COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 15 November 2011 T-PD-BUR(2011) 27_en

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

(T-PD)

Modernisation of Convention 108: proposals

DG I - Human Rights and Rule of Law

INTRODUCTION

This document sets out the approach and objectives of the Convention's modernisation.

Its content is based on the results of the public consultation process carried out in Spring 2011, the discussions held at the T-PD bureau meetings this year as well as contributions from the scientific experts and observers associated to this modernisation work.

The present document aims at giving a first written translation of the outcomes of those discussions for consideration by the T-PD Plenary at its forthcoming meeting (29 November - 2 December 2011) and in view of their finalisation at the following 2012 Plenary meeting, for subsequent submission to the Committee of Ministers.

EXTRACTS FROM THE REPORT OF THE 24th MEETING OF THE BUREAU OF THE CONSULTATIVE COMMITTEE (28-30 June)

General orientations

It is proposed to:

- maintain the Convention's provisions with more detailed sectoral texts by way of recommendations of the Committee of Ministers of the Council of Europe;

- ensure for consistency and compatibility with the legal framework of the European Union;

- maintain technologically neutral provisions;

- reaffirm the Convention's potential as a universal standard and its open character.

Preamble

An essential balance to strike involves the freedom of expression, which takes on another dimension with the Internet: the various fundamental rights have to be reconciled (to be examined in the explanatory report, with a possible reference to the principle of the public's right of access to administrative documents).

Article 1 – Object and purpose

It is proposed to uphold the right to data protection and to refer to the concept of "jurisdiction" instead of "territory".

Article 2 – Definitions

"Personal data": this definition should not be changed (NB: crucial to ensure consistency with EU) but the explanatory report should be reviewed in order to extend the items relating to this definition (see in particular Recommendation (2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling : 'An individual is not considered "identifiable" if identification requires unreasonable time or effort').

"Automated data file": consensus to abandon this notion which is outdated and is only relevant in relation to non-automated files. Should the scope be extended to manual processing, a reference to “structured files” (see Directive 95/46 EU) may be necessary.

"Automatic processing": this definition, exhaustive at present, should be revised in order to be made open-ended and should in any case incorporate the step of the collection of data (to include, for instance, the consultation and the destruction of data). Reference could furthermore be made in the explanatory report to ‘making available’ under ‘dissemination’.

“Controller of the file”: notion to be revised and possibly to be replaced by “controller: (consistency with EU) with a reference to the various levels of responsibility.

New definitions, such as ‘processor’, ‘service provider’, ‘recipient’ or “manufacturer of technical equipment” should be incorporated if specific obligations are foreseen for them.

Article 3 – Scope

It clearly emerges from the replies to the consultation that it is advisable to preserve the comprehensive approach of the Convention, which applies to the public and private sectors alike.

It appears necessary to include an exception for household data processing. It will have to be examined how this shall relate to social networks, blogs etc. which require specific attention.

In respect of manual processing, even if rare, it could be covered in particular to counter the risk of bypassing the conventional obligations.

With regard to legal persons: Parties to the Convention should keep the possibility to extend the scope of the Convention to their data.

Article 4 – Duties of the Parties

The quality of the ‘necessary measures’ should be scrutinised *a priori* by the Committee in the framework of transborder flows provisions, in order to ensure that the conditions for the free flow of data are met.

Article 5 – Quality of data

This article should be revised in order to expressly incorporate the principle of proportionality and where necessary to highlight the grounds for a processing to be legitimate.

It was decided to deal with the introduction of new principles (“accountability”, “privacy by design” i.e. the obligation to apply the principles of protection as from the designing stage) at a later stage.

Article 6 – Special categories of data

The present definition should be retained while adding new illustrations to the explanatory report underlining the functional aspect (data may become sensitive according to the purpose of the processing considered); this aspect could also be inserted in the article itself.

Article 7 – Data security

Security should apply to data as well as to its processing. The obligation to report security breaches should be introduced, but it is underlined that such an obligation should not become trivial (it should only concern breaches related to a certain volume of data). The conditions of this notification require examination (to whom, individuals, data protection authorities, how and when).

Article 8 – Additional safeguards for the data subject

Access to the origin of the data and to the underlying logic of the processing as well as the right of opposition should be introduced.

Certain hesitations were expressed with regard to the explicit inclusion of a "right to oblivion". It is proposed to elaborate further the explanatory report in order to underline the link between the relevant provisions of the Convention (article 5.e – length of time of data storage, and article 8.c – right of rectification or erasure of data).

Article 9 – Exceptions and restrictions

For the time being, no amendments are proposed to this article.

Article 10 – Sanctions and remedies

It is decided not to set out in further details this article and to entrust to the Parties the provision of sanctions and available remedies. With regard to the powers of the supervisory authorities, it is underlined that they should be reinforced (ex officio action, intervention before the courts for existing proceedings).

Article 12 – Transborder data flows

This key question will have to be further examined "recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples" (preamble Convention 108). The co-existence of provisions on transborder data flows in both the Convention and article 2 of the additional Protocol (transfer of data to States which are not Parties) will have to be revised and the current provisions need to be examined with a view to agreeing on a new approach which would amend both the Convention and the Protocol.

Articles 13, 14, 15, 16, 17 Mutual assistance

To be discussed.

Articles 18, 19 and 20 – Consultative Committee

A strengthening of the Consultative Committee's functions and powers should be foreseen. Whether and to what extent this requires additional provisions will be discussed.

TEXT OF THE CONVENTION – PROPOSALS

CURRENT TEXT OF THE CONVENTION	PROPOSALS
Preamble	**Preamble**
The member States of the Council of Europe, signatory hereto,	unchanged
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 desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, **including the right to control one's own data**, taking account of the increasing flow across frontiers of personal data undergoing ~~automatic~~ processing;
Reaffirming at the same time their commitment to freedom of information regardless of frontiers;	Reaffirming at the same time their commitment to freedom of **expression, including freedom of information**, regardless of frontiers;
Recognising that it is necessary to reconcile the Fundamental values of the respect for privacy and the free flow of information between peoples,	unchanged
	Recognising that it is necessary to reconcile the right to data protection, and particularly respect for privacy, with freedom of expression and information;
	Considering that this convention permits account to be taken, in the implementation of the rules laid down therein, of the principle of the right of access to public documents;
	Explanatory report : 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	The purpose of this convention is to secure within the **jurisdiction** of each Party for every individual, whatever his nationality or residence, **the right to data protection, namely** respect

particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").	for his rights and fundamental freedoms, and in particular his right to privacy, with regard to ~~automatic~~ processing of personal data relating to him.
Article 2 – Definitions	**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 a person who would be informed of it, namely in the case of a publication.*
b "automated data file" means any set of data undergoing automatic processing;	b "file" means any set of personal data structured and managed in such a way that it is possible to search for data by data subject;
c "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" refers to operations carried out on personal data in whole or in part by automated means, and in particular the collection, storage, preservation, alteration, retrieval, communication, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data; *In the explanatory report, mention that the communication also covers disclosure and dissemination.*
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 having 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 reasons justifying 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, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;
	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;

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 The Parties undertake to apply this convention to data processing and files in the public and private sectors. 1bis This convention will not apply to data processing carried out by a natural person for the exercise of activities which are exclusively personal or domestic, unless the data are made accessible to persons which do not belong to a personal or domestic sphere. *In the explanatory report, specify what is meant by exercise of exclusively personal or domestic activities, and made accessible to persons outside the personal or domestic sphere.*
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:	unchanged
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;	unchanged
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.	3 Any State which has extended the scope of this convention by a declaration provided for in sub-paragraph 2.b above may give notice in the said declaration that the extension shall apply only to certain categories of files, a list of which will be deposited.
4 Any Party which has excluded certain categories of automated personal data files by a	Delete

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.	
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.	4 Likewise, a Party which has not made **the extension provided for in sub-paragraph 2b** above may not claim the application of this convention on **this point** with respect to a Party which has made **such an extension**.
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.	unchanged
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.	unchanged
2 These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.	unchanged
Article 5 – Quality of data	**Article 5 – Quality of data and legitimacy of data processing**
Personal data undergoing automatic processing shall be:	**1** Personal data undergoing ~~automatic~~ processing shall be:
a obtained and processed fairly and lawfully;	a ~~obtained and~~ processed fairly and lawfully;
b stored for specified and legitimate purposes and not used in a way incompatible with those purposes;	b **processed** for specified and legitimate purposes and not used in a way incompatible with those purposes; *In the explanatory report, give examples of compatible purposes, being supported by the existence of other legal guaranties (e.g. in the field of statistical or scientific research, or for one's own marketing)*

c adequate, relevant and not excessive in relation to the purposes for which they are stored;	c adequate, relevant and not excessive in relation to the purposes for which they are **processed**;
d accurate and, where necessary, kept up to date;	unchanged
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 the data subjects for no longer than is required for the purpose for which those data are **processed**;
	2 The data processing must be proportional to the interests, rights and freedoms of the data subjects and the means and methods used must be as little intrusive as possible for those interests, rights and freedoms.
	3 Each Party shall provide that data processing may not be carried out unless: *a.* it is provided for under domestic law where there is an overriding legitimate interest; (*in the explanatory report, explain overriding legitimate interest, particularly with reference to the examples given in Article of Directive 95/46/EC)* b. the data subject has given his consent in a specific, free and informed manner.
Article 6 – Special categories of data	**Article 6 – Special categories of 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.	**Personal data pertaining to the private sphere of the individual or data the use of which may be susceptible to lead to illegal or arbitrary discrimination, or which may cause a serious risk for the data subject should be considered as sensitive. In particular,** 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 **genetic and biometric data, as well as** to personal data relating to criminal convictions. *Explanatory report : a serious risk notably refers to violations of dignity or physical integrity.*
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	**1** Appropriate security measures shall be taken [~~…~~] against accidental or unauthorised destruction, or ~~accidental~~ loss of personal data, as well as against unauthorised access,

well as against unauthorised access, alteration or dissemination.	alteration or dissemination **of personal data processed**. *Explanatory report : refer to secrecies legally protected.*
	2 Each Party shall provide that the controller shall notify the supervisory authorities within the meaning of Article 12ter of this convention of any security violations which may seriously interfere with the right to data protection.
	3 Each Party shall provide that the controller must choose a processor providing sufficient guarantees in light of the security of processed data and that it is incumbent on the controller to ensure that the processor will respect the security measures. *Explanatory report : security obligations must lie on all actors and this should notably be spelled out contractually.*
	Article 7bis – Transparency of processing
	Each Party shall provide that every controller must ensure transparency of data processing and in particular provide the data subjects with information concerning at least his identity, the purposes of the processing carried out by him, the duration of data preservation, the recipients of the personal data and the means of exercising the rights set forth in Article 8, as well as any other information necessary to ensure fair data processing. *Explanatory report : specify when the information should be given and that 'any other information necessary' notably includes transfers to other countries.*
Article 8 – Additional safeguards for the data subject	**Article 8 – Additional safeguards for the data subject**
Any person shall be enabled:	Any person shall be enabled:
a to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;	a to establish the existence of data **processing**, its main purposes, ~~as well as~~ the identity and habitual residence or principal place of business of the controller **as well as the recipients or categories of recipients of the data**;
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;	b to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are being **processed**, communication to him of such data in an intelligible form and **all available information on the origin of the data**;

	b' to obtain knowledge of the logic involved in the processing. *(to be considered in the context of provisions on automated decisions)*
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 f below
	d to object at any time and for overriding legitimate reasons to processing of personal data concerning him.
	e not to be subject to a decision based solely on the grounds of an automated processing of data without having the right to expose his views.
	f to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure, **or an objection**, as referred to in paragraphs b, b', c, d and e of this article is not complied with.
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 provisions of **Articles 5, 6, 7bis and 8** of this convention shall be allowed except within the limits defined in this article.
2 Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:	2 Derogation from the provisions of **Articles 5, 6, 7bis and 8** of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:
a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;	a protecting State security, public safety, the monetary interests of the State or the **prevention** and suppression of criminal offences; *In the explanatory report, specify by means of examples the scope of the provision, particularly as regards freedom of expression and information, the media, secrecy of communication and business or commercial secrecy and other secrecies legally protected.*
b protecting the data subject or the rights and freedoms of others.	unchanged
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	3 Restrictions on the exercise of the rights specified in Article 8, paragraphs b, **b'**, c , d and **e**, may be provided by law with respect to **data**

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.	**processing** used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy 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.	unchanged
	Article 10bis – Additional measures for the controller
	Each Party shall provide that the controller is responsible for ensuring respect for the right to data protection from the initial design stage of the processing operations and for taking all necessary measures – including when delegating to a controller - to observe the domestic legal provisions giving effect to the principles and obligations of this convention, in particular : a. to carry out a data protection risk analysis before processing personal data. b. to design data processing operations in such a way as to minimise the risk of interference with the right to data protection, and c. to establish internal mechanisms to verify and demonstrate to the data subjects and to the supervisory authorities provided for in Article 12ter of this convention the conformity of the data processing for which he is responsible in relation to the applicable law. *In the explanatory report, specify that one of the possible measures consists of the designation of a 'data protection officer' entrusted with the means necessary to the fulfillment of its mission and designation of which the supervisory authority has been informed of. It can be internal or external to the controller.*
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 – Transborder flows to a recipient within the jurisdiction of a Party to the Convention**

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 provide for the communication or disclosure of personal data, for the purpose of processing, to a recipient within the jurisdiction of one or of several other Parties.
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 A Party shall not, for the sole purpose of the protection of **personal data**, prohibit or subject to special authorisation **the communication or disclosure of personal data referred to in paragraph 1.**
3 Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:	3 Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2 **where**:
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;	a. the communication or disclosure referred to in paragraph 1 is made for a recipient which is not subject to the jurisdiction of a Party to the Convention, through the intermediary of a recipient subject to the jurisdiction of a Party, in order to avoid such communication or disclosure resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph;
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.	b. insofar as its legislation includes specific regulations for certain data processing, because of their nature, except where the regulations of the other Party or Parties referred to in paragraph 1 provide an equivalent protection;
	c. the Party from which the personal data are communicated or disclosed is able to invoke non-compliance with the principles and obligations of this convention by the Party of the recipient of the data.
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 12bis – Transborder flows of personal data to a recipient not subject to the jurisdiction of a Party to the Convention**
	1 Each Party shall provide for the communication and disclosure of personal data, to a recipient which is not subject to the jurisdiction of a Party to the Convention, only if the national law applicable to that recipient ensures, in light of the present Convention, an adequate level of protection of the data subjects.
2 By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow	2 Each Party shall be entitled to derogate from paragraph 1, where the applicable

for the transfer of personal data :	domestic law prescribes that data can be communicated or disclosed if :
a if domestic law provides for it because of :	a. specific interests of the data subject impose it in the concerned case;
– specific interests of the data subject, or	b. legitimate interests, especially important public interests, prevail in the concerned case; *Explanatory report : refer to natural disasters*
– legitimate prevailing interests, especially important public interests, or	3 By way of derogation from paragraph 1, each Party may also allow for the communication and disclosure of personal data, for the purpose of processing, to a recipient which is not subject to the jurisdiction of a Party to the Convention, where, in light of the present Convention, the adequate level of protection is ensured by measures adopted and implemented by the person communicating or disclosing personal data, and by the recipient, in so far as :
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.	a. those persons can demonstrate, to a competent supervisory authority within the meaning of Article 12ter of this convention, prior to the communication or disclosure of data, the quality and effectiveness of the measures taken, notably by means of contractual clauses, binding internal rules or similar measures, and
	b. the national authorities can only have access to data according to rules safeguarding, in light of the present Convention, an adequate protection of the data subjects, and
	c. the competent supervisory authority within the meaning of Article 12ter of this convention, be informed in a reasonable period of time and prior to the measures referred to in litera a, and that it can suspend, forbid or subject to condition the communication or disclosure of data.
	Article 12ter Supervisory authorities (Art. 1 Additional 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 **of this convention**. *Explanatory report : the powers of intervention should notably concern processing which present particular risks for the fundamental rights and freedoms*
	b Each supervisory authority shall hear claims lodged by any person concerning the protection of his rights and fundamental freedoms with regard to the processing of personal data within its competence.
	3 The supervisory authorities shall exercise their functions in complete independence. **For this purpose, they shall have sufficient staff and financial resources and the necessary facilities. They shall not be subject to any external instructions.**
	4 Decisions of the supervisory authorities which give rise to complaints may be appealed against through the courts.
	5 In accordance with the provisions of Chapter IV, and without prejudice to the provisions of Article 13 of the convention, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information, **by co-ordinating their investigations or interventions or by carrying out joint actions.**
Chapter IV – Mutual assistance	**Chapter IV – Mutual assistance**
Article 13 – Co-operation between Parties	**Article 13 – Co-operation between Parties**
1 The Parties agree to render each other mutual assistance in order to implement this convention.	unchanged
2 For that purpose:	unchanged
a each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe;	a each Party shall designate one or more **supervisory** authorities within the meaning of Article 12ter 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 authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.	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.
3 An authority designated by a Party shall at the request of an authority designated by another Party:	A **supervisory** authority designated by a Party shall at the request of a **supervisory** authority designated by another Party:

a furnish information on its law and administrative practice in the field of data protection;	unchanged
b take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.	b take, in conformity with its domestic law and for the sole purpose of protection of **personal data**, all appropriate measures for furnishing factual information relating to specific ~~automatic~~ processing carried out in its territory, with the exception however of the personal data being processed, **unless such data be indispensable for the cooperation or consent has been expressly given by the data subject prior to the processing.**
Article 14 – Assistance to data subjects resident abroad	**Article 14 – Assistance to data subjects resident abroad**
1 Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.	unchanged
2 When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.	When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the **supervisory authority within the meaning of Article 12ter** designated by that Party.
3 The request for assistance shall contain all the necessary particulars, relating inter alia to:	unchanged
a the name, address and any other relevant particulars identifying the person making the request;	unchanged
b the automated personal data file to which the request pertains, or its controller;	b the data **processing** to which the request pertains, or **its controller**;
c the purpose of the request.	
Article 15 – Safeguards concerning assistance rendered by designated authorities.	**Article 15 – Safeguards concerning assistance rendered by designated authorities**
1 An 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.	unchanged
2 Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.	unchanged
3 In no case may a designated authority be allowed to make under Article 14, paragraph 2, a	unchanged

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	**Article 16 – Refusal of requests for assistance**
A designated 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:	unchanged
a the request is not compatible with the powers in the field of data protection of the authorities responsible for replying;	unchanged
b the request does not comply with the provisions of this convention;	unchanged
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.	unchanged
Article 17 – Costs and procedures of assistance	**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 authority making the request for assistance.	unchanged
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.	unchanged
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.	unchanged
Chapter V – Consultative Committee.	**Chapter V – Consultative 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
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	unchanged

the right to be represented on the committee by an observer.	
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.	unchanged
Article 19 – Functions of the committee	**Article 19 – Functions of the committee**
The Consultative Committee:	unchanged
a may make proposals with a view to facilitating or improving the application of the convention;	unchanged
b may make proposals for amendment of this convention in accordance with Article 21;	unchanged
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;	unchanged
d may, at the request of a Party, express an opinion on any question concerning the application of this convention.	unchanged
	e prior to any new accession to the Convention, shall formulate its opinion on the opportunity for the Committee of Ministers to invite the concerned State or international organisation to accede to this Convention.
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.	unchanged
2 A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.	unchanged
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
4 Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.	unchanged
Chapter VI – Amendments	**Chapter VI – Amendments**
Article 21 – Amendments.	**Article 21 – Amendments**
1 Amendments to this convention may be proposed by a Party, the Committee of Ministers	unchanged

of the Council of Europe or the Consultative Committee.	
2 Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the 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.	unchanged
3 Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.	unchanged
4 The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.	unchanged
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.	unchanged
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.	unchanged
Chapter VII – Final clauses	**Chapter VII – Final clauses**
Article 22 – Entry into force	**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.	unchanged
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.	unchanged
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.	unchanged
Article 23 – Accession by non-member States	**Article 23 – Accession by non-member States or international organisations**

1 After the entry into force of this convention, the Committee of Ministers of the Council of Europe may 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.	After the entry into force of this convention, the Committee of Ministers of the Council of Europe may, **in light of the opinion formulated by the Consultative Committee according to Article 19.1**, invite any State not a member of the Council of Europe or **any international organisation** 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 unanimous **vote** of the representatives of the Contracting States entitled to sit on the Committee **of Ministers**. **This decision shall be taken after having obtained the unanimous agreement of the Parties to the Convention.**
2 In respect of any acceding State, 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.	unchanged
Article 24 – Territorial clause	**Article 24 – Territorial clause**
1 Any State 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.	unchanged
2 Any State 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.	unchanged
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.	unchanged
Article 25 – Reservations	**Article 25 – Reservations**
No reservation may be made in respect of the provisions of this convention.	unchanged
Article 26 – Denunciation	**Article 26 – Denunciation**
1 Any Party may at any time denounce this convention by means of a notification addressed	unchanged

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.	unchanged
Article 27 – Notifications	**Article 27 – Notifications**
The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of:	unchanged
a any signature;	unchanged
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;	unchanged
d any other act, notification or communication relating to this Convention.	unchanged

INTERNATIONAL CHAMBER OF COMMERCE (ICC)

PROPOSAL TO THE COUNCIL OF EUROPE FOR REVISION OF CONVENTION 108 PROVISIONS ON TRANSBORDER DATA FLOWS

INTRODUCTION

The proposal, which has been drafted by Christopher Kuner and reviewed by Richard Thomas and members of the ICC Task Force on Privacy and the Protection of Personal Data, reflects the following general considerations:

- It was decided to draft a completely new provision, rather than simply combining the two existing ones. Any provision dealing with transborder data flows should be "future proof" and take into consideration the borderless nature of electronic communications and the evolving nature of the Internet.
- The proposal is drafted at a high level, and contains general principles only. Particular effort was made to keep the text clear and concise.
- The proposal may need to be supplemented by provisions in other sections of the Convention dealing with concepts that are not further specified here (e.g., the principle of accountability).
- Among the sources considered in the drafting were the EU Data Protection Directive 95/46; jurisprudence of the European Court of Human Rights and the European Court of Justice; papers of the Article 29 Working Party; and the Madrid Resolution.
- Explanatory notes are inserted in italics following the provisions to which they refer.

PROPOSED TEXT

Transborder flows of personal data

1. Each Party shall provide that personal data relating to individuals who are located in its territory shall receive an adequate level of protection based on the protections stipulated in this Convention when the data are processed outside its territory, provided that the processing results from an activity directed to such individuals or that otherwise manifests a sufficient connection to such Party.

Note:
- The text avoids using the term "data transfer". It also does not refer to the "data controller", so that it applies as well to data processors. While it is difficult in practice to localize the place of data processing, the reference to the processing of data "outside the territory" of a Party was included to make it clear that the provision is intended to apply solely to transborder data flows.
- The notion of an "adequate level of protection" is tied to the protections of Convention 108, and is further specified in sections 2 and 3 below. The term "protections stipulated in this Convention" is taken from current Article 11.
- The provision does not distinguish between data flows to CoE states and to non-CoE states. While this distinction was understandable when the Convention and the Additional Protocol were originally adopted, maintaining it would make the provision overly complex, and it is no longer tenable given the rapid development of the Internet.
- The second part of the sentence (beginning "provided that the processing results…") specifies that the Convention's provisions on transborder data flows do not apply when a data processing activity outside the territory of a Party does not manifest a sufficient connection to a Party (such as

when an individual merely accesses a web site that is not directed to the individual or the Party in which the individual is located); this is consistent with the judgments of the ECJ in the Lindqvist and Pammer/Alpenhof cases, and with leading decisions of national courts dealing with Internet jurisdiction (e.g., the judgment of the German Federal Supreme Court of 29 March 2011, VI ZR 111/10). Questions such as whether a data processing activity is directed to individuals located in the territory of a Party, or is sufficiently connected to such Party, would be determined under the applicable national law implementing the Convention.

2. An adequate level of protection based on the protections stipulated in this Convention under section 1 may be provided as follows:
    a. the State in which the organisation processing the personal data is located has been found under applicable domestic or international law to offer adequate protection based on the protections stipulated in this Convention; or
    b. the organisation or organisations processing the personal data have been found to offer such protection; or

Note: The above two provisions would cover situations where either the State in which the organisation is located, or the organisation processing the data, has been found to offer adequate protection. Adequacy could be determined nationally or internationally (such as via an EU adequacy decision).

    c. the organisation or organisations processing the personal data have implemented appropriate and effective measures for ensuring such protection (such as through the use of contractual clauses, legally-binding internal privacy rules, or other similar measures), and can demonstrate such measures, and their effectiveness, on request from the relevant supervisory authority.

Note: The above provision implements the concept of accountability, and recognises the use of mechanisms such as standard contractual clauses and BCRs. Provided that suitable and effective measures are in place, it is intended to cover situations where processing occurs within or across a single organisation or where the data is transferred to a third party. The reference to "organisation or organisations" in sections 2(b) and 2(c) allows for transfers to multiple entities that have separately or jointly implemented effective protections to cover the data processing.

3. By way of derogation from sections 1 and 2, adequate protection need not be provided in the following cases:
    a. the individual has given his consent unambiguously to the processing; or
    b. the processing is necessary for the performance of a contract between the individual and the organisation processing the data or the implementation of precontractual measures taken in response to the individual's request; or
    c. the processing is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organisation processing the data and a third party; or
    d. the processing is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
    e. the processing is necessary in order to protect the vital interests of the individual.
    f. *Note: The above section 3 reflects Article 26(1)(a)-(e) of the Directive*.

CURRENT TEXT

Convention 108 (1981):

Article 12 – Transborder flows of personal data and domestic law

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.
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.
3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
    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;
    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.

Additional Protocol to Convention 108 (2001):

Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention

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.

APPENDIX II

Memorandum on introducing the concept of jurisdiction into Article 1 of Convention 108
Jean-Philippe Moiny, Research Fellow, F.R.S.-FNRS (Belgian Scientific Research Foundation – CRIDS (IT Law Research Centre), University of Namur

Note

The purpose of the following discussion, whose conciseness necessarily involves some simplifications, is to offer the reader a few points of analysis as to the possible amendment of Article 1 of Council of Europe Convention 108. This memorandum does not aim at an exhaustive presentation of the question addressed, or at solutions to the issues raised. Considerable further research and exposition would be required for that purpose.

Relevant legal provisions

Article 1 ECHR: "The High Contracting Parties shall secure to everyone within their jurisdiction ["relevant de leur juridiction"] the rights and freedoms defined in Section I of this Convention"

Article 1 Convention 108 – Object and purpose: "The purpose of this convention is to secure in the territory of each Party ["sur le territoire de chaque Partie"] 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")."

Proposed amendment: "The purpose of this convention is to secure **to every individual within the jurisdiction of the Parties**, 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")."

Concept of jurisdiction and ECHR

In general. In English-language legal writings, the concept of "*jurisdiction*" is generally used for that of state competence. It is the power, assigned by international law to the state, to regulate and influence the conduct of individuals and to attach consequences to events. State competence springs from state (territorial) sovereignty which constitutes its foundation.

This general jurisdiction may be divided into two general classes of jurisdiction: "prescriptive jurisdiction" (or "compétences normatives") and "enforcement jurisdiction" (or "compétences d'exécution"). For example, law, regulations adopted by governments (royal orders in Belgium, decrees in France, etc.), judgments, etc., come under the state's prescriptive jurisdiction, while all procedures of enforcement, seizure, expulsion, arrest, finding of evidence, etc., are the upshot of the state's enforcement jurisdiction. It will be noted, however, that legal opinion in the matter makes distinctions and qualifications of other kinds which there is little need to examine in detail for present purposes.

Where state jurisdiction is founded in international law, it rests on several titles. At present, legal opinion unanimously accepts the titles of jurisdiction constituted by national territory (territorial jurisdiction) and nationality (personal jurisdiction). As to a state's territorial sovereignty, this has two features: completeness and exclusiveness. Briefly, the state may issue prescriptions on all subjects in respect of its territory, and is alone in holding that power in that place. In principle, state jurisdiction is territorial in its scope. Only exceptionally can it be recognised as having extraterritorial

scope. We can be infer from the well-known *Lotus* case, settled by the former Permanent Court of International Justice[1], that the state's prescriptive jurisdiction is not limited in territorial scope by public international law – which is disputed in legal theory – but its enforcement jurisdiction is strictly limited to its own territory – which is indisputable. In other words, a state would not infringe public international law if it enacted laws with an extraterritorial effect, but would infringe it by setting out to implement these enactments in foreign territory, through the exercise of its enforcement jurisdiction.

In short, there is room for extraterritorial regulations, even if the state's jurisdiction is essentially territorial by definition. State practice bears clear witness to this reality. Suffice it to mention American and European law of competition – American especially. The latter, whose "*jurisdiction*" is founded on the theory of effects, unarguably has extraterritorial effects, in exactly the same way as its European counterpart, whose applicability is of course founded on a different theory but likewise with extraterritorial effect.

It should be further noted that the two aforementioned titles of jurisdiction – territoriality and nationality – are construed extensively to allow national regulations to have extraterritorial effects[2]. In the sphere of data protection for example, Council of Europe Convention 108 and European Directive 95/46 ordain a legal control over transborder data flows which displays an extraterritorial effect[3]. Where piracy, war crimes, crimes against humanity and genocide, etc. are concerned, there is even question of universal jurisdiction.

Conflicts of jurisdiction. State jurisdictions, depending on their underlying title, are liable to come into conflict. These conflicts of jurisdiction are settled by legal co-operation in civil cases (or criminal, considering that the data protection rules potentially carry criminal sanctions) and consequently by the rules of private international law (or again criminal law). It is therefore of interest to give a succinct illustration of the eventuality, where data protection is concerned, of such conflicts of jurisdiction (in terms of public international law).

A first example relates to a controller of processing who, being established in the territory of a state A, uses means of processing (data centres for instance) in the territory of a state B – it is of little consequence whether or not these states are both parties to Convention 108. In such a situation, both states may at the very least invoke their prescriptive jurisdiction (compétence normative) founded, in public international law, on a territorial title (location of the controller of processing or location of the means of processing). State B, however, will not be able to exercise its enforcement jurisdiction (compétence d'exécution) in the territory of state A without the latter's

[1] P.C.I. J., Lotus case of 7 September 1927, judgment of 6 April 1955, *I.C.J. Reports*, series A, No. 10.

[2] Without going into detail, various titles to jurisdiction – principles – can be invoked, without regard to their possible overlap or to the legal disputes occasioned by them: subjective territorial principle, objective territorial principle, active or passive personal jurisdiction, universal jurisdiction or theory of effects. State jurisdiction is usually founded on elements of territorial and/or national attachment. These may be sidelined when universal jurisdiction or the principle of protection are relevant, or else the legal subject-matter at issue (piracy, war crimes, currency counterfeiting, etc.) serves as the basis of jurisdiction.

[3] The extraterritorial effect is as follows. If a third state wants the controllers of processing established its territory to be able to receive data from the Council of Europe states without the need to invoke the rules of exemption in respect of data flows, it is bound to adopt regulations which are at the very least adequate. An example is the establishment, in the United States, of the Safe Harbor Principles. If an American enterprise wishes to receive, for purposes of processing, data from the European Union, it must accept the Safe Harbor Principles. In such cases, European regulations have effects in the territory of third states: either enterprises choose of their own volition to abide by certain data protection requirements, or a state ensures, also voluntarily, that its regulations are adequate by comparison with the European standard of protection.

consent. Where relevant it might be possible in theory to contemplate exercising this enforcement jurisdiction in respect of property owned by the controller of processing in the territory of state B.

The second example concerns a rather more complex situation of transborder data flows towards third countries. A subsidiary Y of an enterprise X established in a state A – not one of the parties to Convention 108 – under the law of that state, pursues its data processing activity in a state B – also not one of the parties to Convention 108. The personal data which it processes are transmitted to it from a state C, which is party to Convention 108. The police of state A serve enterprise X with a demand, founded in the law of state A, to obtain the data processed by subsidiary Y which, as a subsidiary, does not possess its own legal personality distinct from that of enterprise X. The example is not unrealistic[4]. In the present instance, state C can avail itself of its territorial jurisdiction (prescriptive and enforcing) to forbid anyone present in its territory to transmit personal data to third states. This jurisdiction more specifically concerns any person (legal or natural) with the intention of transmitting data to subsidiary Y. State B can exercise its territorial jurisdiction (prescriptive and enforcing) over the processing activities of subsidiary Y. State A too exercises its jurisdiction (prescriptive and enforcing) over enterprise X on two accounts: territory, since it is established – incorporated – there, and also its nationality. Moreover, it is principally this claim of nationality which would enable it, perhaps not without contention, to get at subsidiary Y. If subsidiary Y was in fact a subsidiary of enterprise X, hence endowed with legal personality, the control exercised by enterprise X over its daughter company could also be invoked by state A in order to exercise its jurisdiction. However, this title of jurisdiction would be all the more arguable. Finally, the state of which the person concerned is a national could invoke a passive personal jurisdiction should the case arise.

In the field of human rights (ECHR). The European Court of Human Rights has examined on three occasions the applicability of Article 1 of the ECHR (cited above) with reference to the concept of jurisdiction. In its well-known *Bankovic* decision[5], it looks back on the emergence of this concept in the ECHR:

> "3. The drafting history of Article 1 of the Convention
>
> 19. The text prepared by the Committee of the Consultative Assembly of the Council of Europe on legal and administrative questions provided, in what became Article 1 of the Convention, that the "member States shall undertake to ensure to all persons residing within their territories the rights...". The Expert Intergovernmental Committee, which considered the Consultative Assembly's draft, decided to replace the reference to "all persons residing within their territories" with a reference to persons "within their jurisdiction". The reasons were noted in the following extract from the Collected Edition of the Travaux Préparatoires of the European Convention on Human Rights (Vol. III, p. 260):
>
> > "The Assembly draft had extended the benefits of the Convention to 'all persons residing within the territories of the signatory States'. It seemed to the Committee that the term 'residing' might be considered too restrictive. It was felt that there were good grounds for extending the benefits of the

[4] State A could be the United States. For example, under USC Title 50 – War and national defence, Chapter 36 – Foreign intelligence surveillance, Subchapter IV – Access to certain business records for foreign intelligence purposes, Sec. 1861 : "*(a) Application for order; conduct of investigation generally (1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution".*

[5] Eur. Court H.R., dec. Bankovic and others v. Belgium and others, 12 December 2001, Application No. 52207/99 (Grand Chamber).

> Convention to all persons in the territories of the signatory States, even those who could not be considered as residing there in the legal sense of the word. The Committee therefore replaced the term 'residing' by the words 'within their jurisdiction' which are also contained in Article 2 of the Draft Covenant of the United Nations Commission."
>
> 20. The next relevant comment prior to the adoption of Article 1 of the Convention, made by the Belgian representative on 25 August 1950 during the plenary sitting of the Consultative Assembly, was to the effect that "henceforth the right of protection by our States, by virtue of a formal clause of the Convention, may be exercised with full force, and without any differentiation or distinction, in favour of individuals of whatever nationality, who on the territory of any one of our States, may have had reason to complain that [their] rights have been violated".
>
> 21. The travaux préparatoires go on to note that the wording of Article 1 including "within their jurisdiction", did not give rise to any further discussion and the text as it was (and is now) was adopted by the Consultative Assembly on 25 August 1950 without further amendment (the above-cited Collected Edition (Vol. VI, p. 132)."

Two points at the very least arise from these considerations. Firstly, the use of the expression "within their jurisdiction" was intended to avoid undue restrictiveness as to the scope of the Convention. Secondly, the drafters of the text definitely had in mind the principle of territoriality, in so far as the persons "in the territories" of the Contracting Parties were to be covered.

It is clear that this element of territoriality does not compel states parties to obstruct any extraterritorial effect of the ECHR. They are obviously free to extend the geographical scope of their rules for the implementation of the Convention, in accordance with public international law, if that is their intention. On the contrary, this element could even require states to recognise the ECHR as having some degree of extraterritoriality. In that connection, the writer would be inclined to consider that the states parties to the ECHR should apply it – and enforce it – to the extent allowed by the jurisdiction which they are entitled to exercise regarding a given situation. In other words, it would be a matter of their having to apply the ECHR in the exercise of all their powers – prescriptive and executive – that is, in the exercise of their territorial or extraterritorial *jurisdiction*.

However, this view is sometimes corroborated and sometimes refuted by the Court's case-law; it is impossible to enlarge on these considerations here. The case-law of the Court and the former Commission are hard to systematise in that regard, and so a few decisions are cited to illustrate the possible applications of Article 1 ECHR, and a degree of extraterritoriality which the ECHR *must* have pursuant to this case-law. Thus, schematically and *non-exhaustively*:

- a state party to the ECHR is bound to apply the Convention when a suspect is handed over to its agents abroad[6], when it exercises effective overall and military control (occupation) over part of a third state's territory [7] and when its diplomatic and consular agents discharge their functions abroad[8];
- with regard to extradition, a state party to the ECHR cannot extradite an individual if he or she incurs genuine risks of receiving, in the requesting state, treatment contrary to Article 3 ECHR or is liable to undergo blatant denial of justice there (violation of Article 6 ECHR)[9];

[6] Eur. Comm. H.R., dec. Freda v. Italy, 7 October 1980, Application No. 8916/80; Eur. Comm. H.R., dec. Reinette v. France, 2 October 1989, Application No. 14009/88; Eur. Comm. H.R., dec. Illich Sanchez Ramirez v. France, 24 June 1996, Application No. 28780/95.

[7] Eur. Comm. H.R., dec. Cyprus v. Turkey, 11 October 1973, Applications Nos. 6780/74 and 6950/75 (plenary); Eur. Comm. H.R., dec. Cyprus v. Turkey, 10 July 1978, Application No. 8007/77 (plenary); Eur. Court H.R.., judgment Loizidou v. Turkey (preliminary objections), 23 March 1995, Application No. 15318/89 (Grand Chamber); Eur. Court H.R.., judgment Issa and others v. Turkey, 16 November 2004, Application No. 31821/96 (second section).

[8] Eur. Comm. H.R., dec. F.J.R. v. S. v. Federal Republic of Germany, 25 September 1965, Application No. 1611/62; Eur. Comm. H.R., dec. M. v. Denmark, 14 October 1992, Application No. 17392/90.

[9] See case of *Soering*, Eur. Court H.R.., Soering v. United Kingdom judgment, 7 July 1989, Application No. 14038/88 (plenary), and the subsequent case-law founded on it.

this precedent will surely be approximated to the provisions governing transborder data flows;

- with regard to judicial co-operation in the civil and criminal spheres, the Court has also acknowledged that the states parties to the ECHR owed certain obligations of a kind that would give the Convention a territorial effect [10].

Amendment of Convention 108

Reasons. There seem to be two main reasons in favour of amending Article 1 of Convention 108 as suggested. Firstly, it would be a matter of aligning the geographical scope of Convention 108 to that of the ECHR and more specifically of Article 8 ECHR which constitutes one of its essential foundations, although Convention 108 does not have the sole object of protecting privacy. Moreover, amendment referring to the concept of jurisdiction, rather than territory, seems likelier to stand the test of time and continual technological developments. The writer considers the new wording more amenable to legal interpretation and more adaptable.

Implications. The change of text is thus not without implications. Today of course, the effect of an amendment along the suggested lines would be limited, perhaps even non-existent in terms of national law. Provisions such as Article 1 of the ECHR and of Convention 108 do not result in any fundamental contestation of the private international law of the states parties, which at all events is destined to be applied. Even, for example, a provision like Article 22 of the Council of Europe Convention on Cybercrime, which goes further into the intricacies of international criminal law[11] – that is the rules which, in domestic law, define the state's jurisdiction in criminal matters –

[10] Eur. Court H.R., judgment in the case of Drozd and Janousek v. France and Spain, 26 June 1992, Application No. 12747/87 (plenary); Eur. Court H.R.., judgment in the case of Pellegrini v. Italy, 20 July 2001, Application No. 30882/96 (second section).

[11] Section 3 – Jurisdiction – Article 22 – Jurisdiction: "1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution"

does not upset domestic law regarding jurisdiction. Moreover, it is rather that the Convention on Cybercrime encapsulates the principles of application in a large number of states.

It can be borne in mind that, where data protection is concerned and in the context of the ECHR, questions of conflicts of jurisdiction (see above) (and the underlying questions of private international law or international criminal law) remain the preserve of the state.

In this matter however, should the European Court of Human Rights some day happen to have before it a question bearing on Article 1 of the ECHR as to the limit *ratione loci* which it places on the ECHR, and a dispute arising from Cloud Computing or Internet, the inferences made could be more readily transposed to the context of Convention 108 owing to the textual similarity which would result from the proposed amendment.

Transborder flows. It is important finally to note that the introduction of the concept of jurisdiction into Article 1 of Convention 108 does not make it ineffectual or immaterial to employ the concept of territory in laying down rules to govern transborder flows of data between parties to the Convention[12]. Here, it is a matter of determining the place of destination of the data. This is the place where the level of protection with which data must circulate freely needs to be known – in this instance the level of a state party.

In relation to a movement of data, the criterion of territory, also used implicitly by European Directive 95/46 ("to a third country"), has a certain simplicity; the recipient of the data need merely be located in order to ascertain whether movement is permitted. The applicable rules constitute a safety-net whose purpose is to prevent data, once transferred abroad, from being processed regardless of data protection requirements.

The Additional Protocol to Convention 108, on the other hand, uses the concept of jurisdiction in respect of transborder data flows towards a third state[13]. That would be a further reason to support the proposed wording of Article 1 of Convention 108[14]. For the sake of coherence and uniformity, one could then think about removing the reference to territory from Article 12 of the Convention and specify instead the recipient "subject to the jurisdiction of a State Party".

[12] Article 12 – Transborder flows of personal data and domestic law: "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.
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*." (author's emphasis).

[13] Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention "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" (author's emphasis).

[14] The wording used by the Additional Protocol nevertheless most certainly designates the recipient subject to the *territorial* jurisdiction of a state which is not party, or even more precisely, to location on the territory of a state which is not party. Indeed, *transborder* flows are concerned.