) as well as the right to object to the personal data processing, the rights of access to the data which are processed, etc.

Regarding to the above mentioned, the Croatian Personal Data Protection Agency fully supports the new proposals for the modernization of the Convention 108 outlined in the submitted draft.

GERMANY / *ALLEMAGNE*

As at: 25 May 2012

Comments of the Federal Government regarding the planned overhaul of Council of Europe Convention 108

The Federal Government is convinced that Convention 108 and its principles have proved satisfactory in the 30 years of their application and have contributed significantly to ensuring data privacy in Europe and in non-European countries.

In an increasingly globalized world and highly complex information societies, data protection requirements have changed over the years. Therefore, the Federal Government welcomes the initiative to revise Convention 108 and to identify parts that may require modernization and adjustments to meet new challenges and needs.

The Federal Government expressly welcomes the objective of the reform project which is to create a universal set of data protection rules setting global standards; it also welcomes the efforts to dovetail the reform process with the one regarding the new data protection framework in the EU.

Negotiations regarding the European Commission's proposals for a General Data Protection Regulation and a Directive Governing the Law Enforcement Area have already begun. Against this backdrop, the following issues are of particular importance to the Federal Government:

13. The Federal Government finds it important to drive the reform efforts at the level of the Council of Europe forward while the negotiations in the EU are ongoing. Germany and the other Member States share the responsibility for making sure that the two new sets of rules are compatible. Therefore, the Federal Government is prepared to make an active and constructive contribution to the envisaged further negotiations of the proposals to reform Convention 108 in an Ad Hoc Committee. This Committee needs enough time to also discuss - in sufficient depth - questions of a general nature. Further negotiations should however aim to put the reformed Convention 108 into effect as soon as possible, while dovetailing the CoE Convention reform process with the one regarding the new data

protection framework of the EU. It does not seem necessary, though, to wait until the considerably more complex and more detailed reform plans of the EU have been finalized.

14. We should stick to our approach which is to keep up the general character of Convention 108. This is the only way to enforce the universal standard the Convention pursues and to ensure that it has a comprehensive scope (public and private sector).

15. The Contracting Parties of the new Convention should be entitled, as they are under the existing one, to regulate data protection for the public sector and that for the private sector in different manners. Also, the Council of Europe should consider whether it would make sense to make a distinction to this effect in the Convention itself, especially because the constitutional situation for these two sectors differ.

16. Against this backdrop we will have to look at the new regulations in greater depth to see whether they meet the particular requirements of specific public sectors such as the processing of data in criminal investigations and criminal court proceedings, in other court proceedings or in administrative social security proceedings.

17. The Federal Government expressly welcomes the current approach pursued by the reform proposals which is to identify further fundamental rights to be balanced against the right to data protection.

18. Ultimately, all new provisions must therefore be measured against their ability to cater for Internet applications or other technical framework conditions, including new developments and services such as cloud computing. Also, they need to be evolutionary and capable of accommodating all sorts of technologies.

19. We should consider including a catalogue of Internet-related user rights, what with the capabilities of the Internet and users' particular need of protection vis-à-vis providers which frequently act internationally. These user rights could add to the principles already contained in the Convention and flesh out the relationship between providers and users in the private sector.

20. We should look at whether a distinction could be made between data processing entailing a smaller threat to privacy and processes generally representing a greater threat, a basic approach already contained in Article 6 (1) and Article 8 bis (4) of the Draft Convention.

21. A sound balance needs to be struck between the basic rights of freedom of expression, freedom of the press and freedom of information on the one hand and the particular threats to the privacy of data subjects on the other. It is not least against this background that we should consider including a separate provision governing the disclosure of data.

22. We should check to what extent anonymized data may suffice to achieve certain objectives, and whether data may be categorized according to their degree of de-identification, so that pseudonymized data may be put to a greater use than direct personal data, for instance.

23. Article 6 bis (6) of the Draft Convention seeks to avoid excessive burdens on smaller and medium-sized enterprises. That said, the entire Convention should be checked once again for whether it balances, adequately, the privacy interests of data subjects and the administrative burdens arising especially for smaller and medium-sized enterprises.

24. The scope of the exception in Article 3 bis (exception for purely personal or household activities) needs to be discussed further, as it is of general importance and has far-reaching effects.

25. The provisions governing data transfers to third countries also need to be discussed in depth. This is also applicable to the role of data protection supervisory authorities. As regards data transfers by private bodes, i.e. in particular by internationally active enterprises, we should consider creating adequate safeguards, through a yet to be concretized process of regulated self-regulation, making sure that the regulations are actually enforceable. The Council of Europe - together with other international organizations such as OECD or APEC - should look at how to ensure such effective enforcement.

IRELAND / *IRLANDE*

For Ireland’s comments please see page 92.

LATVIA / *LETTONIE*

I would like to announce that Latvia has not any comments on draft of Convention mentioned below.

CDCJ Secretariat
cdcj@coe.int

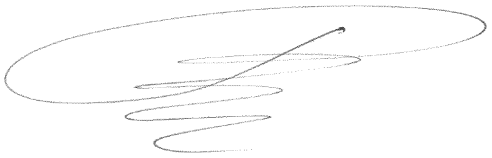
28 May 2012 Ref. No.(1.18.)TR-35

T-PD'S NEW PROPOSALS ON MODERNISATION OF CONVENTION 108

In reply to your e-mail message of 30th April 2012, we would like to inform you that the Ministry of Justice of the Republic of Lithuania supports and welcomes the initiative to set a high level of data protection standards, develop modern and consistent guidelines on transborder flows of personal data and strengthen the rights of data subjects.

However, we would like to draw your attention to certain provisions of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter – Convention 108) proposed in the draft text. There are concerns that the proposed additional text to the explanatory report by introducing the aspect of an individual being "identifiable" would lead to the effect that more data are going to be considered as "personal data" (proposal on Article 2 of Convention 108). As regards the clause "unreasonable time or effort for identification", there are uncertainties whether such a clause would not have the result of being unnecessarily burdensome, in particular for smaller businesses.

Given the fact that there are many different situations where data must be processed, it would be reasonable if proposal on Article 5 paragraph 2 was consistent with the six grounds for lawful data processing as set out in Article 7 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. We would like to emphasize that Lithuania will continue to participate in the negotiation process seeking that the new proposals on modernisation of Convention 108 would ensure coherence and compatibility with the legal framework of the European Union, at the same time guaranteeing a high level of protection of the right to privacy and related human rights.

Vice Minister of Justice  Tomas Vaitkevičius

Povilas Drižas, (8 5) 266 2929, el. p. povilas.drizas@tm.lt
Agnė Veršelytė, (8 5) 266 2909, el. agne.verselyte@tm.lt

PORTUGAL

Please see Portugal’s comments on page 97.

REPUBLIC OF MOLDOVA / *REPUBLIQUE DE MOLDOVA*

Voici quelques remarques sur le projet de la Convention 108 modernisée:

1. Vue les 2 Stratégies du CoE sur les droits de l'enfant et sur la gouvernance de l'Internet, qui font référence au besoin de protection de la vie privée et des données personnelles des enfants, il semble nécessaire que la Convention 108 prévoit une protection adéquate de l'enfant a l'égard du traitement de ses données, ou au moins d'y faire référence dans le rapport explicatif.

2. A l'article 8, lettre (a) exclure le mot "automatise".

3. Le texte ne garde pas une cohérence dans l'utilisation des mots "données" et "données à caractère personnel". Par exemple, l'article 8 lettre (b); article 12 par.2; article 12 bis par.7, lettre (a) font référence aux données a caractère personnel, tandis que dans d'autres articles (art. 9 par. 2; art.12 bis, par.3) les mots "a caractère personnel" sont biffés.

SWEDEN / *SUÈDE*

For Sweden's CDCJ Delegations' comments please see T-PD Delegation's Swedish comments on page 106.

Ministry of JUSTICE

PAPER FROM THE UK OUTLINING PROPOSED AMENDMENTS AND FEEDBACK ON THE LATEST VERSION OF THE MODERNISATION OF THE COUNCIL OF EUROPE'S CONVENTION 108

General points

1. The United Kingdom welcomes this opportunity to contribute suggested amendments to the ongoing modernisation of Convention 108. We have participated actively in previous Plenary and Bureau meetings of the T-PD in order that the modernisation of Convention 108 results in an appropriate outcome that is suitable for the twenty-first century.
2. The United Kingdom supports the protection of personal data based on the principles of necessity and proportionality. We want to see a data protection Convention that protects the rights of data subjects, but does not impose disproportionate costs on data controllers that may adversely impact on their operational capacity.
3. The UK considers it important that Convention 108 and the proposed EU data protection reforms complement one another so that EU member states can easily comply with both frameworks and that there is inter-operability between the two systems, which can of course also affect third countries with whom we share data.
4. The UK supports Council of Europe legislation that is not overly prescriptive and which sets out a high-level and principled set of rules which can serve as a good international standard for data protection.
5. As a common law country, the UK supports wording in legislation that takes into account common law and regards it as included in the terms "national law" and "domestic law".

Specific comments on the proposed text

6. The analysis by the UK of the latest version of the proposed modernisation has focussed on the key policy implications of the proposed changes. The UK therefore may present additional views during the June Plenary meeting.
7. The United Kingdom puts forward the following changes and comments on the proposals:

Article 3(1bis) to read: "This Convention shall not apply to data processing carried out by a natural personal for the exercise of ~~purely~~ personal or household activities ~~unless the data are made accessible to persons outside the personal or household sphere~~." This change is to ensure that no processing that would reasonably be considered household processing is unintentionally covered by the Convention.

Article 6(1): The United Kingdom favours a context-based and risk-sensitive set of rules regarding the classification and restrictions on processing of sensitive data. We also ask for clarity regarding the necessity for and status of the lists of types of sensitive data listed in Article 6(1)(a) and 6(1)(b), given that 6(1)(c) then goes on to give a general condition for what data might be classed as sensitive. The UK would therefore propose the deletion of Article 6(1)(a) and 6(1)(b) if they are not necessary.

Article 8(a) to read (drafting point): "not to be subject to a decision significantly affecting him/her or producing legal effects relating to him/her, based solely on the grounds of an automatic processing of data without having the right to express **firstly** his/her views"

Article 8(d): The UK thinks that this provision should be targeted at automated processing based on profiling, as opposed to all automated processing. It may be useful to read alongside the European Commission's proposed Regulation in this regard, including the outline of what profiling is in Article 20(1). The UK would therefore propose changing Article 8(d) to read: "to obtain knowledge on the reason underlying in the data processing, **if the processing intended to evaluate certain personal aspects relating to this natural person** and the results of which are applied to him/her;"

Article 8bis: The UK would support moving the following provisions to the Explanatory Report as potential "best practice" measures: Article 8bis (2), (3) and (5) (i.e. risk analyses and data protection by design). This is to avoid obligations that are too prescriptive and will allow controllers to implement these as a matter of best practice where necessary and proportionate.

Article 9(2)(b) to read: "protect the data subject or the rights and freedoms of others, notably freedom of expression ~~and information~~." We do not consider that freedom of information should be included in this provision as it is a right provided for in domestic legislation.

Article 10 to read: "Each Party undertakes to establish appropriate ~~judicial and non-judicial~~ sanctions and remedies for violations of domestic law giving effect to the provisions of this Convention." The phrase "judicial and non-judicial" should not be included as this necessarily covers all sanctions. The UK would support an express reference to judicial sanctions in the Explanatory Report.

Delegations of the CDMSI / *Délégations du CDMSI*

DENMARK / *DANEMARK*

No comments to the proposal for modernisation of the 108 Convention.

FRANCE

En réponse à la consultation des membres du CDMSI sur les propositions de modernisation de la Convention 108 du Bureau du T-PD, nous souhaitons plus particulièrement formuler le commentaire suivant :

Nous souhaitons attirer l'attention sur l'existence d'un décalage entre les deux processus de réforme en cours au niveau de l'UE et du Conseil de l'Europe en ce qui concerne la définition des données sensibles. En effet, dans le cadre de la révision de la Convention 108, il est proposé que les données biométriques soient intégrées dans la définition des données sensibles, ce qui n'est pas le cas, pour l'instant, dans les propositions communautaires visant à réformer le cadre de la protection des données.

Aussi, sans se prononcer sur le fond, il nous paraît utile de rappeler la nécessité de veiller à la cohérence des deux exercices de réforme menés en parallèle.

CDMSI observers / *CDMSI observateurs*

EBU

EUROPEAN BROADCASTING UNION / UNION EUROPEENNE DE RADIO-TELEVISION

21.5.2012

EBU comments regarding the Council of Europe's new proposals for modernisation of Convention 108

The EBU welcomes the new opportunity provided by the Council of Europe to comment on its latest proposals to modernise Convention 108 (T-PD-BUR (2010) 01 Rev2_en- 27 April 2012).

As mentioned in its previous comments, dated 28 March 2012, the EBU warmly welcomes the inclusion of an explicit exception for freedom of expression "and information" (those last words should be included) in the Preamble and in Article 9 (1) (b) of the Convention from the requirement of certain provisions. This exception is a key priority for the media.

However, the EBU reiterates its comments and recommends that the Article 9 exception should be reinforced and must cover at least Articles 5, 6, 7 and 8 as foreseen in the current text of the Convention (and in the EC draft Regulation). This exception is already submitted to very restrictive conditions: *"provided for by Law and constitutes a necessary measure in a democratic society".* Moreover, the word "solely" should be removed from the provisions of the explanatory report as it could undermine the purpose of reconciling data protection and freedom of expression.

It is of prime importance that the Convention should find the correct balance between the protection of personal data and freedom of expression and information and should ensure that "the essence of both fundamental rights is not impaired". On the contrary, this could have far-reaching consequences for media activities, and particularly in the online environment.

EUROPEAN MAGAZINE AND MEDIA ASSOCIATION & EUROPEAN NEWSPAPER PUBLISHER'S ASSOTIATION (ENPA & EMMA)

EMMA and ENPA response to proposals from the Council of Europe on the modernization of Convention 108 for the protection of individuals with regard to automatic processing of personal data (5 March 2012)

EMMA, the European Magazine Media Association, and ENPA, the European Newspaper Publishers' Association welcome the opportunity to further comment on the consultation concerning the modernisation of Convention 108.

It is important to underline that in any amendment of the current Convention, the Council of Europe must find the right balance between the fundamental right of personal data protection and the fundamental right of freedom of expression. In particular, it is essential when making any changes to the current framework, to take into account the following:

1. A **robust exemption for processing of personal data for journalistic purposes** is crucial to preserve editorial press freedom and safeguard a free and independent, quality press.

2. The possibility for the press to continue to be able to reach out to potential as well as current subscribers via **direct marketing is essential to safeguard press distribution for the consumer as well as the business to business press**, in order to preserve readership, future press subscriptions and media pluralism.

3. The **future of the digital press must not be jeopardized**: publishers have invested substantial resources in developing digital business models in recent years and a **successful future depends on advertising and digital subscriptions, as well as e-commerce**. It is therefore essential that there are no restrictions that will make it difficult for publishers to be able to interact easily with their readers, and adapt to their needs.

We have several specific comments on various new proposed changes to Convention 108:

Article 2 (a): definition of personal data

We have concerns that the proposed additional text to the explanatory report by introducing the aspect of an individual being 'identifiable', would lead to more data than before being considered as 'personal data'. It is unclear as regards what would be "unreasonable time or effort" for identification. The concern is that such a clause could have the result of being unnecessarily burdensome in particular for smaller businesses, so we would propose amending this.

Article 5.2: legitimacy of data processing

The proposed article 5.2 sets out four grounds for legitimate processing of data: “Free specific informed consent (1) or when domestic law provides for: An overriding legitimate interest (2) or is necessary to comply with legal obligations (3) or contractual obligations binding the data subject (4).” Consent is thus one alternative, but not the only one. This is appropriate because it reflects the fact, that there are many different situations where data must be processed. It would make more sense, however, if this proposal was consistent with the six grounds for lawful data processing set out in Article 7 of Directive 95/46/EC.

A press subscription is a product that must be explained, but which has no retail outlet which would allow a publishers’ representative, for example, to explain it to a potential customer. In order to safeguard press distribution, direct marketing is therefore crucial. It is therefore vital that any explanation in the Explanatory Report of an overriding legitimate interest makes direct reference to the wording in Article 7 f) of Directive 95/46/CE), i.e., which include “*the **legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)*.”

It is **crucial to keep the possibility to process personal data for the legitimate interests of a third party**. Any attempts to suppress this possibility would result in the end of many titles across the EU dependent on subscriptions sales. For example, in many Member States a large percentage of the subscription circulation of certain newspapers and magazines depends on direct marketing by letters sent to third-party addresses without prior consent, which is permitted by national laws based on Art. 7 (f) and Art.14 Directive 95/46/EC under the condition of information to the addressee and his right to object.

- As regards the **business press**, B2B magazines are often sent to their readers (e.g., doctors, computer and financial specialists etc) based on special address lists of the respective target group for free and without prior consent. This so-called ‘controlled circulation’ (which can account for up to 90% of the readership of some business titles in some Member States) is necessary to advertise for a subscription of the magazine but also to secure the required reach in order to attract advertisers and therefore to finance the magazine. This would simply not be possible anymore if this form of marketing was not allowed. The benefits to both customers and publishers from this approach can be contrasted with the marginal objection rates to receiving direct marketing by mail without prior consent (e. g. one example cited was less than 10 objections out of 100.000 letters).

- As regards the **consumer press**, figures we have received from individual publishers in the following Member States show that such marketing letters to third party addressees without consent account for the following percentage of subscribers for various publications: Germany (up to 20%); France (up to 40%); Sweden (up to 46%); Portugal (up to 95%); UK (up to 45%).

Article 7bis: Transparency of processing

In order to be able to continue to provide appropriate press distribution, it has to be possible to provide information in a general way. Overly specific requirements where the processing is necessary for the performance of a contract or to conduct pre-contractual measures is in particular not practical for direct marketing activities that take place by mail or by phone, as opposed to online. We have doubts that the provision of all the information required under 7bis (1) (e.g. on an order card, as regularly used for subscriptions), would be possible.

The proposal provides for an obligation to inform on “the preservation period”. Nevertheless, in many cases it will not be possible to determine the period of data storing in advance. At the time of conclusion of a subscription for an unlimited period it is difficult to know the length of the subscription period, and thus for how long the personal data has to be stored. Even after the termination of the contractual relationship there might be a legitimate interest to continue using the respective data.

The proposal states that: “*The Explanatory Report will specify (…) any other information necessary to ensure a fair data processing, [which] notably includes information on transfers to other countries. The collection of personal data includes both direct and indirect collection. The information regarding the recipients may also refer to categories of recipients*.”

In our view the existence of the word “notably” might create legal uncertainty as regards what type of information a publisher has to provide and would permit an extensive interpretation of the information to be provided.

While we welcome the fact that under Article 7bis (b) a controller shall “*not be required to provide such information where this proves to be impossible or involves disproportionate efforts*”, we are concerned that the question of what constitutes impossible or disproportionate efforts will create legal certainty.

It is also unclear when such information would have to be made available.

Right to information (Article 8, a and b)

Under Article 8 a) individuals are entitled on request to obtain "*at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him / her are being* ***processed or not****, the communication of such data in an intelligible form and* ***all available information on the origin of the data and any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7 bis*** ".

This obligation and the corresponding information requirements (as mentioned above) are vague as "reasonable intervals" is not defined and individual companies will not understand how to comply. To avoid resulting in unnecessary expense it would be more appropriate if this information had to be available upon request.

In Article 8 b) it is further determined that the individual should have the right "***to obtain knowledge of the logic involved in the data processing in the case of an automated decision*** ". Given the risk to confidential internal processes it is important that the Explanatory Report notes – as proposed - that, *"the knowledge of the logic involved in the processing cannot be detrimental to legally protected secrets."*

Decision based on automated data processing (Article 8 e)

Under Article 8 e), any person shall be entitled on request “***not to be subject to a decision significantly affecting him / her or producing legal effects concerning him / her, based solely on the grounds of an automated processing of data without having the right to express his / her views***. " We believe that this broad formulation poses a risk to traditional business models.

One problem is that it is not defined when a decision “significantly” affects someone. It is also unclear what is covered by the requirement “based solely on the grounds of an automated processing of data". It cannot be ruled out that this does not include data processing that is essential for publishers, such as measures for so-called interest-based advertising, which is a crucial means of financing digital publishing offers. These provisions could even potentially affect data processing where there is no identification of a specific person, such as where pseudonymous user profiles have been created to avoid identification of the person concerned.

Exceptions and restrictions (Article 9)

Under Article 9 (1) "*no exception to the provisions of this Convention shall be allowed, except to the provisions of Article 5.3, 6, 7.2, and 7bis and 8 when such derogation is provided for by law and constitutes a necessary measure in a democratic society to [...] b) protect the data subject or the rights and freedom of others,* ***notably freedom of expression and information*** **".**

We are concerned that the **proposed exception by the Council of Europe does not go far enough in protecting the existing standards for journalistic data processing**. The application of data protection rules to journalistic data processing would make free and independent editorial coverage impossible in many cases, given that a large proportion of all information about politics, economics and other social issues would be covered.

As we highlighted in the introduction to this letter, for editorial freedom of the press a robust exception is needed from general data processing rules in order to allow for the processing of the information collected, storage in the editorial archives and the distribution of the finished articles and publications, including in digital form. Furthermore, this exception must be technology-neutral, covering all distribution channels and media types, and any activity associated with the press.

We would recommend that the **exception must therefore cover at least the articles 4-8, 10-21** to ensure a similar level of protection to now. It should be noted, however, that such an exception does not prevent journalistic activities being covered by national media, libel and privacy laws.

We are also concerned that the requirement that such a derogation “**constitutes a necessary measure in a democratic society” could result in further restrictions.** The suggested text to the Explanatory Report, that "*this provision concerns data processing carried out solely for communicating information to the public, ideas or opinions of general interest, or for literary or artistic expression*" does not help in this regard. We would therefore recommend that this restriction is deleted.

EMMA and ENPA call on the Council of Europe to take on board these comments, given the serious implications of changes to Convention 108 for Europe’s press sector.
Please contact us should you wish to discuss this matter further.

Yours sincerely

Francine Cunningham
ENPA Executive Director
Contact: Sophie.scrive@enpa.be
Tel. +32 (0)2 551 01 97

Max Von Abendroth
EMMA Executive Director
Contact: Catherine.starkie@magazinemedia.eu
Tel. +32 (0)2 536 06 02

EMMA and ENPA response to proposals from the Council of Europe on the modernization of Convention 108 for the protection of individuals with regard to automatic processing of personal data (27 April 2012)

EMMA, the European Magazine Media Association, and ENPA, the European Newspaper Publishers' Association welcome the opportunity to comment on the new proposals prepared by the Consultative Committee on the modernisation of Convention 108.
We participated at the meeting with stakeholders organized by the Council of Europe on 2 May and made some remarks.

We would like to reiterate that in any amendment of the current Convention the Council of Europe must find the right balance between the fundamental right of personal data protection and the fundamental right of freedom of expression. In particular, it is essential when making changes to the current framework, to take into account the following:

1. A **robust exemption for processing of personal data for journalistic purposes** is crucial to preserve editorial press freedom and safeguard a free and independent, quality press.
2. The possibility for the press to continue to be able to reach out to potential as well as current subscribers via **direct marketing is essential to safeguard press distribution for the consumer as well as the business to business press**, in order to preserve readership, future press subscriptions and media pluralism.

3. The **future of the digital press must not be jeopardized**: publishers have invested substantial resources in developing digital business models in recent years and a **successful future depends on advertising and digital subscriptions, as well as e-commerce**. It is therefore essential that there are no restrictions that will make it difficult for publishers to be able to interact easily with their readers, and adapt to their needs.
Based on the latest version circulated by the consultative committee (24 April), we would like to reiterate some of our main concerns that we already expressed in our first position paper, as well as making some new comments:

Article 2 (a): definition of personal data

We have concerns that the proposed additional text to the explanatory report by introducing the aspect of an individual being 'identifiable', would lead to more data than before being considered as 'personal data'. It is unclear as regards what would be "unreasonable time or effort" for identification. The concern is that such a clause could have the result of being unnecessarily burdensome in particular for smaller businesses, so we would propose amending this by deleting the word "identifiable" (as well as the corresponding addition concerning "identifiable" proposed to the Explanatory Report).

Article 5.2: legitimacy of data processing

The proposed article 5.2 sets out four grounds for legitimate processing of data: “Free, explicit, specific informed consent (1) or when domestic law provides for: An overriding legitimate interest (2) or is necessary to comply with legal obligations (3) or contractual obligations binding the data subject (4).” Consent is thus one alternative, but not the only one. This is appropriate because it reflects the fact, that
there are many different situations where data must be processed. It would make more sense, however, if this proposal was consistent with the six grounds for lawful data processing set out in Article 7 of Directive 95/46/EC.

However, ENPA and EMMA are concerned by the need to obtain **explicit consent**. This requirement is particularly difficult to apply in the digital environment, especially for those companies, such as newspaper and magazine publishing houses, which are mainly small and medium sized companies, and whose websites are openly accessible to the public. Such a requirement to get explicit consent would therefore advantage major global digital players whose business models are based on log-in, while **putting at risk the digital business models that publishing houses have been investing in. The word explicit should therefore be removed.**

In addition, the wording to Article 5(3)(b), which states that personal data undergoing processing shall be “collected for **explicit**, specified and legitimate purposes”, is too restrictive. It is not sufficient to cite limited examples covering compatible purposes in the Explanatory Report (“statistics, historical or scientific research purposes”), given that there are other purposes which are also legitimate. We are also concerned that Article 5(3)(c), which states that personal data undergoing processing shall be “adequate, relevant, not excessive and **limited to the strict minimum** in relation to the purposes for which they are processed”, is not clear, as well as unnecessary, in particular when considering that the wording “not excessive” is also used.

A press subscription is a product that must be explained, but which has no retail outlet which would allow a publishers’ representative, for example, to explain it to a potential customer. In order to safeguard press distribution, direct marketing is therefore crucial. It is therefore vital that any explanation in the Explanatory Report of an overriding legitimate interest makes direct reference to the wording in Article 7 f) of Directive 95/46/CE), i.e., which include “*the **legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1)*.”

It is crucial to keep the possibility to process personal data for the legitimate interests of a third party. Any attempts to suppress this possibility would result in the end of many titles across the EU dependent on subscriptions sales. For example, in many Member States a large percentage of the subscription circulation of certain newspapers and magazines depends on direct marketing by letters sent to third-party addresses without prior consent, which is permitted by national laws based on Art. 7 (f) and Art.14 Directive 95/46/EC under the condition of information to the addressee and his right to object.

- As regards the business press, B2B magazines are often sent to their readers (e.g., doctors, computer and financial specialists etc) based on special address lists of the respective target group for free and without prior consent. This so-called ‘controlled circulation’ (which can account for up to 90% of the readership of some business titles in some Member States) is necessary to advertise for a subscription of the magazine but also to secure the required reach

in order to attract advertisers and therefore to finance the magazine. This would simply not be possible anymore if this form of marketing was not allowed. The benefits to both customers and publishers from this approach can be contrasted with the marginal objection rates to receiving direct marketing by mail without prior consent (e. g. one example cited was less than 10 objections out of 100.000 letters).

- As regards the consumer press, figures we have received from individual publishers in the following Member States show that such marketing letters to third party addressees without consent account for the following percentage of subscribers for various publications: Germany (up to 20%); France (up to 40%); Sweden (up to 46%); Portugal (up to 95%); UK (up to 45%).

Article 7bis: Transparency of processing

ENPA and EMMA believe that the information required to be provided by the controller would be difficult to implement in practice by publishing houses which are mainly small and medium sized companies.

In order to be able to continue to provide appropriate press distribution, it has to be possible to provide information in a general and concise way. Overly heavy requirements where the processing is necessary for the performance of a contract or to conduct pre-contractual measures are in particular not practical for direct marketing activities. We have doubts that the provision of all the information required under 7bis (1) (e.g. on an order card, as regularly used for subscriptions), would be possible.

The proposal provides for an obligation to inform regarding "the preservation period". Nevertheless, in many cases it will not be possible to determine the period of data storage in advance. At the time of conclusion of a subscription for an unlimited period it is difficult to know the length of the subscription period, and thus for how long the personal data has to be stored. Even after the termination of the contractual relationship there might be a legitimate interest to continue using the respective data.

The proposal states that: "*The Explanatory Report will specify (…) any other information necessary to ensure a fair data processing, [which] notably includes information on transfers to other countries. The collection of personal data includes both direct and indirect collection. The information regarding the recipients may also refer to categories of recipients*."

In our view the existence of the word "notably" might create legal uncertainty as regards what type of information a publisher has to provide and would permit an extensive interpretation of the information to be provided.

While we welcome the fact that under Article 7bis (b) a controller shall "*not be required to provide such information where this proves to be impossible or involves disproportionate efforts*", we are concerned that the question of what constitutes impossible or disproportionate efforts will create legal certainty.

It is also unclear when such information would have to be made available.

Rights of the data subject (Article 8)

The rights of the data subject have been considerably increased and strengthened, but it is questionable whether they are proportionate and can be reasonably fulfilled by legitimate businesses.

As regards Article 8 a), we believe that this broad formulation poses a risk to traditional business models. One problem is that it is not defined when a decision “significantly” affects someone. It is also unclear what is covered by the requirement “based solely on the grounds of an automated processing of data".

It cannot be ruled out that this does not include data processing that is essential for publishers, such as measures for so-called interest-based advertising, which is a crucial means of financing digital publishing offers. These provisions could even potentially affect data processing where there is no identification of a specific person, such as where pseudonymous user profiles have been created to avoid identification of the person concerned.
Under Article 8 c), this obligation and the corresponding information requirements (as mentioned above) are vague as "reasonable intervals" is not defined and individual companies will not understand how to comply. To avoid resulting in unnecessary expense it would be more appropriate if this information had to be available upon request.
In Article 8 d) it is further determined that the individual should have the right "to obtain knowledge of the logic involved in the data processing in the case of an automated decision ". Given the risk to confidential internal processes it is important that the Explanatory Report notes – as proposed - that, "the knowledge of the logic involved in the processing cannot be detrimental to legally protected secrets."

Exceptions and restrictions (Article 9)

Under Article 9 (1) (b), we are concerned that the proposed exception by the Council of Europe does not go far enough in protecting the existing standards for journalistic data processing. The application of data protection rules to journalistic data processing would make free and independent editorial coverage impossible in many cases, given that a large proportion of all information about politics, economics and other social issues would be covered.

A robust exception for press freedom is needed from general data processing rules in order to allow for the processing of the information collected, storage in the editorial archives and the distribution of the finished articles and publications, including in digital form. Furthermore, this exception must be technology-neutral, covering all distribution channels and media types, and any activity associated with the press.

We therefore believe that Article 9(1)b) should ensure that Member States have the obligation to include a press freedom exception in their national law. As the Council of Europe considers that freedom of expression constitutes one of the essential foundations of democratic society and the safeguards to be afforded to the press are of particular importance, this should therefore be reflected in the revised version of the Convention.

We would also recommend that the exception must therefore cover at least the articles 4-8, 10-21 to ensure a similar level of protection to now. Article 5(2), for example, would be particularly problematic as it requires that the data subject must give his/her explicit, specific and informed consent for data processing to be lawful. If this was applied to the press, no reporting would be possible as the press clearly needs to be able to report without this consent.

It should also be noted that such an exception for journalistic data processing is consistent with the subsidiarity principle and it does not prevent journalistic activities being covered by national media, libel and privacy laws.

We are also concerned that the requirement that such a derogation “constitutes a necessary measure in a democratic society” could result in further restrictions. The suggested text to the Explanatory Report, that "this provision concerns data processing carried out solely for communicating information to the public, ideas or opinions of general interest, or for literary or artistic expression" does not help in this regard. We would therefore recommend that this restriction is deleted.

Explanatory report

Many articles of the draft revised Convention refer to the explanatory report for further specification. We find it difficult to comment on the revised articles without knowing the content of the explanatory report. Furthermore, this report could not only increase the administrative burden for companies but also create more legal uncertainty. We therefore question the additional legal effect that the explanatory report could have on the modernized Convention.
EMMA and ENPA call on the Council of Europe to take on board these comments, given the serious implications of changes to Convention 108 for Europe’s press sector.

Please contact us should you wish to discuss this matter further.

Yours sincerely,

Francine Cunningham
ENPA Executive Director
Contact: Sophie.scrive@enpa.be
Tel. +32 (0)2 551 01 97

Max Von Abendroth
EMMA Executive Director
Contact: Catherine.starkie@magazinemedia.eu
Tel. +32 (0)2 536 06 02

Other / *Autre*

BDZV & VDZ

ASSOCIATION OF GERMAN MAGAZINE PUBLISHERS (VDZ)
FEDERATION OF GERMAN NEWSPAPER PUBLISHERS (BDZV)

Position der deutschen Zeitschriften- und Zeitungsverleger zum Vorschlag für eine Modernisierung der Konvention 108
(Stand 08.05.2012)

I. Vorbemerkung

Das Datenschutzrecht ist seit jeher für wesentliche Bereiche der Pressetätigkeit relevant. Redaktionelle Pressefreiheit ist ohne Ausnahmen vom Datenschutzrecht nicht möglich. Adressiertes Direktmarketing klassischer wie digitaler Presseabonnements ist für den Erhalt der Leserschaft unverzichtbar.

Die Digitalisierung und die damit einhergehenden strukturellen Herausforderungen erfordern einen verstärkten Ausbau der digitalen Angebote der Verlage. Die deutschen Zeitschriften- und Zeitungsverleger verfolgen daher auch die Diskussionen über die Modernisierung der Konvention 108 mit großem Interesse. Wichtig ist in diesem Zusammenhang, dass im Rahmen der Modernisierung keine Vorgaben eingeführt werden, die das auf europäischer Ebene mühsam errungene Gleichgewicht zwischen den legitimen Interessen des Einzelnen und den Kommunikationsnotwendigkeiten einer modernen Wirtschaft belasten. Hinzu kommt, dass mit der Veröffentlichung des Kommissionsvorschlags für eine EU-Datenschutzverordnung am 25.01.2012 auf europäischer Ebene gerade die Überarbeitung des EU-Rechtsrahmens begonnen hat. Den Ergebnissen der sich nun anschließenden Diskussionen auf europäischer und nationaler Ebene im Rahmen des Gesetzgebungsverfahrens sollte nicht vorgegriffen werden.

Im Zusammenhang mit der Überarbeitung des Rechtsrahmens für den Datenschutz sind für Zeitschriften- und Zeitungsverleger jedoch generell die folgenden Aspekte relevant:

Robuste Bereichsausnahme für die journalistische Datenverarbeitung erforderlich.

Die Anwendung der Datenschutzvorschriften auf die journalistische Datenverarbeitung würde eine freie redaktionelle Berichterstattung in weiten Teilen unmöglich machen. Ein Großteil aller Informationen über Politik, Wirtschaft und sonstige Gesellschaft, die eine freie Presse frei sammeln, speichern und auswerten sowie veröffentlichen können muss, sind personenbezogen (siehe auch II. Ziffer 5).

Direktmarketing als wesentliche Voraussetzung freier und unabhängiger Presse muss weiter sachgerecht möglich bleiben. Die freie und unabhängige Presse sowie die Medienvielfalt hängen in hohem Maße von der Möglichkeit ab, effektiv für Zeitschriften und Zeitungen zu werben. Es ist daher insbesondere unabdingbar, dass die Datenverarbeitung für zentrale Bereiche des Direktmarketings weiterhin ohne Einwilligung, aber mit Information und Widerspruchsmöglichkeit, zulässig bleibt (siehe II. Ziffern 1 – 4).

Digitale Geschäftsmodelle dürfen nicht belastet werden. Digitale Geschäftsmodelle von der Werbung in der digitalen Presse über die Bewerbung digitaler Abonnements bis hin zum E Commerce sind unverzichtbar**.** Die Überarbeitung der Datenschutzrichtlinie darf daher nicht dazu führen, die Nutzung und weitere Entwicklung solcher Geschäftsmodelle unverhältnismäßig zu beeinträchtigen oder unmöglich zu machen (siehe II. Ziffern 1 – 4).

II. Konkrete Aspekte bezogen auf den Entwurf für die Modernisierung der Konvention 108 vom 27. April 2012

1. Definition of „personal data" (Art. 2 a). Die Definition von „personal data" soll nach dem vorliegendenEntwurf unverändert bleiben. Der Explanatory Report soll jedoch unter anderem um dieAussage ergänzt werden, ''identifiable" does not only refer to the individual's civil identity but alsoto what allows to "individualise" one person amongst others". Dies führt letztendlich dazu, dass dieMenge der als personenbezogene Daten angesehenen Informationen ein nicht mehr überschaubares Maß erreicht. Denn durch Betonung *der Möglichkeit der Individualisierung* könnten wesentlich mehr Daten als bisher als personenbezogen angesehen werden.

Diese Konsequenz wird auch nicht dadurch ausgeschlossen, dass in dem Explanatory Report eingegrenzt werden soll, „an individual is not considered "identifiable" if identification requires unreasonable time and effort for a person who would be informed of it". Nicht näher definiert wird zunächst, unter welchen Voraussetzungen von „unreasonable time and effort" ausgegangen werden kann. Hinzu kommt, dass selbst, wenn man diese Einschränkung weit interpretiert, noch immer eine erhebliche Anzahl an Informationen als „personal data" eingestuft werden könnten. Der somit mögliche weite Anwendungsbereich und die damit einhergehenden Pflichten für die Verarbeitung der entsprechenden Informationen führen für Unternehmen zu einem nicht mehr überschaubaren Aufwand. Angesichts der möglicherweise betroffenen unterschiedlichen Kategorien von Daten, von denen viele nach geltender Rechtslage wohl nicht als personenbezogen angesehen würden, ist dieser Aufwand in vielen Fällen wohl auch mangels Schutzbedürftigkeit aus Verbraucherschutzgesichtspunkten nicht gerechtfertigt. Die zitierte Ergänzung des Explanatory Reports sollte daher wieder gestrichen werden.

2. Legitimacy of data processing and quality of data (Art. 5).
In dem Entwurf für einen neuen Abs. 2 des Art. 5 ist bestimmt, „Each Party shall provide that data processing can be carried out only if a) the data subject has freely given his/her explicit specific and informed consent, or b) the processing is provided for by domestic law for an overriding legitimate interest or is necessary to comply with legal obligations or contractual obligations binding the subject". Durch diese Vorgaben könnten zahlreiche der nach heutiger Rechtslage möglichen und wichtigen Datenverarbeitungsprozesse erheblich belastet, wenn nicht sogar unmöglich gemacht werden.

Dies gilt zum einen, als in dem heute maßgeblichen Art. 7 der Richtlinie 95/46/EG sechs Alternativen festgelegt sind, von denen eine erfüllt sein muss, damit die Datenverarbeitung zulässig ist. Das ist auch sachgerecht, da dadurch dem Umstand Rechnung getragen werden kann, dass es viele unterschiedliche Situationen gibt, in denen Daten legitimerweise verarbeitet werden müssen. Nach dem vorliegenden Vorschlag soll es jedoch nur noch vier Alternativen geben.

Zum anderen lässt sich nicht ausschließen, dass die Möglichkeiten der Datenverarbeitung zur Verfolgung legitimer Interessen des Verarbeitenden und Dritter ohne vorherige Einwilligung, aber mit Information und der Möglichkeit zum Widerspruch, weiter eingeschränkt werden

(derzeit zulässig gemäß Art.7 f) der Richtlinie 95/46/EG). Denn festgelegt wird, dass die Zulässigkeit der entspre3 chenden Datenverarbeitung im nationalen Recht festgelegt werden soll. Hierbei muss man berücksichtigen, dass die Überarbeitung des EU-Rechtsrahmens für den Datenschutz gerade darauf abzielt, ein europaweit einheitliches Recht zu schaffen, und in eine Verordnung münden soll. Nach dem Entwurf der EU-Kommission werden die Bedingungen für die zulässige Datenverarbeitung daher direkt in der Verordnung festgelegt, ohne dass noch eine Umsetzung in nationales Recht erforderlich wäre. Sichergestellt werden muss daher, dass durch eine entsprechende Überarbeitung des europäischen Datenschutzrahmens diese Vorschrift nicht ausgehöhlt wird. Sachgerechterweise sollte daher diese Vorgabe um die Möglichkeit ergänzt werden, dass die entsprechende Festlegung auch in europäischem Recht erfolgen kann.

Ausgeführt wird zudem, der Explanatory Report „will explain the meaning of overriding legitimate interest (including by taking the examples of Section 7 of the Directive 96/46/EC) and that consent may be withdrawn". Richtigerweise sollten zwar die bisher in Art. 7 der Richtlinie aufgeführten Alternativen der zulässigen Datenverarbeitung weiter gelten. Sinnvollerweise sollten diese Alternativen jedoch bereits im Konventionstext selbst aufgeführt werden.

Als Bedingung für die Datenerhebung wird in Abs. 3 b) näher spezifiziert: „Personal data undergoing processing shall be: […] b) collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes". In diesem Zusammenhang wird auch darauf hingewiesen "The Explanatory Report will give examples of compatible purposes (statistic, historical or scientific research purposes that are a priori compatible provided that other safeguards exist and that the processing is not the ground for a decision to be taken concerning the data subject.

Problematisch ist zunächst die Formulierung, dass die Daten für explizite Zwecke gesammelt werden müssen. Diese Formulierung lässt zumindest Raum für realitätsferne Interpretationen, die den Bürokratieaufwand sowohl für Verbraucher als auch für Unternehmen erheblich und unverhältnismäßig erhöhen. Sichergestellt werden muss daher insbesondere, dass es möglich bleibt, den Zweck der Datenerhebung auch generalisierend zu bestimmen (z. B. „Datenerhebung für Werbezwecke" etc.). Zu problematischer Auslegung kann auch der Vorschlag führen, als Beispiele für legitime Zwecke der Datenverarbeitung in dem Explanatory Report lediglich solche aus dem statistischen, historischen oder wissenschaftlichen Forschungsbereich aufzuführen. Eine solche – wenn auch nur beispielhafte – Aufzählung berücksichtigt nicht, dass es auch im wirtschaftliche Bereich zahlreiche Datenverarbeitungsprozesse gibt, die legitimen Zwecken dienen und zudem wichtige Voraussetzung für verschiedenste Geschäftsprozesse sind. Hier sollte daher eine entsprechende Ergänzung erfolgen bzw. von der beispielhaften Aufzählung abgesehen werden.

Die Gefahr erheblicher Rechtsunsicherheit birgt zudem die Ergänzung des Vorschlagstextes in Abs. 3 c) „Personal data undergoing processing shall be: […] c) limited to the strict minimum in relation to the purposes for which they are processed". Für Unternehmen ist nicht ohne Weiteres nachvollziehbar, was unter dem „strict minimum" in diesem Sinne zu verstehen sein soll. Diese Ergänzung ist zudem aber auch nicht notwendig, als bereits durch die Vorgabe, dass die Erhebung der Daten nicht „excessive" sein darf, das Prinzip der Datensparsamkeit Berücksichtigung findet.

Bei etwaigen Überlegungen zur Änderung der geltenden Rechtslage muss in jedem Fall sicher gestellt werden, dass die Möglichkeiten der effektiven Leserwerbung für die Presse nicht weiter eingeschränkt werden. Es ist daher insbesondere unabdingbar, dass die Datenverarbeitung für

zentrale Bereiche des Direktmarketings weiterhin ohne Einwilligung, aber mit Information und Widerspruchsmöglichkeit, möglich bleibt. Dies ist für die Presse wie für viele andere Branchen eine wichtige, und teilweise sogar die einzige, Möglichkeit, mit ihren Kunden in Kontakt zu treten oder neue Kunden zu gewinnen. Das gilt besonders für kleine und mittelständische Unternehmen, die sich keine Postwurfsendungen oder Werbung in den Massenmedien leisten können.

In Deutschland hängen bis zu 20% der Abonnementauflage vieler Zeitungen und Zeitschriften von adressiertem Direktmarketing ohne vorherige Einwilligung an Fremdadressen ab. Für das Segment lokaler und regionaler Zeitungen haben aktuelle Befragungen sogar ergeben, dass Werbebriefe an Fremdadressen bis zu 50 % der befristeten Abonnements und bis zu 20 % der neugewonnenen unbefristeten Abonnements generieren. Dieses Bild wird auch durch die Erfahrungen aus anderen europäischen Ländern bestätigt, in denen der entsprechende Anteil der Auflage sogar teilweise über 40 % ausmacht.

Bei der Fachpresse macht der Abo-Anteil regelmäßig nur einen kleinen Teil der Auflage aus. Der größte Teil der Auflage (teilweise bis ca. 90 %) wird kostenlos im sog. Frei- und Wechselversand auf der Basis spezieller Adresslisten an die jeweils relevante Zielgruppe (zum Beispiel Maschinenbauer, Bäcker oder Architekten) versandt.

Digitale Geschäftsmodelle dürfen nicht belastet werden.
Die Forderung nach einer expliziten Einwilligung könnte aber nicht nur traditionelle Kommunikationswege, sondern auch die Entwicklung und Nachhaltigkeit digitale Angebote der Verlage erheblich beeinträchtigen. Es stellt in diesem Zusammenhang insbesondere die Frage, ob die Forderung nach einer expliziten Einwilligung eventuell Auswirkungen auf die Möglichkeit hat, die erforderliche Einwilligung im Rahmen der EPrivacy Richtlinie 2002/58/EG unter bestimmten Voraussetzungen durch Browser-Einstellungen auszudrücken (wie dies etwa in Erwägungsgrund 66 der Richtlinie 136/2009 vorgesehen ist). In diesem Zusammenhang sollte berücksichtigt werden, dass auch vordergründig nur geringfügige Änderungen des geltenden Rechtsrahmens erhebliche Konsequenzen haben können. Etwaige Verschärfungen des geltenden Rechtsrahmens dürfen nicht dazu führen, dass das Nutzerlebnis beeinträchtigt und die Funktionalität des Internets insgesamt gefährdet wird.

Forderung nach expliziter/genereller Einwilligung bevorteilt große, international tätige Unternehmen. Es muss zudem darauf geachtet werden, dass keine Vorgaben eingeführt werden, die zwar von großen, global tätigen Unternehmen relativ einfach erfüllt werden können, nicht jedoch von der Mehrzahl der kleinen und mittelständischen Unternehmen in Europa.

Das gilt besonders für die im Rahmen der Diskussion teilweise erhobene Forderung nach einer generellen Einwilligung für alle Datenverarbeitungsprozesse. Eine solche generelle vorherige Einwilligung würde grundsätzlich diejenigen Unternehmen begünstigen, deren Geschäftsmodell ohnehin auf einem Log-In-Modell aufgebaut ist. Das gilt etwa für große international tätige E-Mail- Anbieter oder soziale Netzwerke, die vor der Nutzung ihrer Dienste eine Anmeldung erfordern. Diese können wesentlich einfacher und von einer Vielzahl von Nutzern eine solche Einwilligung erhalten als andere, insbesondere national, regional oder sogar lokal gebundene Unternehmen, die einen freien Zugang zu ihren Angeboten ermöglichen.

Es ist zum Beispiel regelmäßig nicht erforderlich, sich vorab anzumelden, um die Online-Angebote von Zeitschriften und Zeitungen zu nutzen. Jeder direkte Kontakt mit dem Kunden zur

Einholung einer Einwilligung (wie etwa entsprechende Pop-Up-Fenster auf Internetseiten) birgt daher die Gefahr, von diesen als Störung und damit als negativer Aspekt des Angebotes wahrgenommen zu werden.

Darüber hinaus besteht bei einer derartigen Pflicht die erhebliche Gefahr, dass Verbraucher großen global agierenden Unternehmen, die ihnen bekannt sind und bei denen sie evtl. bereits sogar ein umfassendes Profil angelegt haben, eher eine Einwilligung erteilen, als evtl. nur national agierenden, nicht in der Öffentlichkeit stehenden kleineren Unternehmen. Für letzte würde dies zu einem erheblichen Wettbewerbsnachteil führen.

Hinzu kommen die ganz praktischen Bedenken, dass die weite Definition personenbezogener Daten zu einer Inflation von Einwilligungsanfragen an den Nutzer führen und zu einem enormen Datenvolumen in den Datenbanken der Unternehmen führen würde.

3. Transparency of processing (Art. 7 bis). Die geltenden Informationspflichten wurdenGegenüber dem geltenden Text erweitert. Sichergestellt werden muss jedoch, dass diese auch praktikabel sind. Dies gilt zunächst etwa für die Information über mögliche Empfänger der Daten. Hier muss es möglich sein, dass diese Information auch generalisierend erfolgen kann. Richtigerweise wird daher auch im Explanatory Report darauf hingewiesen, „the information regarding the recipients may also refer to categories of recipients“. Dieser Hinweis sollte daher auch in den endgültigen Text übernommen werden. Hinzu kommt, dass es für Unternehmen nicht rechtssicher ersichtlich ist, welche Informationen zur Verfügung gestellt werden müssen. Denn diese umfassen nach der Vorschrift auch „any other information necessary to ensure a fair data processing“. In dem Explanatory Report soll zwar näher spezifiziert werden, „any information necessary to ensure a fair data processing“ notably includes information on transfer to other countries”. Die Einschränkung durch “notably” weist jedoch darauf hin, dass dieses Beispiel nicht abschließend gemeint ist. Die in Abs. 2 enthaltene Abwägungsklausel vermag diese Problematik ebenfalls nicht abzumildern. Denn bestimmt ist dort lediglich bestimmt, dass diese Informationen nicht zur Verfügung gestellt werden müssen, wenn „this proves to be impossible or involves disproportionate efforts“. Nicht näher ausgeführt wird jedoch, wann diese Bedingung erfüllt ist.

Unklar ist zudem, was unter beabsichtigten Ergänzung des Explanatory Reports zu verstehen ist, dass die Information „direct, readable, etc.“ sein mus. Dies lässt Raum für verschiedenste Interpretationen und birgt damit die Gefahr erheblicher Rechtsunsicherheit.

Berücksichtigt werden muss im Zusammenhang mit der Festlegung von Informationspflichten aber auch, dass diese Informationsverpflichtungen auf allen Kommunikationswegen sinnvoll verwirklicht werden können müssen. Es muss sichergestellt werden, dass nicht durch die Festlegung von Informationspflichten traditionelle und bewährte Kommunikationswege (z. B. beim Direktmarketing für Zeitschriften und Zeitungen die Bestellkarte oder der Werbebrief) nicht mehr genutzt werden können, da sich bei diesen die Fülle an geforderten Informationen einfach nicht mehr angemessen erfüllen lässt.

Unklar ist nach der jetzigen Fassung des Entwurfes außerdem, wann die entsprechenden Informationen zur Verfügung gestellt werden müssen. Dies ist jedoch ein entscheidendes Kriterium für die Beurteilung der Praktikabilität der entsprechenden Verpflichtung. Ausgeführt ist hierzu lediglich, dass der Explanatory Report dies spezifizieren wird. Dies reicht jedoch nicht aus, um eine abschließende Beurteilung zu ermöglichen.

4. Rights of the data subject (Art. 8)
Auch die erweiterten Vorschriften zu den Rechten des Einzelnen bergen die Gefahr weiterer Belastungen für Verlage.

a) Auskunftsrecht (Art. 8 b und d). Bestimmt ist in Art. 8 c), dass der Einzelne das Recht haben
soll, zu erfahren „at resonable intervals and without excessive delay or expense confirmation or not of the existence of data processing relating to him/her the communication in an intelligible form of the data processed, all available information on their origin as well as any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7bis".

Die Verpflichtung, dem Einzelnen in angemessenen Intervallen die entsprechenden Informationen zukommen zu lassen, ist nicht nur zu unbestimmt, sondern auch zu weitgehend. Zunächst wird nicht näher erläutert, was unter „reasonable intervals" zu verstehen ist. Für das einzelne Unternehmen ist damit nicht rechtssicher ersichtlich, in welchen Zeitabständen er dieser Verpflichtung nachkommen muss. Hinzu kommt, dass diese Verpflichtung unabhängig von dem gewählten Intervall zu einem erheblichen Aufwand für Unternehmen führt und in vielen Fällen auch von dem Einzelnen überhaupt nicht gewünscht sein mag. Sachgerechterweise sollte diese Auskunft daher lediglich auf Anfrage erfolgen.

In Art. 8 c) ist weiter bestimmt, dass der Einzelne auch das Recht haben soll, "to obtain knowledge of the reasoning underlying in the data processing the results of which are applied to him/her,". Abgesehen davon, dass diese Verpflichtung aufgrund des weiten Anwendungsbereiches wohl zu einem nicht mehr überschaubaren Aufwand für Unternehmen führt, dürften in zahlreichen Fällen von dieser Ausnahme auch Geschäftsgeheimnisse betroffen sein. Richtigerweise wird daher auch in dem Explanatory Report darauf hingewiesen, "the knowledge of the logic involved in the processing cannot be detrimental to legally protected secrets". Dies sollte auch in den endgültigen Text übernommen werden.

b) Decision based on automated data processing (Art. 8 a). Festgelegt wird in Art. 8 a) das Recht des Einzelnen, „not to be subject to a decision significantly affecting him/her or producing legal effects concerning him/her, based solely on the grounds of an automated processing of data without having the right to express his/her views". Aufgrund dieser weiten Formulierung birgt diese Vorschrift die Gefahr, traditionelle und bewährte Geschäftsmodelle deutlich zu belasten bzw. sogar unmöglich zu machen.

Aufgrund der generalklauselartigen Formulierung des Art. 8 a) lässt sich nicht abschließend absehen, welche Datenverarbeitungsmaßnahmen konkret darunter fallen. Nicht definiert wird insbesondere, wann eine „decision significantly affecting him/her" vorliegt. Unklar ist außerdem, unter welchen Voraussetzungen von einer „solely on the grounds of an automated processing of data" basierenden Maßnahme ausgegangen werden muss. Dies gilt insbesondere für die Fälle, in denen die entsprechende Datenverarbeitung zwar automatisiert, aber auf der Basis zuvor durch eine Person festgelegter Kriterien erfolgt.

Es lässt sich daher nicht ausschließen, dass darunter auch zahlreiche Datenverarbeitungsprozesse fallen, die für Verlage essentiell sind, wie etwa Maßnahmen im Rahmen der Kundenbindung oder sog. interessenbasierte Werbung, die als eine wichtige Werbeform im Online-Bereich zur Finanzierung digitaler Verlagsangebote relevant sein kann.

Diese Vorschriften könnten aufgrund der weiteren Formulierung sogar für Datenverarbeitungsprozesse gelten, bei denen keine Identifizierung einer bestimmten Person erfolgt, wie die Erstellung pseudonymisierter Nutzungsprofile zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

5. Exceptions and restrictions (Article 9). In Art. 9 Abs. 1 ist bestimmt, "no exception to the basic principles expressed in this Chapter shall be allowed, except to the provisions of Article 5.3, 6, 7.2, 7bis and 8 when such derogation is provided for by law and constitutes a necessary measure in a democratic society to […] b) protect the data subject or the rights and freedom of others, notably freedom of expression and information".

Robuste Bereichsausnahme für Presse unumgänglich. Die Ausnahme geht nicht annähernd weit genug und würde die geltenden Schutzstandards für die journalistische Datenverarbeitung erheblich einschränken. Für die redaktionelle Pressefreiheit ist eine robuste Bereichsausnahme von den Datenschutzvorschriften unumgänglich. Diese muss technologieneutral alle Verbreitungswege und Medientypen und jede mit der Pressetätigkeit einhergehende Datenverarbeitung von der Beschaffung der Information und ihrer Archivierung im Redaktionsarchiv bis hin zur Verbreitung der fertigen Artikel und Publikationen – auch in digitaler Form – umfassen.

Die Anwendung der Datenschutzvorschriften auf die journalistische Datenverarbeitung würde eine freie redaktionelle Berichterstattung in weiten Teilen unmöglich machen. Ein Großteil aller Informationen über Politik, Wirtschaft und sonstige Gesellschaft, die eine freie Presse frei sammeln, speichern und auswerten sowie veröffentlichen können muss, sind personenbezogen. Deutlich wird dies etwa bei der Vorschrift des Art. 5 Abs. 2, der die Voraussetzungen für die Datenverarbeitung festlegt. Die Datenverarbeitung soll danach nur zulässig sein, wenn er Einzelne darin eingewilligt hat oder diese im nationalen Recht vorgesehen bzw. notwendig ist, um rechtliche oder vertragliche Pflichten zu erfüllen. Würde diese Vorschrift auch auf die journalistische Berichterstattung angewendet, wäre eine kritische oder kontroverse Berichterstattung in weiten Teilen unmöglich, weil regelmäßig wohl keine Einwilligung zu dieser gegeben würde. Aber auch eine Festlegung im nationalen Recht schafft insoweit keine Abhilfe. Die Presse muss gerade unabhängig von einer etwaigen und wie auch immer gearteten staatlichen Erlaubnis berichten können, soll sie in sachgerechter Weise ihre Rolle in einer demokratischen Gesellschaft erfüllen können.

Die Ausnahme muss daher zumindest die Artikel 4-8, 10-21 vollständig umfassen, um ein vergleichbares Schutzniveau wie bisher sicher zu stellen.

Direkt anwendbare Ausnahme erforderlich. Die Möglichkeit der Mitgliedstaaten, entsprechende Ausnahmen vorzusehen, reicht nicht aus, um den geltenden Schutzstandard zu wahren. Die Ausnahmen müssen vielmehr verpflichtend und ohne Relativierung von den Mitgliedstaaten eingeführt werden**.** Eine Umsetzung auf nationaler Ebene, die im Ermessen der Mitgliedstaaten liegt, birgt zudem die Gefahr unterschiedlicher Schutzstandards. Der jetzige Wortlaut fördert dies, indem er nur vorgibt, dass *Ausnahmen* von bestimmten Artikeln lediglich „erlaubt" sind.

Auch die Vorgabe, dass es sich bei den entsprechenden Ausnahmen um „a necessary measure" handeln muss, damit ein Mitgliedstaat überhaupt eine solche Ausnahme einführen darf, eröffnet einen weiten Ermessenspielraum und birgt die Gefahr weiterer Einschränkungen. Diese Problematik wird noch dadurch unterstrichen, dass im Explanatory Report spezifiziert werden soll, „a measure shall be considered as „necessary in a democratic society" to pursue a

legitimate aim if it meets a „pressing social need“ which cannot be achieved by less intrusive means and, especially, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it appear “relevant and sufficient”” Diese Einschränkung muss daher gestrichen werden, soll das geltende Schutzniveau nicht aufgeweicht werdenEs sollte vielmehr eingefügt werden, dass die Mitgliedstaaten die Ausnahmen zu den o.g. Artikel einführen müssen, da eine solche notwendig in einer demokratischen Gesellschaft ist, um das Recht auf Schutz der Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Rechten in Einklang zu bringen.

Unmittelbare Geltung der Ausnahme wird auch Postulat der Subsidiarität gerecht. Eine entsprechende Ergänzung der Ausnahmen bedeutet im Übrigen nicht, dass die jeweiligen journalistischen Aktivitäten in einem rechtfreien Raum stattfinden. Diese können vielmehr weiterhin durch das jeweilige nationale Medien-, Äußerungs- und Persönlichkeitsrecht geregelt werden.

Ansprechpartner:

VDZ BDZV
Dr. Christoph Fiedler Helmut Verdenhalven
Geschäftsführer Europa- und Medienpolitik Geschäftsführer Medienpolitik
Tel.: 0049 30 72 62 98 120 Tel.: 0049 30 72 62 98 203
c.fiedler@vdz.de verdenhalven@bdzv.de

Dr. Karina Lott Carolin Wehrhahn
Referentin Europa- und Medienpolitik Referentin Europapolitik
Tel.: 0032 2 536 06 03 Tel.: 0032 2 551 01 94
k.lott@vdzv.de wehrhahn@bdzv.de

CEDPO

COMMENTS
of theConfederation of European Data Protection Organisations (CEDPO)
on the MODERNISATION OF CONVENTION 108: new proposals
*T-PD-BUR(2012)01Rev2_en -**France Germany Spain The Netherlands***
CEDPO: info@cedpo.eu

---

www.cedpo.eu

CEDPO comments on the modernisation of Convention 108

I. INTRODUCTION

The Confederation of European Data Protection Organisations (CEDPO) was founded in 2011. Founding members of CEDPO are:

***AFCDP** Association Française des Correspondants à la Protection des Données à Caractère Personnel*

(http://www.afcdp.net)

***APEP** Asociación Profesional Española de Privacidad (http://www.apep.es)*

***GDD** Gesellschaft für Datenschutz und Datensicherheit (http://www.gdd.de)*

***NGFG** Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (http://www.ngfg.nl)*

Together the above organisations represent the interests of private and public sector organisations, data protection officers (DPOs) and other data protection professionals from the four European Member States.

The main purpose of CEDPO is to promote the important role of the data protection officer (DPO) and balanced, practicable, and effective data protection in general. In addition, CEDPO aims to contribute to better harmonisation of data protection law and data protection practices in the European Union / European Economic Area. Based on the experiences gathered and shared by the national data protection organisations, the confederation plans to initiate and maintain constructive communications with competent European institutions. Harmonisation of data protection practices will also be achieved thanks to the interaction between the members of the different national associations.

CEDPO recently published its First Position Paper on the European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). The Position Paper is available on the CEDPO website at www.cedpo.eu.

CEDPO would like to take the opportunity to also comment on the envisaged modernisation of CONVENTION 108, especially with regard to the role of the DPO.

II. COMMENTS ON THE MODERNISATION OF CONVENTION 108

CEDPO welcomes the initiative to modernise Convention 108.

However, CEDPO is disappointed to learn that the designation of Data Protection Officers (DPOs)
shall be limited to only briefly being mentioned in the commentary of Article 8bis. There it is stated
as follows:

"The Explanatory Report will specify that one of the possible measures could consist of the designation of a 'data protection officers' entrusted with the means necessary to fulfil its mission independently and of whose designation the supervisory authority has been informed. They can be internal or external to the Controller."

Experience shows that appointing DPOs helps to improve the protection of personal data. An independent study commissioned by the Dutch Ministry of Justice found that organisations that have appointed a DPO have a higher degree of compliance awareness and knowledge1. This is also underscored by the long and successful tradition of DPOs in Germany and the growing number of 'the Controllers of the file'2 appointing DPOs in France. In Spain, where the DPO role is not mandatory except for security measures regarding specific processing, it has become evident – at least for large companies - that this role is indispensable. DPOs play a key role in accountable organisations.

Both, the European Commission3 and the Article 29 Working Party4 have already recommended the appointment of DPOs. In addition, the important and growing role of DPOs has been recognised globally in the “Madrid Resolution” on international privacy standards approved by data protection authorities from over 50 countries at the 31st International Conference of Data protection Commissioners in 2009. One of the most relevant chapters of the document is the one that refers to proactive measures5. It includes the recommendation to appoint data protection or privacy officers, with adequate qualifications, resources and powers for exercising their supervisory functions adequately.

1 Brouwer-Korf, A. (2009). Rapport 'Gewoon Doen, beschermen van veiligheid en persoonlijke levenssfeer'. Den Haag, the Netherlands.
Pro Facto (2008) H.B. Winter et. al *Wat niet weet, wat niet deert: Een evaluatieonderzoek naar de werking vande Wet bescherming persoonsgegevens in de praktijk*
Conclusion reached by the Second Chamber based on the research, “Evaluation of the Data Protection Act” (Tweede Kamer, vergaderjaar 2009-2010, 31 051, nr. 5, page. 29.)
2 Referring to the current *Convention 108 - Convention for the Protection of Individuals With Regard to the Processing of Personal Data*, Article 2 d
3 COM(2003) 265 final – Report, p. 18 and 24
4 WP 106, p.22 and 23
5 *Internacional [sic] Standards on the Protection of Personal Data and Privacy* The Madrid Resolution, Part VI: Compliance and Monitoring, 22, 1st paragraph point b.

The European Commission is obviously seeing the DPO as an important element within a modern legal framework; it has dedicated three articles solely on the designation, position and

tasks of DPOs in both the proposed General Data Protection Regulation as well as in the Police Directive.

Given all the strong signals, CEDPO recommends the Council of Europe to explicitly include wordings in the main text of Article 8bis of the new Convention 108 which deal with the designation and the role of DPOs.

Moreover, ***CEDPO feels that additional incentives for the designation of the DPO are needed.***

In this regard the First CEDPO Position Paper mentioned in the above introduction may serve as a valuable resource.

CEDPO welcomes the opportunity to support the modernisation of Convention 108 and to constructively contribute to the improved protection of individuals with regard to automatic processing of personal data.

Bonn, Den Haag, Madrid, Paris,
25th May 2012

EDRI

European Digital Rights (EDRI) Submission
to
The Council of Europe Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS 108] (T-PD)

Modernisation of Convention 108: New Proposals
T-PD-BUR(2012)01Rev2_en of 27 April 2012

Meryem Marzouki
30 May 2012

About EDRi

European Digital Rights, EDRi, is a European not for profit, non-governmental digital rights organisation. EDRi was founded in 2002 by 10 organisations (only NGOs may be members) from 7 European countries. Since then EDRi membership has grown consistently. Currently 32 organisations have EDRi membership. They are based in or have offices in 20 different countries in Europe. In addition 27 observers participate in the organisation's mailing lists and activities. We think of Europe in terms of the Council of Europe territory - not strictly its Member States.

EDRi's objectives are to promote, protect and uphold fundamental human rights and freedoms in the digital environment. Examples of such fundamental human rights are the freedom of expression, privacy, data protection and access to knowledge.

To this end, we strive to monitor, report and provide education about threats to civil rights in the field of information and communication technology. Among our recent awareness raising tools are our widely disseminated booklets on the various issues EDRi deals with (available at: http://www.edri.org/papers). Another example is our bi-weekly newsletter, the EDRi-gram, which is in its 10th year of high quality reports on digital rights in Europe.

We conduct policy research and offer the results to the public and to national and international bodies. Recent examples are our contributions to the European Commission's expert groups on RFID and on the Internet of Things, our responses to the European Commission and Council of Europe (CoE) consultations and our work as observers to CoE working groups.

Furthermore, EDRi and its members advocate at a national and international level by actively engaging with bodies such as the European Union, the Council of Europe, the OECD (EDRi was instrumental in CSISAC formation and recognition by OECD), The International Conference of Data Protection and Privacy Commissioners (through The
Public Voice Global Civil Society Coalition, which authored the Madrid Privacy Declaration on "Global Standards for a Global World"), The WIPO and the United Nations as well as organising and participating in a number of conferences and public events.

EDRi also serves as a platform for cooperation and common activities, combining the influence, experience, knowledge, and research of its members. EDRi's activities are primarily driven and carried out by its members' representatives in addition to their national activities. Together EDRi members, observers and friends advocate and inform civil society, industry and the policy sector to uphold fundamental rights such as privacy and freedom of speech in the information society.

Introduction

These comments from European Digital Rights (EDRi) refer to the new proposals for the Modernisation of Convention 108, made by the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS N°108] (T-PD) and dated 27 April 2012 (T-PD-BUR(2012)01Rev2_en).

These EDRi comments complement its comments on previous versions of the Modernisation of Convention 108, submitted at the following occasions:

- Organization of a civil society consultation as a special session of the PrivacyCamp.eu, held on 24 January 2012 in Brussels (http://edri.org/Privacy-Camp-EU)
- Presentation by Meryem Marzouki during the 5th International Conference on Computers, Privacy and Data Protection, as a speaker on the Panel "Modernising Convention 108 in the Face of the IT Revolution" (27 January 2012, Brussels ; available at: http://edri.org/files/2012Marzouki-CPDP-CoEConv108.pdf).
- Oral comments made by Meryem Marzouki during her participation to the consultation organized by the Council of Europe on 2 May 2012 in Brussels, and attended by both civil society and business organizations.

EDRi reiterates its support to the overall objectives of the Modernisation process, and expresses its satisfaction that most of its earlier comments have been taken into account in subsequent versions of the proposal. While EDRi generally welcomes this latest draft, some provisions still needs some revision as discussed in the current submission. EDRi notes that a number of the criticised provisions below are additions that only appeared, or re-appeared, in the draft dated 27 April 2012.

Article 2 – Definitions

[§a] The current definition of a personal data rightly relates to the notion of the possible identification of the data subject, directly or indirectly. However, the proposed explanatory report note is likely to weaken this definition, since it will lead to consider an individual as not identifiable in case the identification process requires "unreasonable time or effort". This explanatory note should be more restrictive, since in some cases "unreasonable time or effort" may be worth spending in comparison to the (commercial or non commercial) advantage derived from identification. Such reasonableness should thus be evaluated on a case by case basis, with regards to the interests at stake, i.e. with regards to both the privacy interests of the data subject and the purpose of the identification by the data controller.

Article 3 - Scope

[§1bis] EDRi supports the exclusion of the data processing carried out by an individual in the course of purely personal or household activities, unless the data are made accessible to persons outside of this circle. However, this paragraph should specify that this restriction applies

whether the data are made accessible intentionally or unintentionally. Indeed, since this paragraph mainly addresses the case where the individual uses social networks or other cloud-based services in order to process the data, there are situations where these data become accessible beyond the private circle, while this was not the user's intention and even in some cases without his/her knowledge (e.g. through changes of privacy settings by the service).

[§1ter] EDRi considers that this paragraph, which allows any Party to the Convention to apply it to legal persons, should be deleted. First of all, it is beyond the scope of the Convention, which deals with the protection of "individuals". Secondly, this provision contradicts the very notion of "personal" data protection. Furthermore, the paragraph raises major concern with respect to freedom of information and the right to access to documents (where the concerned legal person is a public entity) and with respect to the principles of transparency and accountability that are necessary in a democratic society (where the concerned legal person is a private entity). Additionally, the proposed EU Regulation on data protection does not include such a provision, and it defines the data subject as a natural person only.
While EDRi understands the concern expressed by some current Parties to the Convention, arguing for compliance with their current national law, the reasons stated above relate to the respect of fundamental rights and fundamental democratic principles, and thus supersede the inconvenience of modifying an existing national law. Such legitimate harmonisation is, after all, the ultimate objective of an international Convention.
Similarly, the argument that such provision already exists in the current version of Convention 108 cannot be considered as really sound in the framework of a modernisation process. As a matter of fact, the provision was already tentatively weakened – though not entirely removed as it should be – in previous draft versions of the modernisation, where the provision was relegated to the explanatory report.

Article 5 – Legitimacy of data processing and quality of data

[§2a] This paragraph introduces a consent regime, where the data subject's consent need to be "free, explicit, specific and informed". This provision calls for particular caution, since these characteristics are highly variable according to the context, and are difficult to assess in practice. What is a "free" consent when it is given by the data subject in order to benefit from a so-called free of charge service? What is an "informed" consent when the data subject accept terms of services through a simple click, in most cases without having even read and understood the contract, and sometimes when defaults settings are modified without notice by the service provider? What is an "explicit" or "specific" consent given when using web2.0 services that process data collected via other services? What really matters here is that the given consent be meaningful.

[§2b] This paragraph provides for lawful conditions of data processing in absence of the data subject's consent. EDRi's opinion is that these conditions should be more restricted than in the currently proposed version. To this end, the "overriding legitimate interest" should be an "overriding public legitimate interest in a democratic society" (in reference to data processing by government agencies). In reference to data processing by private entities, EDRi considers that domestic law should not provide for exceptions to comply with "contractual obligations binding the data subject" without any restriction, and thus suggests binding such exceptions with compliance to the fundamental rights to privacy and personal data protection.

Article 6 – Processing of sensitive data

[§1] EDRi supports the need to consider that some data are, or become, sensitive either by their nature, the way they are used or because their processing presents serious risks to the interests, rights and freedoms of the data subject. However, it seems inappropriately restrictive to identify such cases with pre-established categories of data as it is currently done in this provision. For instance, some biometric data are sensitive by their nature and not simply by the use made of them. Same applies to other categories of data listed under **1(b)**.
EDRi therefore suggests to rewrite paragraph 1 as follows:
"The processing of certain categories of personal data shall be prohibited, whether such data are sensitive by their nature, by the use made of them, or where their processing presents as serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

Such sensitive data are: genetic and biometric data; data related to health or sexual life; data related to criminal offences or convictions or security measures; and data revealing, directly or indirectly, racial origin, political opinions or trade-union membership, religious or other beliefs".
[§2] This paragraph provides for an exception on the prohibition of sensitive data processing, "where domestic law provides appropriate safeguards". EDRi's opinion is that such safeguards should be more precisely qualified in order to avoid abuses. EDRi suggests as a minimum to add that in such case the processing be subject to prior authorization from the national Supervisory Authority. This would ensure that the Supervisory Authority has the knowledge of this processing of sensitive data and of its operational conditions, and has the ability to assess its relevance and the respect of appropriate safeguards. The result would be to guarantee the exceptional character of a derogation to the general regime of prohibition of sensitive data processing.

Furthermore, the definition of biometric data envisioned in the explanatory report is not accurate: on the one hand, biometric data not only relate to physical, biological or physiological characteristics of an individual, but also relate behavioural ones (such as dynamic signature, key stroke dynamics, walk patterns, etc.); on the other hand, biometric data not only allow the unique identification of an individual but also his/her authentication.

Article 7 - Data security

[§2] This provision, dealing with data breach notifications, is welcome but currently too weak to actually avoid possible breaches of the fundamental rights and freedoms of the data subject or his interests. In order to overcome this problem without imposing too cumbersome and unnecessary obligations on the controller (especially when the controller is an SME), EDRi suggests to consider a two-level system of data breach notification obligation, so that (i) the Supervisory Authority is notified in any case of data breach and (ii) the data subject is also notified when the data breach presents serious risks for him/her or when the Supervisory Authority decides so. A suggested rewriting of this paragraph could thus be as follows:
"Each Party shall provide that the controller shall notify, without delay:

- *The Supervisory Authorities within the meaning of Article 12bis of this Convention of any violation of data;*
- *The data subject when the violation of data presents a serious risk of interference with his/her fundamental rights and freedoms or with his/her interests*
- *The data subject upon request by the Supervisory Authorities."*

Article 7bis - Transparency of processing

[§2] One of the mention currently intended to be made in the explanatory report (information of measures taken in case of transfers to countries which do not have an adequate system of data protection) should appear in the text of the Convention itself, namely as an exception to paragraph 2 of Article 7bis, which currently provides that the controller is not required to provide information on the data processing when "it proves to be impossible or involves disproportionate efforts". Otherwise, it is likely that Article 7bis(2) would be invoked precisely in contexts of transfers to countries which do not have an adequate system of data protection, thus jeopardizing the very purpose of Article 7bis.

Article 8 - Rights of the data subject

All provisions of Article 8 are currently are entitled only upon the data subject request. There is a need to differentiate in this respect between provisions of paragraphs (a) to (f). EDRi suggests that the differentiation be made on the following bases:

- Some provisions need to be guaranteed even without any explicit request from the data subject. These rights are those provided in:

  [§a] which refers to the data subject's right not to be subject to a significant decision based on the ground of a data processing.

  [§b] which refers to the data subject's right to object to the processing of his/her personal data. If this right is only entitled upon request, EDRi is concerned that this provision may be formulated in a way that could undermine the data subject's right to refuse consent on his/her data processing and could contradict provisions contained in Article 5.

- Some provisions necessarily require a proactive action from the data subject in the form of a request. These rights are those provided in:

  [Old§c] which refers to the data subject's right to rectification or erasure.

  [§e] which refers to the data subject's right to remedy.

  [§f] which refers to the data subject's right to benefit from the assistance of a Supervisory Authority.

- Some provisions are indeed entitled only upon request in the current version of Convention 108. However, EDRi expects much more from the modernization process than simply a status quo on these issues. The modernization process should lead to improvement and widening of the right to information and access to processed data. One way to achieve this progress for citizen rights should be to ensure that such information is provided to the data subject without the need for his/her request, on a regular and reasonable basis (e.g. once a year), in a systematic manner. This would allow for citizen empowerment, and would entitle the data subject to specifically ask for more information, upon request. Otherwise, one might wonder how the data subject could send a request for information and access to his/her data, when s/he does not even know that these data are processed. Rights needing such improvement are provided in:

[New§c] which refers to the data subject's right to information and access to his/her processed data.

[§d] which refers to the data subject's right to information related to the logic underlying the data processing.

Article 9 - Exceptions and restrictions

[§1a] Among the exceptions to the basic data protection principles, this paragraph now includes again the "prevention" of criminal offences. EDRi is very concerned with this new development in the latest draft, since it relates to intelligence purposes, before any infraction has been committed, and not simply to law enforcement purposes. EDRi thus suggests that this exception should either be removed from the current list, or at the very least be accompanied with adequate additional safeguards.

Article 12bis - Supervisory authorities

[§3] (competent authority). EDRi wonders whether this provision would remain compatible with the EU Regulation, especially given that the Modernization process of Convention 108 will be completed before the adoption of the EU proposed Regulation on Data Protection. This paragraph should thus be written in a neutral way with this respect.

[§9] (lack of competence of Supervisory Authority with respect to data processing by judicial bodies). EDRi fears that this very generic wording could apply not only to a judge, but also to a prosecutor during police investigation. EDRi thus suggests to clarify the wordings of this paragraph.

EPA

TEXT OF THE CONVENTION – PROPOSALS
TITLE : CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

CURRENT TEXT OF THE CONVENTION	PROPOSALS
Preamble	Preamble
The member States of the Council of Europe, signatory hereto,	The signatories of this Convention,
Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;	unchanged
Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;	Considering that it is necessary, given the increase in and diversification of processing and exchanges of personal data, to guarantee the dignity and protection of fundamental rights and freedoms of every person, in particular through the right to control one's own data and the use made of them. *Explanatory report will underline that human dignity implies that individuals can not be treated as objects and be submitted to machines, and consequently that decisions based solely on the grounds of an automated processing of data can not be made without individuals having the right to express their views.*
Reaffirming at the same time their commitment to freedom of information regardless of frontiers;	Recognising that the right to data protection is to be considered in respect of its role in society and that it has to be reconciled with the other human rights and fundamental freedoms, including the freedom of expression;
Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,	Recognising that it is necessary to promote at the global level the fundamental values of respect for data protection, thereby contributing to the free flow of information between peoples;
	Recognising that this Convention is to be interpreted with due regard to its explanatory report,

Comment [DP4]: We suggest that an appropriate wording of this provision can be "**of respect for privacy with regard to the processing of personal data**".

Article 3 – Scope	Article 3 – Scope
1 The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.	1 Each Party undertakes to apply this Convention to data processing carried out by any controller subject to its jurisdiction. 1bis This Convention shall not apply to data processing carried out by a natural person for the exercise of purely personal or household activities, unless the data are made accessible to persons outside the personal or household sphere for the exercise of activities other than purely personal or household activities. 1ter Any Party may decide to apply this Convention to information on legal persons.
	In the explanatory report, specify what is meant by the exercise of purely personal or household activities, and making accessible to persons outside the personal or household sphere (to be illustrated according to several criteria, including notably the indefinite number of persons of the CJUE judgement in the Lindqvist case). Also cover services and products offered in the context of domestic activities (if the service provider acts for his/herself or for a third party with respect for data which has been provided to him/her, in other wordsif it goes beyond what is necessary in terms of the service offered, he/she begins a processing of data. If he/she is within the jurisdiction of a Party to the Convention, he/she will be subject to the data protection law of that Party). *Specify that while the processing concerns data of natural persons, the Parties nevertheless have the possibility to extend the protection to legal persons.*
2 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe:	delete

Comment [DP5]: We suggest deleting this provision to guarantee consistency with the positions adopted at the European Union level.

a that it will not apply this Convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law;	delete
b that it will also apply this Convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality;	delete
c that it will also apply this Convention to personal data files which are not processed automatically.	delete

Article 6 – Special categories of data	Article 6 – Processing of sensitive data
Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.	1 The processing of certain categories of personal data shall be prohibited, whether such data are sensitive: by their nature, namely genetic data, data related to health or sexual life, data related to criminal offences or convictions, or security measures; by the use made of them, namely biometric data, data whose processing reveals racial origin, political opinions or trade-union membership, religious or other beliefs, or; where their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination. 2 Such data may nevertheless be processed where domestic law provides appropriate safeguards or with the consent of the data subject.

	The *Explanatory Report will explain that "serious risk" includes injury to dignity or to physical integrity, "genetic data" means all data concerning the hereditary characteristics of an individual or characteristics acquired during early prenatal development, "biometric data" means all data concerning the physical, biological of physiological characteristics of an individual that allow his/her unique identification.*
Article 7 – Data security	Article 7 – Data security
Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.	1 Every Party shall provide that the controller, and, where applicable the processor, takes the appropriate security measures against accidental or unauthorised modification, loss or destruction ~~accidental~~, as well as against unauthorised access or dissemination of personal data processed.
	2 Each Party shall provide that the controller shall notify, without delay, at least the supervisory authorities within the meaning of Article 12 bis of this Convention of any violation of data which may seriously interfere with the fundamental rights and freedoms of the data subject. *The Explanatory Report will specify that the controller should be encouraged to also notify, where necessary, the data subjects.*
	Article 7bis – Transparency of processing
	1. Each Party shall provide that every controller must ensure the transparency of data processing and in particular provide data subjects with information concerning at least his/her identity and habitual residence or establishment, the purposes of the processing carried out by him/her, the data processed, the recipients of the personal data, the preservation period and the means of exercising the rights set forth in Article 8, as well as any other information necessary to ensure a fair data processing.

	2. The controller shall nonetheless not be required to provide such information where this proves to be impossible or involves disproportionate efforts. The *Explanatory Report will specify when the information should be given, that the information should be direct, readable etc, and that "any other information necessary to ensure a fair data processing" notably includes information on transfers to other countries.* *The information should also include measures taken to guarantee data protection in the context of transfers to countries which do not have an adequate system of data protection.* *The collection of personal data includes both direct and indirect collection. The information regarding the recipients may also refer to categories of recipients.*
Article 8 – Additional safeguards for the data subject	Article 8 – Rights of the data subject
Any person shall be enabled:	Any person shall be entitled on request:
a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;	a not to be subject to a decision significantly affecting him/her or producing legal effects relating to him/her, based solely on the grounds of an automatic processing of data without having the right to express his/her views;
	b to object at any time for legitimate reasons to the processing of personal data concerning him/her;
b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;	c to obtain at reasonable intervals and without excessive delay or expense confirmation or not of the existence of data processing relating to him/her, the communication in an intelligible form of the data processed, all available information on their origin as well as any other information that the controller is required to provide to ensure the transparency of processing in accordance with Article 7bis; d to obtain knowledge of the reasoning underlying in the data processing, the results of which are applied to him/her ;

Comment [DP6]: We suggest adding that the information can be given by all means adapted to be intelligible and understandable by all groups of data subjects concerned, including children and people with low education. In this sense we suggest adding that figurative means of providing information such as cartoons are deemed to be adequate means to provide information.

Comment [DP7]: This provision seems not completely in line with data protection rationale, but more with access rights and rights to be informed in specific sectors, such as banking, public administration etc. The scope of the provision goes beyond the purposes of data protection legislation since it imposes obligations to companies that are not (only) strictly related to data processing. More specifically, the provision aims at prohibiting the practice of automated decisions without the power of the data subject to express his view. This is more a subject matter for consumers' protection legislation. Furthermore, this provision risks not to be very effective since there are no sure effects as regards the views expressed by the data subject, more precisely there is no guarantee that the views expressed by the data subjects will be taken into due account by the recipient. Finally, this provision (and the obligations thereof) hinders many business sector, for instance the insurance sector, where it is current practice that the consumer/client interacts with an IT system to obtain an offer or to enter into an agreement based on several criteria, included e.g. the accidents caused by the user etc. Therefore we suggest deleting this provision. In the view of EPA, the aim of this provision represents the typical case of tension between "privacy by theory" (to be ... [1]

Comment [DP8]: The considerations expressed as regards letter a) partially apply as well. A general obligation to motivate all decisions taken by public and private entities is out of the scope of the Convention and risks to generate useless red tapes for businesses and public authorities.
This provision risks to have a too wide application field well beyond data protection.
Therefore we suggest deleting this provision.

	Explanatory Report: this right can, in accordance with Article 9, be limited where this is necessary in a democratic society, in order to protect "legally protected secrets".
c to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;	unchanged
d to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.	See e below
	e to have a remedy if no response is given to a request for confirmation, communication, rectification, erasure or to an objection, as referred to in this Article;
	f to benefit, whatever his/her residence, from the assistance of a supervisory authority within the meaning of Article 12 bis, in exercising the rights provided by this Convention. *Explanatory report: 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.*
	Article 8bis – Additional obligations

	1- Each Party shall provide that the controller is responsible for ensuring respect for the right to the protection of personal data at all stages of the processing and for taking all appropriate measures to implement the domestic legal provisions giving effect to the principles and obligations of this Convention. 2- The controller, or where applicable the processor, shall carry out a risk analysis of the potential impact of the foreseen data processing of sensitive data within the meaning of Article 6 of this Convention on the rights and fundamental freedoms of the data subject. 3- The controller, or where applicable the processor, shall design data processing operations in such a way as to prevent or at least minimise the risk of interference with the right to the protection of personal data. 4- The controller shall establish internal mechanisms to verify and demonstrate to the data subjects and to the supervisory authorities provided for in Article 12 bis of this Convention the compliance of the data processing for which he/she is responsible with the applicable law. 5- Each Party shall provide that the products and services intended for the data processing shall take into account the implications of data protection from the stage of their design and include easy-to-use functionalities allowing the compliance of the processing with the applicable law to be ensured. 6- The obligations included in the domestic law on the basis of the provisions of the previous paragraphs may be adapted according to the size of the controller, or where applicable the processor, the volume of data processed and the risks for the interests, rights and fundamental freedoms of the data subjects. *The Explanatory Report will specify that one of the possible measures could consist of the designation of a 'data protection officers' entrusted with the means necessary to fulfil its mission independently and of whose designation the supervisory authority has been informed. They can be internal or external to the controller.*

Article 9 – Exceptions and restrictions	Article 9 – Exceptions and restrictions
1 No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.	1 No exception to the basic principles expressed in this Chapter shall be allowed, except to the provisions of Articles 5.2, 5.3 , 6, 7.2, 7bis and 8 when such derogation is provided for by law and constitutes a necessary measure in a democratic society to: *Explanatory Report: a measure shall be considered as "necessary in a democratic society" to pursue a legitimate aim if it meets a "pressing social need" which cannot be achieved by less intrusive means and, especially, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it appear "relevant and sufficient".*

Comment [DP9]: This insertion is necessary to adequately protect *inter alia* freedom of expression and of information of journalists. It is not reasonable that no exception to the rule of consent of data subjects is foreseen.

Chapter III – Transborder data flows Article 12 – Transborder flows of personal data and domestic law	Chapter III – Transborder data flows Article 12
1 The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.	1 Each Party shall ensure that personal data will only be disclosed or made available to a recipient who is not subject to its jurisdiction on condition that an adequate level of data protection is ensured.
2 A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.	2 When the recipient is subject to the jurisdiction of a Party to the Convention, the law applicable to this recipient is presumed to provide an adequate level of protection and a Party shall not, for the sole purpose of data protection, prohibit or subject to special authorisation the disclosure or making available of data. The Conventional Committee may nevertheless conclude that the level of protection is not adequate.

Comment [DP10]: We see a potential conflict between the text of the Convention and the text of the EU Data Protection legislation, provided that some countries are not members of the EU/EEC but are signatory states of the Convention. Probably we have to rely on a high level of uniformity between the European Commission and the Conventional Committee in establishing which countries have an adequate level of protection.

Chapter V – Consultative Committee.	Chapter V – Conventional Committee
Article 18 – Composition of the committee	Article 18 – Composition of the committee
1 A Consultative Committee shall be set up after the entry into force of this Convention.	Unchanged except the title of the Committee

2 Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the Convention shall have the right to be represented on the committee by an observer.	unchanged
3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the Convention to be represented by an observer at a given meeting	3 The Conventional Committee may, by a decision taken by a majority of two-thirds of its representatives entitled to vote, invite an observer to be represented at its meetings.

Article 20 – Procedure	Article 20 – Procedure
1 The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.	1 The Conventional Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this Convention. It shall subsequently meet at least once a year and in any case when one-third of the representatives of the Parties request its convocation.
2 A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.	Conventional Committee
	3 Every Party has a right to vote. Each State which is a Party to the Convention shall have one vote. On questions related to its competence, the European Union exercises its right to vote and casts a number of votes equal to the number of its member States that are Parties to the Convention and have transferred competencies to the European Union in the field concerned. In this case, those member States of the European Union do not vote. When the Committee acts according to provisions of litera (h), (i) and (j) of Article 19, however, both the European Union and its Member States vote. The European Union does not vote when a question which does not fall within its competence is examined.
3 After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the Convention.	Unchanged except the title of the Committee and numbering

FEDMA

THE FEDERATION OF EUROPEAN DIRECT AND INTERACTIVE MARKETING

FEDERATION OF EUROPEAN DIRECT AND INTERACTIVE MARKETING
PUBLIC AFFAIRS & SELF-REGULATION 25 May, 2012

FEDMA submission on the proposals (version 27th April) for the modernisation of Convention 108

FEDMA (Federation of European Direct and Interactive Marketing Associations) would like to take this opportunity to respond to the Council of Europe's proposal for the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data.

General Comments:

FEDMA welcomes the Council of Europe's work on modernising Convention 108 on data protection, providing a comprehensive framework equipped to handle privacy issues resulting from technological developments, and ensuring enforcement of data protection standards within the jurisdictions of the Convention.

FEDMA supports the basic principles of the Convention, and especially appreciates that the Convention protects individuals against privacy intrusions not only by the private sector, but also by public authorities. FEDMA believes that both industry and governments should abide by the same rules, especially, when one considers that governments generally collect and process large amounts of sensitive data (health, criminal record) and have the means to interconnect these databases. Truly believing in the balance of interest, FEDMA would also be supportive of the insertion of a reference to the right to do business within the preamble of the Convention along the following lines:

"Recognising that it is necessary to promote at the global level the fundamental values of respect for privacy and data protection, thereby contributing to the free flow of information between peoples **and organisations."**

FEDMA greatly appreciates that the Council of Europe has taken on board the comments received from stakeholders, including FEDMA, in preparing this new draft revised proposals for the review of the Convention 108 (version from 27 April 2012). However, we remain concerned about some provisions of the draft revised text of Convention 108.

Article 5:

• Purpose limitation

Article 5.3 b states that personal data may not be further processed in a manner that is incompatible with the purposes for which they were originally collected, except when the processing is provided for by law, or the data subject has given its consent. Moreover, the

Council of Europe plans to detail in the future Explanatory Report examples of compatible purposes, such as statistics, historical or scientific research purposes. FEDMA strongly believes that when assessing compatible use of data, the overall legitimate interest of the data controller

to process data should be taken into account. Only when a purpose for processing personal data can't be based on the data controller's legitimate interest, should it be considered as incompatible purposes. Moreover, FEDMA is worried that the Explanatory Report to be prepared in the future by the Council of Europe will not only provide just a few examples, but rather an exhaustive list of compatible purposes rather than just examples. This will mean that the definition of 'compatible purposes' will not be able to adapt to industry developments

Article 6:

• Special categories of data

FEDMA appreciates the changes made in article 6, to provide lists of sensitive data category. However, we feel that the reference to "where their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination," needs further guidance. There is a risk that Convention members may interpret the 'risk of discrimination' too widely.

FEDMA considers this article will lead to legal uncertainty for industry and governments alike. The categories of personal data deserving 'special protection', are very much individually and culturally determined. Furthermore, personal data, such as name and address when applied in a different context can be considered as presenting serious risks to data subjects. For example, age, or year of birth, is generally considered harmless1. However, when combined with other personal data and used in a different context, such 'harmless personal data' can become 'sensitive personal data' as when selecting recipients for promoting hearing aids. Today on the internet, names and pictures can provide racial information on the data subject, but are not necessarily considered as sensitive personal data. The same data can present different level of risk depending on the national and cultural background.

FEDMA therefore strongly urges the Council to explicitly state what data are considered sensitive data in an exhaustive list.

Article 8:

• Automated decisions

The proposal introduces in article 8. the right of the data subject not to be subject to a decision based solely on the grounds of automated processing without having the right to express his/ her views. In FEDMA's opinion this right should be limited. An individual should only have such a right when the automated decision-making process has negative legal effects on him/her. FEDMA believes in the benefits and value of profiling for marketing purposes for both the controller and the data subject and in profiling being a fundamental part of commercial, ideal and charitable business processes, essential for any economical activities and growth. In order to bring clarity, this article should reflect the clear distinction existing between normal and expected profiling, and profiling with negative legal effects.

Thus, we believe the Article 8 should refer to negative legal effects affecting the data subject.

When an individual for example wants to retract money from an ATM machine and the machine refuses, this is an automated decision solely based on the fact that the data subject doesn't have enough credit (contractual agreement). In this case, the individual should not have the right to express his views. The Convention should recognize that automated decisions are a

fundamental part of commercial, governmental, retail charitable and business processes. Only when the interests pursued by the controller are overridden by the interests for fundamental rights and freedoms of the individual, should the individual have the right not to be subject to an automated decision without having expressed his views.

Article 8 bis:

• Additional measures for the controller

Article 8 bis introduces additional measures of accountability for the data controller, such as a privacy risk analysis and other documentation on processing. However, we feel that the article is too prescriptive, and places too much emphasis on documentation. The problem of being prescriptive is that the flexibility which a general accountability principle gives is lost. There is no one-size-fits-all model, as measures to be put in place to satisfy compliance with the accountability principle depend on multiple factors such as the size of a database, whether or not data will be disclosed to third party, type of data, type of processing, just to name a few. Moreover, the importance placed on documentation leads to unnecessary administrative burden. Just for maintaining sets of documents that prove the organisation's compliance with the Convention, many SMEs would need to dedicate a person/department to fulfil these duties. This investment could be better spent on, for instance, privacy awareness education for employees, which would contribute far more to protecting data subject's rights under the Convention. FEDMA therefore strongly recommends the Council to suggest clauses stating the accountability principle in general terms. This will in turn provide the data controller with the freedom to choose his own means to ensure compliance with the Convention within his organisation, as well as reducing the administrative burden.

Vagelis Papakonstantinou

In pursuit of the meeting of May 2, 2012, held in the Council's premises in Brussels, on the modernization of its *Convention for the protection of individuals with regard to automatic processing of personal data* (Convention 108) and the Secretariat's subse-quent request for the participants' written amendments and proposals on the Conven-tion's latest draft (T-PD-BUR(2012)01Rev2_en/27.04.2012), please note the follow-ing:

a. Amendment of the draft Convention's Article 1 (purpose) to include the 'free flow of information'

Convention 108 is the only data protection instrument applicable in Europe that does not place the '*free flow of information*' as its, joint, objective together with the protec-tion of personal data undergoing processing. Both the EU Data Protection Directive (as is also the case with the draft Regulation as released by the Commission in early 2012) and the OECD Guidelines place the '*free flow of information*' as their explicit objective – also in the transborder data flow context. This is an important distinction, because data protection instruments are not intended to prohibit the circulation of in-formation but rather to regulate it to the benefit of both data subjects and data proces-sors.

The T-PD appears to have acknowledged the importance of the 'free flow of information', because it explicitly refers to it to the Preamble of the draft Convention. In addition, a whole Chapter of the draft Convention regulates transborder data flows (Chapter III). **It is consequently justified and expected that the 'free flow of in-formation' is added in Article 1 of the Convention, as its explicit purpose togeth-er with the right to data protection**.

b. Elimination of legal persons from the draft Convention's scope

Here again, Convention 108 is unique among European data protection instruments that applies the right to data protection also to legal persons. On the contrary, the EU Data Protection Directive excludes legal persons for its scope and the same appears to be the case with the OECD Guidelines. Only in secondary EU legislation (on elec-tronic communications) are legal persons protected in the same way as individuals – but admittedly such legislation regulates a single and particular field of processing.

The application of the right to data protection to legal persons appears awk-ward. With regard to the text of the draft Convention, it is difficult to explain, for in-stance, how its object and purpose ("*to secure for every individual the right to the protection of personal data, thus ensuring the respect for their rights and fundamental freedoms*", Article 1) would apply to a legal person. The same is the case with the da-ta quality principles ("*personal data undergoing processing shall be processed law-fully and fairly*", Article 5) or with sensitive data (Article 6). In fact, it is difficult even to imagine that, for the purposes of applying the right to data protection to legal per-sons, '*data subjects*' within the meaning of Article 2 of the draft Convention ("*identi-fied or identifiable individuals*") may refer to an organization!

In the same context it should also be noted that recently the USA Supreme Court ruled that the right to privacy is not applicable to an organization (AT&T). It is possible that, if such a right was

actually granted to legal persons, it would be used as a tool to reduce access to their documents, files and decision-making, thus reducing monitoring and accountability options.

In view of the above, we recommend that Article 3.1ter be deleted.

c. The new approach on the 'processing of sensitive data' (Article 6) is dynamic, but clear instructions ought to be provided to data controllers

The Council appears to be undertaking a bold approach to the processing of sensitive personal data in Article 6 of the draft Convention, whereby the 'sensitivity' of person-al information is dynamically established each time, depending on their nature or ac-tual use or risks presented by the particular processing. Although this approach indeed appears to resolve the long-identified problem of using plain personal data in a sensi-tive data processing context (for instance, inferring religion or ethnicity on the basis of a person's name or residence), it also means in practice that data controllers will require guidance as to when they should contact their supervisory authority and ask for a permit to process data kept in their files. Under the current data protection re-gime, data controllers know which of their datasets are sensitive and which are not, through the simple action of comparing their actual contents with the list of categories of sensitive information provided in data protection legislation. A dynamic definition of sensitive processing, depending each time on the particular processing details, would in practice mean that data controllers would not know when to treat their data as sensitive (and could also plead negligence, if they do undertake such processing unlawfully).

d. Transparency of processing (Article 7bis) at the time of collection of personal information

The draft Convention includes the right to information to data subjects in its Article 7bis. However the issue of when exactly ought data controllers inform data subjects on the collection of their data is left to be regulated in the Explanatory Report. **We recommend that information is provided to data subjects at the time of collec-tion**, and also believe that this is an important enough point to be **included in the main body of the Convention and not in its Explanatory Memorandum**.

We remain at your disposal for whichever further information you may require,

Yours sincerely,
Vagelis Papakonstantinou

Attorney at Law

INSURANCE EUROPE

Position Paper Insurance Europe contribution to the 3rd Council of Europe consultation on the Modernisation of Convention 108

Our reference: SMC-DAT-12-042 Date: 25 May 2012 Referring to: T-PD-BUR(2012)01Rev2_en Related documents: SMC-DAT-12-015 Contact person: Lamprini Gyftokosta, Policy Advisor Life & Health Insurance E-mail: gyftokosta@insuranceeurope.eu Pages: 5 Transparency Register ID no.: 33213703459-54

Insurance Europe aisbl rue Montoyer 51, B-1000 Brussels Tel: +32 2 547 5811 • Fax: +32 2 547 5819 www.insuranceeurope.eu

Introductory remarks

Insurance Europe (formerly CEA), the European insurance and reinsurance federation, welcomes the opportunity to contribute to this third consultation on the Modernisation of Convention 108, launched by the Council of Europe (CoE).
Insurance Europe participated in the second CoE consultation this year and would like to comment on the following points of the new proposals on the Modernisation of the Convention 108 (27 April 2012) which were already addressed during the meeting between the CoE and the private sector stakeholders on 2 May.
Having in mind the on-going process of revision of the EC Directive 95/45 on data protection, Insurance Europe wishes to reiterate its expectation that there will be no significant discrepancies between the future modernised CoE Convention 108 and the future EU regulation and directive.
Insurance Europe also wishes to reiterate its request to be provided with the draft of the Explanatory Report as this would facilitate our understanding of the provisions contained in the proposal.

Article 3 – Scope

Par.1ter "Any Party may decide to apply this Convention to information on legal persons".

Insurance Europe strongly opposes the possibility for any Party to decide applying the Convention to information on legal persons. They do not have fundamental rights as natural persons and are protected by other legal means.

Article 5 – Legitimacy of data processing and quality of data

 *Par.1 "Data processing shall be **proportionate** in relation to the **legitimate purpose** pursued and reflect a fair balance between the public or private interests, rights and freedoms at stake".*

Insurance Europe highlights that where the processing of personal data is based on consent, contract or specific public authorisations, there is no need for an additional examination of proportionality.

It should also be noted that the existing EU legislation requires the insurance industry to collect certain data in order to carry out its business. For example the EU anti-money laundering (AML) legislation requires insurers to verify the accuracy of certain personal data, eg the identity of the policyholder/beneficiary, the origin or the destination of the funds. It is vital that the interpretation and application of these new provisions do not hinder the fulfilment of existing regulatory requirements imposed on insurers.

Moreover, as part of anti-fraud measures, insurers need to collect, process and share certain relevant data. We support measures that ensure appropriate consumer protection, however the legislative framework must recognise the need for organisations to share information for such purposes.

Detecting fraud protects honest consumers. It is important that efforts to combat fraud (which are in the overriding interests of individual consumers and of society as a whole) are supported and explicitly recognised in the development and application of the law rather than being restricted.
Furthermore, as part of the underwriting and claims settlement process, insurance companies need comprehensive information and data about the risk to be insured. Being able to access, process and store relevant personal data is central to insurers' ability to provide consumers with appropriate products at fair prices.

Par.2a) "Each Party shall provide that data processing can be carried out only if the data subject has ***freely given his/her explicit specific and informed consent".***

Insurance Europe believes the requirements of and for consent must be relevant and suitable to the purposes for which the consent is obtained. Requirements should not act as a barrier to consumers accessing insurance or prevent the insurer from delivering necessary services to the consumer.

Based on insurers experience across member states, Insurance Europe understands that consumers do not encounter problems with the current rules on consent. Therefore, Insurance Europe opposes any changes to the existing rules of consent.

Insurance Europe is concerned about the introduction of ***data subject's right to withdraw consent*** in the Explanatory Report. This would hinder the execution of the contract, lead to an unauthorised cancellation and conflict with other pieces of legislation.

For instance, based on insurance contract law, the insurer and the consumer fix the terms of the contract at the beginning of their contractual relationship. Some contracts permit cancellation during a policy period under specific circumstances. Such circumstances should be distinguished from the consumer's right to withdraw consent which would lead to an unauthorised cancellation of the contract.

Moreover, insurers need to store data for regulatory, legal or anti-fraud purposes. For example, based on Directive 2005/60/EC on anti-money laundering and terrorist financing (AML), insurers should store data for ***at least 5 years after*** the end of the business relationship with specified natural or legal persons. According to the abovementioned legislation, insurance companies are also obliged to maintain data and information for a certain period, because of the public authorities' controls.

Therefore, Insurance Europe suggests the ***data subject's right to withdraw consent*** should be appropriately designed to take into account situations where data must be retained and in some instances processed for regulatory, anti-fraud or legal purposes.

 *Par.3c) "adequate, relevant, not excessive **and limited to the strict minimum** in relation to the purpose for which they are processed".*

Insurance Europe encourages redrafting the paragraph so that it reads ***"minimum necessary***".

Article 6 – Processing of sensitive data
Par.1 "The processing of certain categories of personal data shall be prohibited, whether such data are sensitive:

a) By their nature, namely genetic data, data related to health or sexual life, data related to criminal offences or convictions, or security measures;

b) By the use made of them, namely biometric data, data whose processing reveals racial origin, political opinions [or trade union membership], religious or other beliefs, or:

c) Where their processing presents a serious risk to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

If the Consultative Committee includes genetic or biometric data in the "special category of data", then it must be ensured that characteristics such as gender and age, which are visible to everyone, and also family history, are not part of them. Otherwise the definition will be incompatible with the provisions of other pieces of national or European legislation.
Insurance Europe would like to underline that the Explanatory Report includes a broad definition of *genetic data*, ie *characteristics acquired during early prenatal development* which are not in fact caused by genetic conditions but by external conditions such as lack of oxygen to the foetus during pregnancy. Moreover, Insurance Europe is concerned that the reference to "*hereditary characteristics"* is too vague and wide.

The prohibition to process data referring to hereditary characteristic could have detrimental consequences for insurers, as they will be no longer able to use them as risk factors for their underwriting. Inability to use data effectively would result in consumer detriment in the form of higher prices and/or under insurance. This could also lead to the withdrawal of some products from the market, resulting in less consumer choice.
Insurance Europe suggests that the *biometric data* definition should be restricted to biometric detection data such as retina scans and finger prints. Data on physical attributes should not be included.

Article 7 – Data Security
2. "*Each Party shall provide that the controller shall notify, without delay, at least the supervisory authorities within the meaning of Article 12 bis of this Convention of any violation of data security which may seriously interfere with the right to the fundamental rights and freedoms of the data subject.*

*The Explanatory Report will specify that the controller should be encouraged to also **notify where necessary** the data subjects.*

Insurance Europe welcomes the CoE approach on data security and agrees that the supervisory authorities and data subjects should be notified only about breaches that pose a significant risk of harming data subjects.

If the data subject is notified for every breach of data, ie those posing significant risk and others that do not, important notifications might be overlooked. This could lead to consumers' apathy, making them more vulnerable in circumstances where there is a serious data privacy breach.
For greater clarity of the concept of "*seriously interfere"*, the obligation to report security breaches to the authority should only concern breaches related to sensitive data and data with significant effects for the data subject concerned. Insurance Europe suggests that the explanatory note of the Report of the 24th Meeting of the Bureau of the Consultative Committee (28-30 June 2011) should be added to the Explanatory note on the Convention, to confirm this.
Insurance Europe would like to underline insurance companies and other financial institutions have to notify the data breaches only to supervisory Authorities within the meaning of Article 12 bis of the Convention and to sectorial supervisory Authorities.

Article 8 – Rights of the data subject

a) Any person shall be entitled on request not to be subject to a decision significantly affecting him/her or producing legal effects relating to him/her, based solely on the grounds of an automatic processing of data without having the right to express his/her views.

d) To obtain knowledge of the reasoning underlying in the data processing, the results of which are applied to him/her;

Explanatory Report: this right can, in accordance with Article 9, be limited where this is necessary in a democratic society, in order to protect "legally protected secrets".

Insurance Europe believes that the data subject should have the right to access data. It is worth noting that following an access request, insurers have an obligation to review the information to ensure the redaction of any non-disclosable data, or data relating to third parties or legal professional privilege. Therefore, Insurance Europe asks for any legislation to be flexible enough to reflect the need of insurers to redact certain information.

Careful consideration must be given not to introduce any requirement to disclose information while such disclosure could be in breach of competition law. In the case of the insurance industry, the legislative framework must not make it possible for insurers to reveal their underwriting criteria or processes to other insurers as this would be in breach of competition law. For these reasons, Insurance Europe would propose the ***deletion of Article 8d***.

GSMA

Many thanks for inviting the GSMA to the recent meeting on the revision of Convention 108. I am pleased to send the following high-level comments on the draft reviewed at the meeting.

We feel that:

- The proposals should recognise and consider the European Commission's review of Directive 95/46EC and emerging proposals, so that businesses and individuals have legal certainty and consistency with regards to data protection obligations and rights.

- The convention should remain a principle-based instrument that is concise and technologically neutral. [E.g extending the definition of personal data to geo-location may lead to further ambiguities over what is caught in what context and set false expectations of privacy).

- The definition of data controller is dependent on the decision making power of one or joint parties which covers the purposes, conditions and means of processing. This will introduce significant challenges in today's mobile interconnected and interdependent online world that involved multiparty data flows.

- We call for further clarification with regards to the proposed change that consent must be explicit, where required. It is important that any requirement for explicit consent is dependent on the risks posed by specific processing and that the legitimate interests of data controllers are not unnecessarily restricted where risk is not present or deemed acceptable.

- The creation and definition of sensitive categories of data are still overly wide and need to be narrowed to reflect that 'sensitivity' is increasingly shaped by context – social, technical.

- Security breach notification obligations must be consistent with emerging EU best practice and not create unnecessary, burdensome and ineffective rules that generate unwarranted anxiety, security notice fatigue etc..

- Clarify Article 8b and proposals to introduce an obligation to ensure privacy by design – as written this would include obliging hardware and software companies. We believe any such measures must also be reflected in the proposed EC data protection regulation.

- Derogations for the purposes of protecting the interests of state security, public security and the economic and financial interests of the state are too broad. They need to be framed by an obligation on member states to establish a legal framework that sets out a citizen’s expectations to privacy and which framework defines the powers of the state with regards to access to personal data of individuals and which also regulates the investigatory powers of law enforcement etc.

– Proposals for sanctions and remedies must not create forum shopping – e.g. that data controllers can choose to establish themselves in a state with weak enforcement and sanction powers. We are concerned to ensure that different regimes are not created under Convention 108, the proposed GDPR and the e-privacy directive.

Pat Walshe

ORACLE

Comments of Joseph Alhadeff to the COE April revision draft:

1. Premable p. 8. The removal of the reference to information flows eliminates the parallelism with OECD and EU Directive/Regulation. The focus of COE on human rights explains the need to limit balancing between fundamental rights, but global information flows are an important societal objective and should be declared so in the recitals. It is through those information flows that rights of association, expression, choice and prosperity/pursuit of happiness are often exercised. Thus a preamble reference to the importance of information flows to today's digital economy and information society and when applying rules to protect data and preserve privacy to assure that they are not unduly burdensome to information flows and seek to avoid unintended consequences that constrain innovation should be reinserted.
2. Article 2 definitions – personal data – a question arises from the term to individualise one person amongst others – does this require persistence of that ability. At any point in time one might be able to identify two dynamically generate IP addresses as different but it does little to idividualise a person beyond that point in time. This should be expressed more as a factor which, depending upon circumstances could tend to identify a person – it reads more like an objective or test unto itself without the need to be informed by context and application.
3. Definitions – data controller. One must be careful in how "means" are discussed. Processors may make numerous determinations related to means in order to execute the instruction (purposes) of the controller. That is why controllers need processors. Thus means in the controller space are a subset of an exercise of control and should not be drafted where decisions on means alone implicate control.
4. Definitions – recipient. In definitions recipient is defined in between the two major roles (controller/processor) – explanatory memo should differentiate the nature of the term.
5. Article 5 para 1 explanatory memo reference. "in relation to the benefits expected from the controller " is too subjective and impossible to quantify as it may change with every user. Better to address expectations reasonably created by the statements/promises/services offered by the controller.
6. Article 5 Para 2. There is great confusion interpreting what the meaning is of 2a and 2b when taken together, both here and in other parts of the document, as there is no clarity where legitimate interest overrides consent. We await the resolution of this critical issue in the explanatory memo.
7. Article 6 para 2. It is unclear what "appropriate safeguards" might be? Is a general privacy regulation an appropriate safeguard? Could that be a code of conduct or research protocol? Health data must be processed to treat patients; there is no option not to process. We should better define appropriate safeguards and better consider the real work applications and constraints of this section.
8. Article 7 para 1. There is a danger in placing obligations directly on the processor. While processors may well need to demonstrate the security they provide to satisfy legal

requirements of a controller related to types of information or for some level of certification or accreditation, independent obligations in relation to the security of specific information may require the processor to have greater knowledge of the information – defeating the principle of data minimization and further may lead the processor to question the way in which the controller secures the information leading to legal uncertainty. The requirement of processors providing sufficient security is not at issue, but it should be accomplished by a requirement derivative from the controller's obligation (controller should require processor to….) as opposed to independent from it.

9. Article 7 para 2. Question arises as to how "seriously interfere with the right to the protection of personal data" will be interpreted. Is this the same as reasonably likely to cause harm or adverse effect? Greater clarity, practicability and consistency with global approaches would be welcome.
10. Article 7 Bis para 1- we should consider the granularity and the utility of the documentation. In some cases categories of recipients may be sufficient – some of this information may vary across types of elements, but users may only be interested in the range of retention periods (between 3 and six months; not more than 12 months…) there may also need to be a qualifier added such as: 'as appropriate to the circumstances to inform the user".
11. Article 8 para a- how does this right to comment apply to identification of spam, virus and fraud origination in security and antivirus tools? Does this right to comment apply to credit reports? What about issues of national health and pandemic? Explanatory memo clarification of scope of application might be useful.
12. Article 8 para b – clarification of scope and application of "legitimate" reasons would be welcome.
13. Article 8 para c – "all available information" seems overbroad. Perhaps "information relevant to". May also wish to have the ability to scope the request to address issues of scale, reasonableness, cost and potential for abuse.
14. Article 8 pars d – while I do not believe that this is intended in the draft – a clarification that logic applies to the general thinking or rational not algorithms or proprietary methods would be welcome.
15. Article 8 para e. this section is part of the rights of the data subject thus it is unclear to who the need for a remedy is addressed. If to the singing party that is appropriate, language would be less appropriate for companies.
16. Article 8 Bis. Continued issue of independent obligations on the processor for the reasons outlined above.
17. Article 12 overall – "supervisory authority" does not seem to include concepts of accountability agents (re APEC, Safe Harbor etc); they have a growing role. It may be useful to express the need to explore methods of cooperation; though maybe less robust than with other supervisory authorities…
18. Article 12 overall and 12Bis 7 et seq.. The EU Draft regulation has recognized the benefits of more harmonized application of rules and decisions, perhaps some greater emphasis on that topic could be introduced.
19. Article 12 para 3. Preference for "may" as duty to inform can be overbroad as considered. Also where established and recognized means (contracts, BCRs, codes,

research protocols) are used duty to inform should at a minimum be streamlined if not eliminated. May also be addressed by creating a exception in Article 8 para 4.

20. Article 12 Bis para 4 – while independence should not be compromised that para could be read to preclude the ability to consult technical and other experts which should be encouraged. Could also be addressed in para 5 as an example of beneficial external consultative resources.

Page 198: [1] Comment [DP7] **Davide Parrilli** **6/6/2012 12:39:00 PM**

This provision seems not completely in line with data protection rationale, but more with access rights and rights to be informed in specific sectors, such as banking, public administration etc. The scope of the provision goes beyond the purposes of data protection legislation since it imposes obligations to companies that are not (only) strictly related to data processing. More specifically, the provision aims at prohibiting the practice of automated decisions without the power of the data subject to express his view. This is more a subject matter for consumers' protection legislation.

Furthermore, this provision risks not to be very effective since there are no sure effects as regards the views expressed by the data subject, more precisely there is no guarantee that the views expressed by the data subjects will be taken into due account by the recipient.

Finally, this provision (and the obligations thereof) hinders many business sector, for instance the insurance sector, where it is current practice that the consumer/client interacts with an IT system to obtain an offer or to enter into an agreement based on several criteria, included e.g. the accidents caused by the user etc.

Therefore we suggest deleting this provision. In the view of EPA, the aim of this provision represents the typical case of tension between "privacy by theory" (to be avoided) vs. "privacy by practice" (to be preferred).