COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 20 November 2012/ 20 Novembre 2012 T-PD(2012)11 Mos
Addendum

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

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES A CARACTÈRE PERSONNEL [STE n°108]

(T-PD)

Modernisation of Convention 108: compilation of comments received

Modernisation de la convention 108 : compilation des commentaires reçus

DG I - Human Rights and Rule of Law

INDEX

I – T-PD Members/ Membres du T-PD

Bosnia Herzegovina/ Bosnie Herzégovine ……..... 3

Czech Republic/ République Tchèque……. 4

Ireland/ Irlande……. 10

Portugal……. 14

Spain/ Espagne…… 15

Sweden/ Suède…….. 20

Switzerland/ Suisse…….. 26

BOSNIA HERZEGOVINA/ BOSNIE HERZEGOVINE

Following your request to send you our proposals with changes and amendments (changes and amendments only and not general comments) to the document T-PD (2012)04Rev2, i.e., Modernization of the Convention 108, we hereby inform you that **we do not have concrete proposals with changes and amendments.**

We would like to thank you on giving us the opportunity to give our proposals with changes and amendments and we are particularly pleased to have participated at the meetings dealing with the development of the Final document on the modernization of the Convention 108.

After detailed analysis of the Final document on the modernization of the Convention108, we would like to encourage all the efforts concerning the development of this document and we are fully aware of its significance and contribution to protection of personal data.

CZECH REPUBLIC/ REPUBLIQUE TCHEQUE

Preamble

(3)
Considering ….. ~~„use of such data“~~ „processing of such data“.

CZ believes that it is better to speak in defined terms („processing“ - the clear definitiv exists)

Article 2(c) should read:

„ data processing means any structured operation or set of operations…“

CZ prefer to stress the character of automated operation, not only non-automated

Article 2(d) should read:

“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 core features of data processing.

CZ believes that the definition of “controller” is too broad in that it refers to “decision-making” power without any limits. In practice, decisions on some modalities, such as the conditions of data processing may well be taken by the processor rather than the controller. CZ would welcome if the “decision-making” power of the controller was described in a way that would not make any processor who makes some minor or technical decision or a decision on the security of processing, into a controller.

Article 2(e) – it is not clear why the definition of recipient is necessary.

Article 3(1bis) should read:

Article 3(1bis) should read:

This Convention shall not apply to data processing carried out by a natural person for the exercise of purely personal or household activities. If **personal data of someone else/another person** processed in the course of such activities are intentionally made accessible to persons outside the personal sphere, only Articles XY apply.

CZ believes that making personal data accessible to a relatively wide and uncertainly delimited group of people is a recognizable feature of modern times. While such data processing may exceed the “personal sphere” of controller, the application of whole set of rules may in many cases be unrealistic. CZ advocates focus on bare minimum of duties in such cases.

Article 4(1) and (2) should be deleted, **Article 4(3)** should be moved to Article 19(h) and worded appropriately.

Paragraphs (1) and (2) are obsolete in light of contemporary treaty practice. It goes without saying that each Party should implement its obligations under the Convention prior to its ratification or accession. Treaties must be applied by Parties in good faith for the whole time they are binding on the Parties.

Article 5(2)(a) should read:

a. the data subject has freely given his/her provable, specific and informed consent, or

CZ believes that describing consent as provable strikes the right balance between the duties of the controller to prove the legality of processing on the one hand and flexibility in various forms of obtaining consent on the other.

Article 5(2)(d) should read:

d. processing is necessary for the purposes of legitimate interest,

CZ believes that also legitimate interests not provided for explicitly by the law should be accommodated. The necessary balance to this provision is a right of the data subject to object such processing, as provided for by Article 8(b). Incidentally, if this change is not implemented, the data subject would not, in fact, have anything that could be objected under Article 8(b).

Article 5(2)(e) should be added:

e. the personal data have been lawfully published.

CZ believes that lawfully published data may be processed as well. Deletion of the word "obtained" in Article 5(3)(a) does not help very much as any collection or taking over of data falls under the definition of "processing" in Article 2(c). Also, this important principle should not be conveyed by such rather non-obvious change.

Article 6

CZ believes that this provision should focus on risks of processing rather than on sensitive data. That is not the case now. Article 6(2) means that e.g. a list of persons baptized on a certain day that is available as a hard copy on a church notice board is always presenting serious risks described in Article 6(1).

CZ supports ongoing harmonization with rules being drafted at the EU level.

Article 7(1) should read:

Each Party shall provide that the controller, and, where applicable the processor, takes the appropriate security measures against accidental or unauthorised modification or loss ~~or~~

~~destruction~~ of personal data, as well as against unauthorised access or ~~dissemination or~~ disclosure of such data

CZ believes that if Convention is to remain general in its wording, it should refrain from cumulating very close or identical terms.

Article 7(2) should read:

Each Party shall provide that the controller shall notify, without unreasonable delay, at least the supervisory authorities within the meaning of Article 12 bis of this Convention of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

CZ believes that immediate notifications to supervisory authorities constitute an unreasonable and in many cases also ineffective requirement. The controller will primarily have to make substantial effort to identify the extent of the security breach and to prevent further breaches. The supervisory authority would usually not be in a position to offer substantial assistance. Therefore reporting duties may be postponed. In fact, reporting to data subjects may be more urgent if that is necessary to prevent damage.

Article 7bis(1) should read:

Each Party shall provide that every controller may ensure the transparency of data processing in informing data subjects 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 categories of recipients of the personal data, and the means of exercising the rights set out in Article 8~~, as well as any other information necessary to ensure fair and lawful data processing~~.

CZ believes that such information duty should be limited to requests of data subjects pursuant to Article 8(1)(c). Of course, if the controller has an on-line presence, it may fulfill such duty easily in a general manner as well. However, off-line controllers should not have their administrative burdens increased unreasonably.

CZ believes that the last part of the sentence is too vague and thus cannot be made obligatory to controllers.

Article 8(b) should read:

to object at any time to the processing of personal data based on Article 5(2)(d) concerning him/her unless ~~such a processing is compulsory by virtue of the law or~~ the controller can justify of prevailing legitimate grounds ;

CZ believes that this provision should be consistent with other provisions on legality and legitimacy of processing, such as Article 5(2)(d), as proposed above.

Article 8bis(4) should read:

Each Party can decide to derogate in full or in part to the provisions of the previous paragraphs, according to the size of the controller, or where applicable the processor, the nature of the

processing, the volume of data processed and the risks for the interests, rights and fundamental freedoms of the data subjects.

CZ believes that it should be possible to adapt obligations of controllers also with regard to the nature of the processing, in particular where the processing is a well-established or routine activity that is regulated by other rules.

Article 9(1) should read:

No exception to ~~the principles expressed in~~ this Chapter shall be allowed, except to the provisions of Articles 5.3, 6, 7.2, 7bis and 8 and 12 when such derogation is provided for by ~~an accessible and foreseeable~~ law and constitutes a necessary measure in a democratic society for:

While this Chapter is still called "Basic Principles of Data Protection", its content clearly indicates that it contains much more than "basic principles", for example "additional obligations" in Article 8a.

CZ believes that inaccessible or unforeseeable laws cannot, as a matter of principle, derogate rights of persons in a democratic society. This Convention should be considered a set of obligations rather than a textbook on the rule of law. Therefore such utterances are unnecessary.

CZ believes that a reference to Article 12 must be added to Article 9(1), as exceptions from Article 12 are needed for the general purposes of Article 9(1)(a). Article 9(2) could be deleted, or, if considered necessary, Article 9(1)(b) and 9(2) may be joined together.

Article 9(1)(b) should read:

the protection of the data subject or the rights and freedoms of others, notably freedom of expression and information

CZ believes that freedom of information is a right necessary in a democratic society and that interests of transparency must in many cases be weighed against the interests of privacy.

Article 10 should read:

Each Party undertakes to establish appropriate judicial and/or non-judicial sanctions and remedies for violations of domestic law giving effect to the provisions of this Convention.

CZ believes that it is not necessary to provide for both judicial and non-judicial sanctions for the same violation.

Article 12(1) should be considered also in relation to data kept in cloud. Situations may arise e.g. that data are kept in country A, disclosure is made by a processor in country B to a recipient in country C.

CZ supposed that it must be kept in mind in context of harmonization with EU regulatory document

Article 12(5) should read:

Notwithstanding the provisions of paragraphs 2, 3 and 4, each Party may provide that the disclosure or making available of data may take place, if in a particular case:
a) the data subject has given his/her specific, free and explicit [/unambiguous] 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 reflects the change to Article 9(1). CZ believes that the purposes listed in Article 9(1)(a) have general validity and legitimacy and that it is up to the legislator to provide for systemic solutions in such cases. Case-by-case decision-making is not a proper model of regulation in such systemic issues.

Article 18(3) should read:

The Convention Committee may, by a decision taken by a majority of two-thirds of the representatives of the Parties entitled to vote, invite any non-member State of the Council of Europe which is not a Party to the Convention to appoint an observer to be representing it at its meetings.

CZ believes that it should be clear that the observers under 18(2) are not further restricted by Article 18(3) and that it should be clear which States can be thus invited. This will help to avoid unhelpful misunderstandings in future relations with third countries.

Article 19(h) should read:

may review the implementation of this Convention by the Parties in accordance with the provisions of Article 4.3 and decide upon recommendations addressed to the Parties ~~measures to take where a Party is not complying with its engagements~~;

CZ believes that the Convention Committee should direct its own work. It must have the power to address recommendations to both the Party evaluated and other Parties. Recommendations being not legally binding, this enables the Convention Committee to avoid the level of formalism that would be necessarily associated with adopting some "measures" for the enforcement of a Party's perceived failure to comply with its obligations. In fact, such measures would need to be provided for within the Convention and the procedure for adopting such measures would need to be clearly set. CZ does not believe that such mechanism would represent a significant added value.

Article 20(4) should read:

~~After each of its meetings, t~~The Convention Committee shall submit regularly to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the Convention.

CZ believes that e.g. yearly reports are sufficient. Submitting a report after every meeting may in some instances present too large a burden on other activities the Committee should focus on.

Article 21(7) should be deleted.

In many instances, such as before the elections, the two-year period may not be sufficient for the national parliaments to decide on the obligations that would or would not be binding on a particular Party. Standard models for amending the Convention are fully sufficient and conform to democratic procedures of the Parties.

IRELAND/ IRLANDE

Preamble

Recital 3
Replace 'own' with 'personal'**.**

Recital 4
Ireland suggests that 'Reminding' should be replaced by 'Recalling'.

Article 1
It is suggested that this article should be amended as follows:

- add 'their' before 'personal data';
- add 'when undergoing processing' after 'personal data'
- delete ',with regard … personal data'.

Article 2
Paragraph c
It is suggested that 'any criteria which allows to search' be replaced with 'criteria which facilitates the retrieval of'.

Paragraph e
The word 'service' in the definition of 'recipient' should be replaced by 'agency' in order to ensure consistency with other definitions in this Article.

Article 3
Paragraph 1bis
Ireland favours the deletion of the text in square brackets.

Article 4
Paragraphs 1 and 2
Ireland is concerned that paragraphs 1 and 2 will create difficulties for EU member States when the Proposal for a General Data Protection Regulation, which will have direct effect, is adopted. We would therefore suggest that 'in their domestic law' should be deleted from paragraph 1.

Paragraph 3
Ireland is concerned that the process of evaluation and observation has the potential to create conflict with implementation of the proposed EU Regulation.

Article 5
Paragraph 2
Point a
The inclusion of 'explicit' will depend on what is included in the EU Regulation.

Point b
It is suggested that the following text be added to the end of point b:
' .. prior to entering into such a contract, or'
Point d
It is suggested that 'provided by domestic law' should be replaced by 'necessary'..

Paragraph 3
Point c
It is suggested that 'not excessive' should be deleted as this is covered by 'minimum necessary'.

Article 6
The definition of sensitive data needs to be in line with the definition in the EU Regulation.

Article 7
Paragraph 2
It is suggested that 'undue' should be inserted before 'delay'.

Article 7bis
Paragraph 1
It is suggested that this requirement should not apply where the data subject already has the information.

Article 8
Article 8 will have to be in line with the EU Regulation.

Paragraph b
It is suggested that 'a processing …. to legitimate grounds be replaced' with the following test: 'processing is authorised or required by law or is necessary for the purposes of the overriding legitimate interests of the controller.'

Article 8bis
We have a general reservation on this Article. We would question how States parties can legislate to give effect to this Article.

Article 9
Paragraph 1
It is suggested that 'an accessible and foreseeable' should be delete.

It is suggested that point a be amended by
- replacing 'suppression' with 'detection or investigation'; and
- adding 'or apprehension or prosecution of offenders' after 'offences'.

Paragraph 2
It is suggested that the following amendments be made to paragraph 2:
- replace 'admitted' with 'be permitted'; and
- insert 'purpose of' before 'freedom of expression'.

Paragraph 3
It is suggested that the following amendments be made to paragraph 3:
- insert 'for' after 'provided'; and
- delete 'obviously'.

Article 12
Paragraph 1
It is understood that this paragraph is intended to cover information put on the internet on the basis that a controller who puts information on the internet accepts that there is a potential for a

cross border flow of the information. We think that this article is only feasible where data are actively transmitted. We would question how this article would affect personal data put on social media websites e.g. Facebook?

It is also suggested that 'stored' should be added to end of paragraph.

Paragraph 2
It is suggested that 'can not be' should be replaced by 'are not'.

Paragraph 4
We are not sure that 'ad hoc' is the correct term here. We would also suggest the deletion of ', the latter having to be binding' and its replacement with 'binding' in the appropriate part of the sentence.

Paragraph 6
The meaning of this paragraph is unclear.

Article 12bis
Paragraph 1
It is suggested that 'in its domestic law' should be deleted. See comments on Article 4.

Paragraph 2
It is suggested that the following changes should be made to paragraph 2:

- point a: insert 'shall' before 'have'
- point b: insert 'shall' before 'perform' and replace 'competences' with 'functions';
- point c: the text needs to be clarified;
- point d: insert 'shall' before 'have'; and
- point e: replace 'are' with 'shall be'.

In addition it is suggested that the order in which functions are set out should be changed by moving point e to the beginning of the paragraph.

Paragraph 3
It is suggested that the following changes should be made to paragraph 3:

- replace 'can be seized' with 'shall have the power to investigate claims lodged';
- delete 'data' before 'processing'; and
- retain 'of personal data'.

Paragraph 4
It is suggested that paragraph 4 should be amended as follows:

- replace 'perform their duties and exercise their powers in complete independence' with 'be independent in the performance of their duties and exercise of their powers'; and
- delete 'they shall neither seek nor accept instructions from anyone'.

Paragraph 5
It is suggested that 'mission' should be replaced by 'functions'.

Paragraph 7
Point a: This text needs to be clarified.

Point c: It is suggested that 'in' before 'data protection' should be replaced by 'relating to'.

Article 15
It is suggested that following changes should be made to paragraph 2

- replace ‘persons belonging to’ with ‘members and staff’; and
- insert ‘persons’ before ‘acting’.
-

Article 16
Replace ‘Articles’ with ‘Article’.

Article 19
Paragraphs d and g
We have doubts about the advisability of paragraphs d and g since they could lead to conflicts with implementation of the EU Regulation.

Paragraph h
It is suggested that ‘complying with its engagements’ should be replaced by ‘in compliance with the Convention’.

Article 20
Paragraph 5
It is suggested that the following amendments should be made to paragraph 5:

- replace ‘of’ after ‘procedures’ with ‘for’;
- replace ‘of’ before ‘examination’ with ‘for’; and
- replace ‘the present’ with ‘this’.

PORTUGAL

Article 3 – Scope

Par. 1bis

We deem indispensable to keep the text now inside square brackets.

The reason is because, within the framework of this article, it is our interpretation that we consider in-line with the notion of personal and household processing within the present text of the Convention, notion that we would like to keep because still valid despite technological progresses, that:

1 - A personal activity is one who affects only the person in question not involving any other person at least outside the household;

2 - A household activity, for data processing purposes, is one that takes place inside a residence, be it the one of the concerned data subject or the one of other person, provide the processing of data from the concerned data subject is made and the personal data being processed is intended only for use by the concerned data subject and the persons who are considered to share his household.

Therefore, for us, any processing of personal data, either intended or accidental, namely through the use of social networks or any other means, outside this scope, must be treated under the general rules.

Article 9 Exceptions and restrictions

Par. 1

We propose to amend the draft in order to say “provided for by law and constitutes a…), therefore deleting “by an accessible and foreseeable”.

Further comments, objections or suggestions may be presented if deemed necessary.

SPAIN/ ESPAGNE

Article 2. Definitions

It is necessary to unify the criteria regarding who could be considered controller, recipient or processor, referring all of these concepts to "the natural or legal person, public authority, agency, service or any other body".

In the current draft the definition of recipient refers to "service" but not to "agency", that is mentioned however in the definitions of controller and processor. In our opinion a "Service" (as a part of a public administration agency or department) could have been empowered by the internal legislation to have the power of decision with respect to the data processing or could be appointed by a controller to process data on its behalf. On the other hand there are numerous provisions that designate a public agency as possible recipient of personal data. Therefore, it is considered that the reference to the three entities provided will better fit with the actual situation of data processing.

Article 3: Scope

We propose to add at the end of paragraph 1 the following: "(…) therefore protecting the right to personal data protection of any person covered by that jurisdiction".

We are fully aware of the debate in the Plenary and the Bureau in order to replace the term "territory" by "jurisdiction" and fully understand the concerns of several delegates of keeping the former term. However some clarification should be given by the text in order to prevent the existence of any legal loophole and to provide a high level of protection. The criterion of protecting the persons covered by the jurisdiction of each Party could in this case become essential in order to prevent those situations, as the reference to territorial criteria could generate difficulties, as it has happened in the past.

If this proposal is not fully accepted, some specification of the criteria preventing the existence of legal loopholes should be provided and at least detailed in the Explanatory Memorandum.

Article 5: Legitimacy of data processing and quality of data

We propose to delete the brackets in paragraph 2 a)

As it was pointed out during the previous debates, we consider this reference redundant with the rest of requirements provided for consent by article 5.2 of the draft and could create several interpretative gaps, since it could not become clear if the use of this term means that an "expressed" acceptance of the data processing will always be required for processing personal data on the basis of the data subject's consent. However in a large number of cases the authorisation for processing personal data may be given by an active conduct of the data subject that is not entirely referred to the processing of personal data but to the circumstances surrounding that processing (for instance, the acceptance of general terms or conditions of a contract or entering specific information required to following surfing on the Internet).

In our opinion it is much more important that in those cases data subject consent could always be considered not only explicit but "unambiguous", which means that the data subject is fully

aware of the processing of personal data, its purpose and its consequences and still accept the processing of the personal data on the basis of a positive action that could not be strictly considered as an "explicit" consent.

If this proposal is not accepted it will anyway be necessary to clarify in the Explanatory memorandum the scope of the term "explicit consent" in the way aforementioned, in order to prevent those gaps.

Article 6. Processing of sensitive data

We propose the following text:

> *"1. Data processing of personal data revealing racial origin, political opinions, trade-union membership, religious or other beliefs they reveal, as well as genetic data, data concerning health or sexual life, data concerning criminal offences, convictions and related security measures or data processed for identifying the biometric information they contain, shall only be allowed where the applicable law provides additional appropriate safeguards, complementing the safeguards of the present Convention*
>
> *2. Those measures should be meant to prevent the risk that the processing of those data may present to the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination."*

We are aware of the important step forward that the provisions currently included in the draft could represent in the assessment of the "sensibility" of the personal data processing, considering adequate to make a difference between personal sensitive data *per se* and personal data due to the way they are actually processed (as it was provided by the Madrid standards). However the draft text could create several conflicts with the applicable law of a large number of parties (EU Member States) that are subject to an approach based on the categories of personal data and not on the purposes of data processing.

In any case the content and spirit of the current draft is also provided by the proposed text, notably specifying the causes and risks for which additional safeguards are required.

Article 7 bis: Transparency of processing

We propose the following:

> *a) To complete the wording of paragraph 1 resulting as follows: "Each Party shall provide that every controller must ensure the transparency of data processing and in particular provide informing data subjects, unless they have been already informed, with information concerning at least (…)"*
>
> *b) To complete the wording of paragraph 2 in the following way: "When the data are not collected from the data subject the controller shall nonetheless not be required to provide such information where the processing is prescribed by law or this proves to be impossible or involves disproportionate efforts. In these cases the information may be replaced by alternative measures."*

The purpose of this provision is to adapt the text to the current provisions applicable in a large number of Parties, taking into account what is envisaged in articles 10 and 11 of the EU Directive.

Addition proposed to paragraph one takes into account the fact that the data subject does not need to be informed about the processing of personal data that has already been communicated to him or her. This is particularly important if referring to processing consisting in a disclosure of data to a recipient who is also going to process the information for its own purposes. In this case the previous information facilitated to the individual about the disclosure could cover entirely the information the recipient could be obliged to provide.

On the other hand the exemptions provided by paragraph 2 should only cover those cases where no direct relationship between the controller and the data subject occur. When the data are directly collected from the data subject it should be irrelevant the legitimacy for the processing and on the other hand it could be difficult to prove the existence of a disproportionate effort, since due to the direct relationship information could be provided during the transaction.

Moreover, when the exemption applies it might still possible to offer the information by thwe use of alternative, collective means, that would help the data subject be aware of the processing. Therefore additional measures for informing the data subject should be required in these cases.

Article 8 bis

We propose the following wording of paragraph 4:

> *4- Each Party <u>should modulate the application of</u> the provisions of the previous paragraphs, 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 current draft only foresees the possibility that Parties derogate in part or in full the accountability obligations set in article 8 bis. In our opinion the specific conditions of different categories of controllers or processor should always be taken into account by the Parties' domestic legislation.

Article 9: Exceptions and restrictions.

> *We propose to delete the term "accessible and foreseeable".*

These terms should be considered inherent to the law and the reference could result redundant and generate some future risks. If the meaning of this expression is to avoid situations on which exemptions could not be previously foreseen by the individual and a legitimate expectation of the data subject should be taken into account, we think this provision should be clarified by the Explanatory Memorandum, and not by the text itself.

Article 12. Transborder data flows.

We propose the following wording:

> *"1. The following provisions shall apply to the disclosure or making available of data to a recipient who is not subject to the jurisdiction of the Party whose legislation is applicable to the prior processing.*
>
> *2. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the disclosure or making available of data to a recipient who is subject to the jurisdiction of another Party to the Convention, unless the Party whose legislation is applicable to the prior processing is regulated by harmonised regional binding rules of protection shared by several States that require additional safeguards and the disclosure or making available of data can not be governed by measures foreseen in paragraph 4.b.*
>
> *3. When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to the Convention or in the case provided for by paragraph 2, the disclosure or making available of data can only occur where an appropriate level of personal data protection is guaranteed.*
>
> *4. An appropriate level of protection can be ensured by:*
>
> *(…)*
>
> *b) approved standardised legal measures or ad hoc binding legal measures capable of effective remedies and implemented by the person who discloses or makes data accessible and by the recipient.*
>
> *(…)*
>
> *6. Each party shall provide that the competent supervisory authority within the meaning of Article 12 bis of the Convention be informed of the modalities regulating the data flow, such as ad hoc measures foreseen in paragraph 3.b. It shall also provide that the supervisory authority be entitled to adopt standardized ad hoc binding measures provided for in paragraph 3 b) and to request that the person who discloses or makes data available, or the recipient, demonstrate (…)"*

The current wording of the draft seems to provide a specific rule regarding the scope of the Convention, since it considers applicable the law of the place were the data "are" or where they have been "originated from". These two criteria, apart from the fact that they could become incompatible to each other, do not take into account that in some cases the location or origin of personal data become irrelevant to determine the applicability of a Party's law due to other general or regional criteria. For instance, if a data controller chooses a cloud services provider and therefore decides that the data should be transferred from one provider to a new one, both outside the controller's territory, the data "are not" necessarily in the jurisdiction of the controller, but that jurisdiction will actually be applied to the new transfer of data. We can find the same problem in case of on-line collection of the data, since it could be understood that could be subject to the jurisdiction of the controller, the processor or the user according to the interpretation give to the expression "origin of data". For that reason, and respecting the spirit of the Text it is considered better to take into account the legislation is applicable to the processing prior to the transfer, although the wording could not cover all cases, but probably more than the current.

Moreover, regarding provision of paragraph 2 and taking into account the rationale of the proposal, we consider that the harmonised regional rules should be legally binding and not be found on other basis, such as soft law. We consider this reference is actually related to the effect of international treaties or at least to the existence of an international legal instrument. Besides, and due to logical reasons there should be a provision specifying those particular rules should be stricter that the Convention itself, providing or requiring additional safeguards for the transfer to take place.

Proposal in paragraph 3 only provides the applicability of the exemptions contained in this paragraph not only to third parties but also in the special case included in paragraph 2, since the opposite could lead to make the transfer to other Parties impossible if no adequate level of protection in provided for by domestic law.

Finally, regarding ad hoc measures we consider necessary in order to facilitate the transfers where adequate safeguards are provided to allow the national data protection supervisory authorities to adopt standardized measures that allow the different participants to more easily fulfil the requirements of the Convention. If it is considered not adequate to provide this rule in article 12.6 it could also be included in article 12 bis as a new competence of the data protection authorities, providing that the “may adopt standardized ad hoc binding measures provided for in paragraph 3 b) of article 12”.

SWEDEN/ SUEDE

Recitals

[5] 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 **[~~for Parties which recognise this principle~~ Move to explanatory memorandum]**;

Comment:
Sweden welcomes the T-PD Plenary's decision in June 2012 to introduce this recital which corresponds to recital 72 in Directive 95/46/EC. The recital reflects the importance of the right of access to documents demonstrated in inter alia Article 42 of the EU Charter of Fundamental Rights. It should be underlined that the recital expresses a *possibility and not an obligation* to take account of the right of access to documents at the national level. Hence, the text within brackets is not necessary and should therefore be moved to the explanatory memorandum.

Article 3 – Scope

1. Each Party undertakes to apply this Convention to data processing 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 intentionally made accessible to persons outside the personal sphere.~~]**

Comment:
As a consequence of the technological development everyday processing by natural persons have become widespread, e.g. on public social network pages and auction sites. Complex data protection rules are not adapted to such processing. It is therefore necessary to provide for a sufficiently wide exemption in Article 3.1bis.

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 at all stages of the processing a fair balance between all interests concerned, be they public or private interests, and the rights and freedoms at stake.

2. Each Party shall provide that data processing can be carried out only if:
a. the data subject has freely given his/her **[~~explicit,~~** unambiguous**~~]~~**, specific and informed consent, or
b. it is necessary for the performance of a contract to which the data subject is a party, or
c. it is necessary to comply with legal obligations binding the data controller, or
d. it is provided by domestic law for an overriding legitimate interest. [**Amendments should be made to bring Article 5.2 in line with Article 7 in Directive 95/46.]**

3. Personal data undergoing automatic processing shall be:
a. processed lawfully and fairly;

b. collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes;
c. adequate, relevant, not excessive ~~**and limited to the minimum necessary**~~ 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.

Comment:
As regards Article 5.2 we are concerned that the legitimate grounds for processing are too narrow compared to Article 7 in Directive 95/46. Grounds corresponding to Article 7 (d)-(f) of the Directive should therefore replace Article 5.2 d in the draft. As regards consent, we believe that "unambiguous" should be used instead of "explicit". This would keep the provision in line with Article 7 (a) of Directive 95/46.

Furthermore, changes should be made to Article 5.3 c in order to bring it in line with Article 6.1 (d) of Directive 95/46.

Article 7bis – Transparency of processing

1. Each Party shall provide that every controller must [~~**ensure the transparency of data processing in**~~ **Consider moving to Article 5.3**] inform~~**ing**~~ data subjects 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 categories of recipients of the personal data, and the means of exercising the rights set out in Article 8, as well as any other information necessary to ensure fair and lawful data processing.

2. The controller shall nonetheless not be required to provide such information where the processing is prescribed by law or this proves to be impossible or involves disproportionate efforts.

Comment:
In our view the transparency of processing does not only include the obligation to provide information according to Article 7bis but also the right of access in Article 8.d. If a general principle of transparency is to be introduced it should, therefore, rather be inserted in Article 5.3 than in Article 7bis.

Article 8 – Rights of the data subject

Any person shall be **entitled**:

a not to be subject to a decision significantly affecting him/her, based solely on an automatic processing of data without having his/her views taken into consideration;

b to object **on compelling legitimate grounds** at any time to the processing of personal data concerning him/her unless such a processing is compulsory by virtue of the law, **expressly authorised by law** or if the controller can justify of prevailing legitimate grounds;

c to obtain, on request, at reasonable intervals and without excessive delay or expense confirmation of the processing of personal data relating to him/her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period**, if known,** as well as any other information **to guarantee fair and lawful processing in respect of the data subject.** ~~**that the controller is required to provide to ensure the transparency of processing in accordance with Article 7bis paragraph 1;**~~

d to obtain, on request, knowledge of the reasoning underlying the data processing, **at least in the case of decisions referred to in litera a;** ~~**the results of which are applied to him/her;**~~

e to obtain, upon request, as the case may be, rectification or erasure of such data if these have been processed contrary to the law giving effect to the provisions of this Convention;

f 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 to benefit, whatever his/her residence, from the assistance of a supervisory authority within the meaning of Article 12bis, in exercising the rights provided by this Convention.

Comment:
Article 8 b should be adjusted to bring it more in line with Article 14 of Directive 95/46.

The reference in Article 8 c to Article 7bis paragraph 1 is rather vague and we therefore suggest some clarifications. Further, we are not convinced that information on "preservation period" should be obligatory and have therefore suggested an amendment also in this respect. An alternative to the said amendment could be to clarify in the Explanatory Report that information on the preservation period may be necessary to ensure fair data processing.

Article 8 d should be adjusted to bring it in line with Article 12 (a) of Directive 95/46. In this context it should be noted that Article 8 d introduces a more far-reaching information obligation than Article 15.1(h) in the proposed General Data Protection Regulation.

Article 8bis – Additional obligations

1. Each Party shall provide that the controller, or where applicable the processor, shall take at all stages of the processing all appropriate measures to implement the provisions giving effect to the principles and obligations of this Convention and to establish internal mechanisms to verify and **be able to** demonstrate to the data subjects and to the supervisory authorities provided for in Article 12bis of this Convention the compliance of the data processing for which he/she is responsible with the applicable law.

2. Each party shall provide that the controller shall carry out a risk analysis of the potential impact of the intended data processing on the rights and fundamental freedoms of the data subject and design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights and fundamental freedoms.

3. Each Party shall provide that the products and services intended for the data processing shall take into account the implications of the right to the protection of personal data from the stage of their design and facilitate the compliance of the processing with the applicable law.

4. Each Party can decide to derogate in full or in part to the provisions of the previous paragraphs, 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:
Sweden welcomes the *risk and context based approach* in this article. We firmly believe that a differentiation of the rules is necessary in order to strike a proper balance between the right to the protection of personal data and other interests.

In order to avoid the impression that the controller shall, on his/her own initiative, demonstrate compliance to the supervisory authority and the data subjects, it is suggested to insert "be able to" before "demonstrate".

Article 12

1. The following provisions shall apply to the **transfer ~~disclosure or making available~~** of data to a recipient who is not subject to the jurisdiction of the Party where data are.

2. A Party shall not, for the sole purpose of the protection of personal data, prohibit or subject to special authorisation the **transfer ~~disclosure or making available~~** of data to a recipient who is subject to the jurisdiction of another Party to the Convention, unless the Party where data originate from is regulated by harmonised regional rules of protection shared by several States and the **transfer ~~disclosure or making available of data~~** cannot be governed by measures foreseen in paragraph 4.b.

3 When the recipient is subject to the jurisdiction of a State or international organisation which is not Party to the Convention, the **transfer ~~disclosure or making available~~** of data can only occur where an appropriate level of personal data protection is guaranteed.

4. An appropriate level of protection can be ensured by:
a) the law of that State or international organisation, in particular by applicable international treaties or agreements, or
b) approved standardised legal measures or ad hoc legal measures, the latter having to be binding, capable of effective remedies and implemented by the person who **transfers the data ~~discloses or makes data accessible~~** and by the recipient.

5. Notwithstanding the provisions of paragraphs 2, 3 and 4, each Party may provide that **the transfer ~~the disclosure or making available~~** of data may take place, if **~~in a particular case~~**:
a) the data subject has given his/her specific, free and **~~explicit~~ [~~/~~**unambiguous**~~]~~** 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 **prevailing** interests**, especially important public interests, where provided for by domestic law~~protected by law and meeting the criteria of Article 9~~**, **~~prevail~~**.

6. Each party shall provide that the competent supervisory authority within the meaning of Article 12 bis of the Convention be informed of [the modalities regulating the data flow, such as ad hoc measures foreseen in paragraph 3.b **More precision needed.]**. It shall also provide that the supervisory authority be entitled to request that the person who **transfers the data**

~~discloses or makes data available~~, or the recipient, demonstrate the quality and effectiveness of actions taken or entitled to prohibit, suspend, or subject to condition the **transfer ~~disclosure or making available~~** of data within the meaning of paragraphs 4,b. or 5 [a and b].

Comment:
In order to bring Article 12 in line with the Article 25 of Directive 95/46 "transfer" should be used instead of "disclosure or making available". It should be noted that "transfer" is also used in the current CoE context (Article 2 in the Additional Protocol to Convention 108) and in the proposed General Data Protection Regulation (Chapter V). It is not appropriate to deviate from this well-established terminology.

Moreover, the expression "disclosure or making available" could be construed as also covering publication on the internet. This would be contrary to the ECJ ruling in the Lindqvist case. In that case the ECJ pinpointed the unrealistic consequences of an interpretation to the effect that publication of personal data on the internet would be covered by the rules on transfer to third countries, by stating that if "*even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.*" Such a regime would mean that – as a rule – all internet publication involving personal data would be forbidden. This would be unacceptable considering the importance of internet for the freedom of expression and information. The negative consequences in this respect would not be sufficiently mitigated by the proposal for a new exemption in Article 9.2.

As regards Article 12.5 we prefer a wording more in line with the current regime in the Additional Protocol. This would also be more coherent with Article 26 in Directive 95/46. For the same reason "unambiguous" should be used instead of "explicit".

In order to ensure legal certainty it has to be specified what "the modalities regulating the data flow" in Article 12.6 means in addition to "such as ad hoc measures foreseen in paragraph 3.b".

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. have powers of investigation and intervention;
b. perform the competences relating to transborder data flows foreseen under Article 12.6;
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. have power to engage in legal proceedings or to bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the provisions of this Convention;
e. are responsible for raising awareness of and providing information on data protection;

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 perform their duties and exercise their powers in complete independence~~,~~. **They~~they~~** shall neither seek nor accept instructions from anyone **in the performance of their duties**.

[---]

Comment:
It should be clarified that the ban on instructions only regards the performance of the supervisory authority's duties (compare Article 47.2 in the proposed General Data Protection Regulation).

SWITZERLAND/ SUISSE

Article 6 Traitement de données sensibles

1. Les traitements de données à caractère personnel pouvant présenter un risque grave pour les intérêts, droits et libertés fondamentales de la personne concernée, notamment un risque de discrimination, ne sont possibles qu'à la condition que le droit applicable prévoie des garanties appropriées, de nature à prévenir ce risque, ~~venant compléter celles de la présente convention.~~

Article 7 Sécurité des données

~~2 Chaque Partie prévoit que le responsable du traitement est tenu de notifier immédiatement à tout le moins aux autorités de contrôle au sens de l'article 12bis de la présente Convention les violations des données susceptibles de porter gravement atteinte aux droits et libertés fondamentales des personnes concernées.~~

Article 8 Droits des personnes concernées

Toute personne doit pouvoir :

a. ne pas être soumise à une décision l'affectant de manière significative, qui serait prise sur le seul fondement d'un traitement automatisé de données, sans que son point de vue soit pris en compte, à moins d'être autorisé par une loi qui prévoit également des mesures destinées à préserver les intérêts légitimes de la personne concernée;

Article 8bis Obligations complémentaires

1.Chaque Partie prévoit que le responsable du traitement, ou le cas échéant le sous-traitant, doit prendre à toutes les étapes du traitement toutes les mesures appropriées pour mettre en œuvre les dispositions donnant effet aux principes et obligations de la présente Convention et mettre en place des mécanismes internes pour vérifier et démontrer ~~aux personnes concernées et~~ aux autorités de contrôle prévues à l'article 12bis de la présente convention la conformité des traitements de données dont il est responsable au regard du droit applicable.

Article 9 Exceptions et restrictions

a. à la **sécurité nationale**, à la sûreté publique, à des intérêts **économiques et financiers importants** de l'Etat ou **à des fins de prévention et de détection** ~~et à la répression~~ des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales.

Chapitre III Flux transfrontières de données
Article 12

6 Chaque Partie prévoit que l'autorité de contrôle compétente au sens de l'article 12bis de la Convention soit informée des modalités encadrant les flux de données, notamment des mesures ad hoc prises au sens de l'article 12, paragraphe 4.b.
Elle prévoit également que l'autorité de contrôle puisse exiger de la personne qui communique ou rend accessibles les données ou du destinataire de démontrer la qualité et l'effectivité des mesures prises, ou que celle-ci puisse interdire, suspendre ou soumettre à condition la communication des données ou leur mise à disposition au sens des paragraphes 4, lettre b ou 5 [lettres a et b] ou demander à une autorité juridictionnelle de prendre de telles mesures.

Chapitre IIIbis Autorités de contrôle
Article 12bis Autorités de contrôle

2 A cet effet, ces autorités :

a. disposent de pouvoirs d'investigation et d'intervention ;
b. exercent les compétences en matière de flux transfrontières de données prévues à l'Article 12.6;
c. ~~Peuvent prononcer les décisions nécessaires au respect des mesures du droit interne donnant effet aux dispositions de la présente Convention et notamment sanctionner les infractions administratives~~ ;
d. disposent du pouvoir d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux dispositions **de la présente Convention ;**
e. **sont chargées de sensibiliser et d'éduquer à la protection des données.**

…

9 Les autorités de contrôle ne sont pas compétentes s'agissant des traitements effectués par les autorités compétentes dans le cadre d'une procédure judiciaire.
Ces traitements sont régis par le droit national.