COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 24 June / juin 2016 T-PD(2016)06Mos

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

Compilation of comments received on

DRAFT GUIDELINES ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA IN A WORLD OF BIG DATA

****

COMITE CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISE DES DONNEES A CARACTERE PERSONNEL (T-PD)

Compilation de commentaires reçus sur les

LIGNES DIRECTRICES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL DANS UN MONDE DE DONNEES MASSIVES

Directorate General / Direction Générale

Human Rights and Rule of Law / Droits de l'Homme et Etat de droit

TABLE / INDEX

AUSTRIA/ AUTRICHE

Preliminary remark: The substantive part of the text refers frequently to provisions of the draft modernized Convention. Since the negotiations concerning the modernized Convention have not been completed and since it is still not clear whether the modernized Convention will enter in to force, it is proposed not to refer to the draft provisions.

I. Introduction

These guidelines take into account the differences existing among the Parties, with regard to data protection regulation and have been drafted on the basis of the Convention 108, in the light of its ongoing process of modernisation. They are primarily addressed to rule-makers, data controllers and data processors, as defined in section III.

The Preamble of the Draft modernised Convention focuses on the protection of "personal autonomy based on a person's right to control his or her personal data and the processing of such data". The nature of this right to control should be carefully addressed with regard to the use of Big Data.

Control requires awareness of the use of data and real freedom of choice. These conditions, which are essential to the protection of fundamental rights, can be met through different legal solutions. These solutions should be tailored according to the given social and technological context, taking into account a lack of knowledge on the part of individuals.

The complexity and obscurity of Big Data applications should therefore prompt rule-makers to consider the notion of control as not circumscribed to mere individual control (e.g. notice and consent). They shall adopt a broader idea of control over the use of data, according to which individual control evolves in a more complex process of multiple-impact assessment of the risks related to the use of data.

II. Scope

The present Guidelines recommend measures which Parties, Data Controllers and Data Processors shall take to prevent the potential negative impact of the use of Big Data on human dignity, human rights and fundamental individual and collective freedoms, mainly with regard to data protection.

Given the nature of Big Data, the application of some of the traditional principles of data processing (e.g. minimization principle, purpose specification, meaningful consent, etc.) may be challenging in this technological scenario. These guidelines therefore suggest a tailored application of the principles of the Convention 108, to make them more effective in practice in the Big Data context.

The purpose of these guidelines is to define principles and practices to limit the risk related to the use of Big Data. These risks mainly concern the potential bias of data analysis, the underestimation of the social and ethical implications of the use of Big Data for decision-making processes, and the marginalization of a real and conscious involvement by individuals in these processes.

Since these guidelines concern Big Data in general and not sector-specific applications, they provide general and high-level guidance, which may be complemented by further guidelines on the protection of individuals within specific fields of application of Big Data (e.g. healthcare, financial sector).

Nothing in the present Guidelines shall be interpreted as precluding or limiting the provisions of the Convention 108 and the safeguards for the data subject recognised by the Convention.

III. Terminology used for the purpose of these guidelines:

a) Big Data: there are many definitions of Big Data, which differ depending on the specific discipline. Most of them focus on the growing technological ability to collect, process and extract predictive knowledge from great volume, velocity, and variety of data. Nevertheless, in terms of data protection, the main issues do not only concern the volume, velocity, and variety of processed data, but also the analysis of the data using software to extract predictive knowledge for decision-making purposes. For the purposes of these guidelines, therefore, the definition of Big Data encompasses both Big Data and Big Data analytics.

b) Draft modernised Convention: the Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (consolidated text revised in January 2016).

c) Parties: the parties who have ratified, accepted or approved the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.1.1981).

d) Personal Data: any information relating to an identified or identifiable data subject. Personal data are also any information used to take decisions affecting an individual belonging to a group based on group profiling information.

e) Risk-assessment Process: the process of risk-assessment as described below in section IV.2.

f) Sensitive Data: data belonging to the categories of Article 6 of the Convention 108. Data that do not directly reveal sensitive information, but may provide such information when further processed or combined with other data, are considered sensitive data.

g) Supervisory Authority: an ~~independent~~ authority which is established by a Party pursuant to Article 13 (2) of the Convention 108.

Comment [SM1]: This clearly goes beyond Art. 6 of Convention 108. It should be discussed in detail whether the T-PD wants to broaden the scope of sensitive data that significantly.

Comment [SM2]: the independence of supervisory authority is enshrined in Art. 1 of the AP to Convention 108 and not in the Convention itself.

IV. Principles and guidelines

1. Ethical and socially aware use of data

1.1 According to the principle of the fair balance between all interests concerned in the processing of personal information, where information is used for predictive purposes in decision-making processes, Data Controllers and Data Processors shall adequately take into account the broader ethical and social implications of Big Data to ensure the full respect for data protection obligations set forth by Convention 108 and to safeguard fundamental rights.

1.2 Data use cannot be in conflict with the ethical values commonly accepted in the relevant community or communities or prejudice societal interests, including the protection of human rights. While defining prescriptive ethical guidance may be problematic, due to the influence of contextual factors, the common guiding ethical values can be found in international charters of human rights and fundamental freedoms, such as the Convention for the Protection of Human Rights and Fundamental Freedoms.

1.3 If the Risk-assessment Process highlights a high impact of the use of Big Data on ethical values, data controllers may establish an ad hoc ethical committee to identify the specific ethical values that shall be safeguarded in the use of data.

2. Preventive policies and risk-assessment

2.1 Given the increasing complexity of data processing and the transformative use of Big Data, the Parties shall adopt a precautionary approach in regulating data protection in this field.

2.2 Data controllers shall adopt preventive policies concerning the risks of the use of data and its impact on individuals and society.

2.3 Pursuant to Article 5.1 and Article 8bis (2) of the Draft modernised Convention, a risk-assessment of the potential impact of data processing on fundamental rights and freedoms is necessary to balance the different interests affected by the use of Big Data.

2.4 Since the use of Big Data may affect not only individual privacy and data protection, but also the collective dimension of these rights, preventive policies and risk-assessment shall consider the social and ethical impact of the use of Big Data, including with regard to the right to equal treatment and to not be discriminated.

2.5 Data controllers shall conduct a Risk-assessment Process in order to:

1) Identify the risks
2) Evaluate the risks of each specific Big Data application and its potential negative outcome on individuals' rights and freedoms, in particular the right to the protection of personal data and the right to non-discrimination, taking into account the social and ethical impacts
3) Provide adequate solutions by-design to mitigate these risks
4) Monitor the adoption and the efficacy of the solutions provided

2.6 The Risk-assessment Process shall be carried out by persons with adequate professional qualifications and knowledge to evaluate the different impacts, including the social and ethical dimensions.

2.7 With regard to the use of Big Data which may affect fundamental rights, the Parties shall encourage the involvement of the different stakeholders in the Risk-assessment Process and in the design of data processing.

2.8 Data controllers shall regularly review the results of the Risk-assessment Process.

2.9 Data controllers shall document the assessment and the solutions referred to in paragraph 2.5.

2.10 Supervisory Authorities should provide recommendations to data controllers on the state-of-the-art of data processing security methods and guidelines on the Risk-assessment Process.

2.11 The Parties may introduce some limitations to the liability of Data Controllers for damage caused by the risks referred to in paragraph 2.5, when Data Controllers have processed Personal Data according to the provisions of this article.

3. Purpose specification and transparency

3.1 Given the transformative nature of the use of Big Data, the purposes of data processing to be considered explicit and specified, pursuant to Article 5 (b) of the Convention 108 and Article 5.4 (b) of the Draft modernised Convention, should also identify the potential impact on individuals of the different uses of data.

3.2 Pursuant to Article 7bis. (1) of the Draft modernised Convention, the results of the Risk-assessment Process shall be made publicly available, without prejudice to secrecy safeguarded by law. In the presence of such secrecy, Data Controllers shall provide any sensitive information in a separate annex to the risk-assessment report. This annex should not be public, but may be accessed by Supervisory Authorities.

3.3 Where the data gathered are further processed for historical, statistical and scientific purposes, they shall be stored in a form that permits identification of the data subjects for no longer than is necessary. In some of these cases, appropriate safeguards may include restriction to access and/or public availability of data where, according to the law, there is no public or individual legitimate interest to access such information.

4. By-design approach

4.1 On the basis of the Risk-assessment Process, Data Controllers and Data Processors shall adopt adequate by-design solutions at the different stages of the processing of Big Data.

4.2 Data Controllers and Data Processors shall carefully consider the design of their data analysis, in order to avoid potential hidden data biases, in both the collection and analysis stages, and minimize the presence of redundant or marginal data.

4.3 When it is technically feasible, Data Controllers and Data Processors shall test the adequacy of the by-design solutions adopted on a limited amount of data by means of simulations, before their use on a larger scale. This would make it possible to assess the potential bias of the use of different parameters in analysing data and provide evidence to minimise the use of information and mitigate the potential negative outcomes identified in the Risk-assessment Process.

4.4 Regarding the use of sensitive data, by-design solutions shall be adopted to avoid non-sensitive data being used to infer sensitive information and, if so used, to extend the same safeguards to these data as adopted for sensitive data.

5. Consent

5.1 Given the complexity of the use of Big Data, meaningful consent shall be based on the information provided to data subject pursuant to Article 7bis of the Draft modernised Convention. This information shall be comprehensive of the outcome of the Risk-assessment Process and might also be provided by means of an interface which simulates the effects of the use of data and its potential impact on the data subject, in a learn-from-experience approach.

5.2 When data have been collected on the basis of data subject's consent, they cannot be processed in a manner incompatible with the initial purposes. Data Controllers and Data Processors shall provide easy and user-friendly technical ways for data subjects to withdraw their consent and to oppose data processing incompatible with the initial purposes.

5.3 Pursuant to Article 5 (b) of the Convention 108, data processing is considered as incompatible when the use of data exposes data subjects to risks greater, or other than, those contemplated by the initial purposes.

5.4 Consent is not freely given if there is an imbalance of power between the data subject and the Data Controllers ~~or Data Processors~~. The Data Controller shall provide proof that this imbalance does not exist or does not affect the consent given by the data subject.

Comment [SM3]: the addressee of consent is the controller not the processor.

6. Anonymization

6.1 In the Big Data context, the anonymous nature of the data processed does not exclude, in general, the application of the principles concerning data protection, due to the risk of re-identification.

6.2 Anonymization may combine technical measures with legal or contractual obligations not to attempt to re-identify the data.

6.3 On the basis of the risk of re-identification, the Data Controller shall demonstrate and document the adequacy of the measures adopted to anonymize data. This assessment of the risk of re-identification shall take into account both the nature of the data and the costs of implementation of the available anonymizing technologies.

7. Role of the human factor in Big Data-supported decisions

7.1 The use of Big Data shall preserve the autonomy of the human factor in the decision-making process.

7.2 Decisions based on the results provided by Big Data analytics shall take into account all the circumstances concerning the data and shall not be based on merely decontextualized information or data processing results.

7.3 Where decisions based on Big Data might affect individual rights significantly or produce legal effects, a human decision-maker shall provide the data subject with detailed motivation.

Comment [SM4]: see Art. 15.1 of Directive 95/46/EC concerning automated decisions

Comment [SM5]: see Art. 22.1 of the GDPR concerning automated decisons

7.4 On the basis of reasonable arguments, the human decision-maker should be allowed the freedom to disagree with the recommendations provided using Big Data.

7.5 Where direct or indirect discrimination based on Big Data recommendations is suspected, Data Controllers and Data Processors shall demonstrate the absence of this discrimination.

7.6 The subjects that are affected by a decision based on Big Data have the right to challenge this decision before a competent authority.

8. Open data

8.1 Given the availability of Big Data analytics, public and private entities shall carefully consider their open data policies concerning personal data. When Data Controllers adopt open data policies, the Risk-assessment Process shall take into account the effects of merging and mining different data belonging to different open data sets.

9. Derogations for historical, statistical and scientific purposes

9.1 Where the Parties provide specific derogations to the provisions of Articles 7-bis and 8 of the Draft modernised Convention with respect to data processing for historical, statistical and scientific purposes, they should exclude any risk of infringement of the rights and fundamental freedoms of data subjects.

9.2 Derogations shall be limited to the extent strictly necessary and not be applied unless expressly provided for by the law.

9.3 Derogations cannot prejudice fundamental rights, the principle of non-discrimination, and the right of data subjects to challenge before a competent authority decisions taken on the basis of automated data processing.

10. Education

10.1 To help citizens understand the implications of the use of information and personal data in the Big Data context, the Parties shall recognize digital literacy as an essential educational skill, and incorporate it in the standard curriculum.

* * *

FRANCE

I. Introduction

These guidelines take into account the differences existing among the Parties, with regard to data protection regulation and have been drafted on the basis of the Convention 108, in the light of its ongoing process of modernisation. They are primarily addressed to rule-makers, data controllers and data processors, as defined in section III.

The Preamble of the Draft modernised Convention focuses on the protection of "personal autonomy based on a person's right to control his or her personal data and the processing of such data". The nature of this right to control should be carefully addressed with regard to the use of Big Data.

Control requires awareness of the use of data and real freedom of choice. These conditions, which are essential to the protection of fundamental rights, can be met through different legal solutions. These solutions should be tailored according to the given social and technological context, taking into account a lack of knowledge on the part of individuals.

The complexity and obscurity of Big Data applications should therefore prompt rule-makers to consider the notion of control as not circumscribed to mere individual control (e.g. notice and consent). They shall adopt a broader idea of control over the use of data, according to which individual control evolves in a more complex process of multiple-impact assessment of the risks related to the use of data.

II. Scope

The present Guidelines recommend measures which Parties, Data Controllers and Data Processors shall take to prevent the potential negative impact of the use of Big Data on human dignity, human rights and fundamental individual and collective freedoms, mainly with regard to data protection.

Given the nature of Big Data, the application of some of the traditional principles of data processing (e.g. minimization principle, purpose specification, meaningful consent, etc.) may be challenging in this technological scenario. These guidelines therefore suggest a tailored application of the principles of the Convention 108, to make them more effective in practice in the Big Data context.

The purpose of these guidelines is to define principles and practices to limit the risk related to the use of Big Data. These risks mainly concern the potential bias of data analysis, the underestimation of the social and ethical implications of the use of Big Data for decision-making processes, and the marginalization of a real and conscious involvement by individuals in these processes.

Since these guidelines concern Big Data in general and not sector-specific applications, they provide general and high-level guidance, which may be complemented by further guidelines on the protection of individuals within specific fields of application of Big Data (e.g. healthcare, financial sector).

Nothing in the present Guidelines shall be interpreted as precluding or limiting the provisions of the Convention 108 and the safeguards for the data subject recognised by the Convention.

Comment [MA6]: Cette réserve devrait être étendue au profit de la récente réglementation UE en matière de protection des données personnelles (règlement 2016/679 et directive 2016/680))

III. Terminology used for the purpose of these guidelines:

a) Big Data: there are many definitions of Big Data, which differ depending on the specific discipline. Most of them focus on the growing technological ability to collect, process and extract predictive knowledge from great volume, velocity, and variety of data. Nevertheless, in terms of data protection, the main issues do not only concern the volume, velocity, and variety of processed data, but also the analysis of the data using software to extract predictive knowledge for decision-making purposes. For the purposes of these guidelines, therefore, the definition of Big Data encompasses both Big Data and Big Data analytics.

b) Draft modernised Convention: the Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (consolidated text revised in January 2016).

c) Parties: the parties who have ratified, accepted or approved the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.1.1981).

d) Personal Data: any information relating to an identified or identifiable data subject. Personal data are also any information used to take decisions affecting an individual belonging to a group based on group profiling information.

e) Risk-assessment Process: the process of risk-assessment as described below in section IV.2.

f) Sensitive Data: data belonging to the categories of Article 6 of the Convention 108. Data that do not directly reveal sensitive information, but may provide such information when further processed or combined with other data, are considered sensitive data.

g) Supervisory Authority: an independent authority which is established by a Party pursuant to Article 13 (2) of the Convention 108.

IV. Principles and guidelines

1. Ethical and socially aware use of data

1.1 According to the principle of the fair balance between all interests concerned in the processing of personal information, where information is used for predictive purposes in decision-making processes, Data Controllers and Data Processors shall adequately take into account the broader ethical and social implications of Big Data to ensure the full respect for data protection obligations set forth by Convention 108 and to safeguard fundamental rights.

1.2 Data use cannot be in conflict with the ethical values commonly accepted in the relevant community or communities or prejudice societal interests, including the protection of human rights. While defining prescriptive ethical guidance may be problematic, due to the influence of contextual factors, the common guiding ethical values can be found in international charters of human rights and fundamental freedoms, such as the Convention for the Protection of Human Rights and Fundamental Freedoms.

1.3 If the Risk-assessment Process highlights a high impact of the use of Big Data on ethical values, data controllers may establish an ad hoc ethical committee to identify the specific ethical values that shall be safeguarded in the use of data.

2. Preventive policies and risk-assessment

2.1 Given the increasing complexity of data processing and the transformative use of Big Data, the Parties shall adopt a precautionary approach in regulating data protection in this field.

2.2 Data controllers shall adopt preventive policies concerning the risks of the use of data and its impact on individuals and society.

2.3 Pursuant to Article 5.1 and Article 8bis (2) of the Draft modernised Convention, a risk-assessment of the potential impact of data processing on fundamental rights and freedoms is necessary to balance the different interests affected by the use of Big Data.

2.4 Since the use of Big Data may affect not only individual privacy and data protection, but also the collective dimension of these rights, preventive policies and risk-assessment shall consider the social and ethical impact of the use of Big Data, including with regard to the right to equal treatment and to not be discriminated.

2.5 Data controllers shall conduct a Risk-assessment Process in order to:

1) Identify the risks
2) Evaluate the risks of each specific Big Data application and its potential negative outcome on individuals' rights and freedoms, in particular the right to the protection of personal data and the right to non-discrimination, taking into account the social and ethical impacts
3) Provide adequate solutions by-design to mitigate these risks
4) Monitor the adoption and the efficacy of the solutions provided

2.6 The Risk-assessment Process shall be carried out by persons with adequate professional qualifications and knowledge to evaluate the different impacts, including the social and ethical dimensions.

2.7 With regard to the use of Big Data which may affect fundamental rights, the Parties shall encourage the involvement of the different stakeholders in the Risk-assessment Process and in the design of data processing.

2.8 Data controllers shall regularly review the results of the Risk-assessment Process.

2.9 Data controllers shall document the assessment and the solutions referred to in paragraph 2.5.

2.10 Supervisory Authorities should provide recommendations to data controllers on the state-of-the-art of data processing security methods and guidelines on the Risk-assessment Process.

2.11 The Parties may introduce some limitations to the liability of Data Controllers for damage caused by the risks referred to in paragraph 2.5, when Data Controllers have processed Personal Data according to the provisions of this article.

Comment [MA7]: Une clarification serait utile, notamment, afin d'éviter un problème de cohérence avec les articles 35 et 82 du règlement 2016/679 et les article 27 et 56 de la directive 2016/680 .

3. Purpose specification and transparency

3.1 Given the transformative nature of the use of Big Data, the purposes of data processing to be considered explicit and specified, pursuant to Article 5 (b) of the Convention 108 and Article 5.4 (b) of the Draft modernised Convention, should also identify the potential impact on individuals of the different uses of data.

3.2 Pursuant to Article 7bis. (1) of the Draft modernised Convention, the results of the Risk-assessment Process shall be made publicly available, without prejudice to secrecy safeguarded by law. In the presence of such secrecy, Data Controllers shall provide any sensitive information in a separate annex to the risk-assessment report. This annex should not be public, but may be accessed by Supervisory Authorities.

3.3 Where the data gathered are further processed for historical, statistical and scientific purposes, they shall be stored in a form that permits identification of the data subjects for no longer than is necessary. In some of these cases, appropriate safeguards may include restriction to access and/or public availability of data where, according to the law, there is no public or individual legitimate interest to access such information.

Comment [MA8]: « For archiving purposes in the public interest, scientific or historical research purposes or statistical » (langage agéée à la réunion du CAHDATA du 15 et 16 juin 2016) ;

4. By-design approach

4.1 On the basis of the Risk-assessment Process, Data Controllers and Data Processors shall adopt adequate by-design solutions at the different stages of the processing of Big Data.

4.2 Data Controllers and Data Processors shall carefully consider the design of their data analysis, in order to avoid potential hidden data biases, in both the collection and analysis stages, and minimize the presence of redundant or marginal data.

4.3 When it is technically feasible, Data Controllers and Data Processors shall test the adequacy of the by-design solutions adopted on a limited amount of data by means of simulations, before their use on a larger scale. This would make it possible to assess the potential bias of the use of different parameters in analysing data and provide evidence to minimise the use of information and mitigate the potential negative outcomes identified in the Risk-assessment Process.

4.4 Regarding the use of sensitive data, by-design solutions shall be adopted to avoid non-sensitive data being used to infer sensitive information and, if so used, to extend the same safeguards to these data as adopted for sensitive data.

5. Consent

5.1 Given the complexity of the use of Big Data, meaningful consent shall be based on the information provided to data subject pursuant to Article 7bis of the Draft modernised Convention. This information shall be comprehensive of the outcome of the Risk-assessment Process and might also be provided by means of an interface which simulates the effects of the use of data and its potential impact on the data subject, in a learn-from-experience approach.

5.2 When data have been collected on the basis of data subject's consent, they cannot be processed in a manner incompatible with the initial purposes. Data Controllers and Data Processors shall provide easy and user-friendly technical ways for data subjects to withdraw their consent and to oppose data processing incompatible with the initial purposes.

5.3 Pursuant to Article 5 (b) of the Convention 108, data processing is considered as incompatible when the use of data exposes data subjects to risks greater, or other than, those contemplated by the initial purposes.

5.4 Consent is not freely given if there is an imbalance of power between the data subject and the Data Controllers or Data Processors. The Data Controller shall provide proof that this imbalance does not exist or does not affect the consent given by the data subject.

6. Anonymization

6.1 In the Big Data context, the anonymous nature of the data processed does not exclude, in general, the application of the principles concerning data protection, due to the risk of re-identification.

6.2 Anonymization may combine technical measures with legal or contractual obligations not to attempt to re-identify the data.

6.3 On the basis of the risk of re-identification, the Data Controller shall demonstrate and document the adequacy of the measures adopted to anonymize data. This assessment of the risk of re-identification shall take into account both the nature of the data and the costs of implementation of the available anonymizing technologies.

Comment [MA9]: A clarifier pour éviter toute confusion entre l'anonymisation et la pseudonymisation (au sens de l'article 4, sous 5, du règlement 2016/679). Il serait préférable de parler de pseudonymisation s'agissant de données n'excluant pas l'identification

7. Role of the human factor in Big Data-supported decisions

7.1 The use of Big Data shall preserve the autonomy of the human factor in the decision-making process.

7.2 Decisions based on the results provided by Big Data analytics shall take into account all the circumstances concerning the data and shall not be based on merely decontextualized information or data processing results.

7.3 Where decisions based on Big Data might affect individual rights, a human decision-maker shall provide the data subject with detailed motivation.

Comment [MA10]: A clarifier pour éviter un problème de cohérence avec l'article 22 du règlement 2016/679, dans la mesure où le paragraphe 1er de cet article une interdiction de principe des décisions individuelles automatisées. Idem pour l'article 11 de la directive 2016/680. Il est proposé de rajouter « Those decisions can be prohibited by the parties where necessary for the protection of individual rights ».

7.4 On the basis of reasonable arguments, the human decision-maker should be allowed the freedom to disagree with the recommendations provided using Big Data.

7.5 Where direct or indirect discrimination based on Big Data recommendations is suspected, Data Controllers and Data Processors shall demonstrate the absence of this discrimination.

7.6 The subjects that are affected by a decision based on Big Data have the right to challenge this decision before a competent authority.

8. Open data

8.1 Given the availability of Big Data analytics, public and private entities shall carefully consider their open data policies concerning personal data. When Data Controllers adopt open data policies, the Risk-assessment Process shall take into account the effects of merging and mining different data belonging to different open data sets.

9. Derogations for historical, statistical and scientific purposes

9.1 Where the Parties provide specific derogations to the provisions of Articles 7-bis and 8 of the Draft modernised Convention with respect to data processing for historical, statistical and scientific purposes, they should exclude any risk of infringement of the rights and fundamental freedoms of data subjects.

Comment [MA11]: Idem commentaire MA 3

9.2 Derogations shall be limited to the extent strictly necessary and not be applied unless expressly provided for by the law.

9.3 Derogations cannot prejudice fundamental rights, the principle of non-discrimination, and the right of data subjects to challenge before a competent authority decisions taken on the basis of automated data processing.

10. Education

10.1 To help citizens understand the implications of the use of information and personal data in the Big Data context, the Parties shall recognize digital literacy as an essential educational skill, and incorporate it in the standard curriculum.

* * *

SWEDEN/ SUEDE

Comments on Draft Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data

General:

The issue of data protection in relation to Big Data is very important and requires close examination. It is necessary to both acknowledge the value of Big Data e.g. for research, statistic and health care purposes and to mitigate the risks for the protection of privacy.

We believe that the Guidelines require further elaboration and that it is necessary to consult stakeholders using Big Data in the work on the Guidelines. Furthermore, it is unusual to provide Guidelines in relation to a Draft Convention which is under negotiation. Therefore, the Guidelines should not be adopted at the upcoming plenary. The work should continue in order to achieve high quality Guidelines which may provide both real value for users of Big Data and better protection of personal data.

The purpose of the Guidelines should, thus be to provide advice and best practice to users of Big Data in order to achieve better data protection for individuals. The Guidelines should not provide new norms for data protection in relation to Big Data.

A general remark is that the language in the Guidelines gives the impression that the Guidelines are binding. “Shall” should be replaced by “may”, “could” or “should”.

We have some comments regarding specific parts of the Guidelines, which are presented below. These comments should be regarded as preliminary.

Comments on specific parts of the Guidelines:

III. Terminology used for the purpose of these Guidelines

The Guidelines provides in d) and f) for different and wider definitions of personal data and sensitive data than the Draft Convention. The applicability of the convention cannot be widened through the Guidelines. The definitions in the Guidelines should therefore be aligned with those in the Draft Convention.

IV. Principles and guidelines

3.1.

It is difficult to understand how the "purposes of data processing" can "identify the potential impact on indiviuals". This provision therefore needs to be redrafted.

3.2

The requirement to make the results of the Risk Assessment Process publicly available appears far reaching and requires further elaboration.

5.3

A higher level of risk or another risk may be one factor to take into account when assessing compatibility of purposes, but does not automatically mean that there actually is incompatibility. The provision should be redrafted accordingly.

5.4

It cannot be said that a mere imbalance of power between controller and data subjects invalidates consent. In the Data Protection Regulation "clear imbalance" is used (see recital 43). The rule on burden of proof in the second sentence is too far reaching and should be redrafted.

6.1

To our understanding anonymous data are not personal data. The Convention is only applicable to personal data and thus not applicable to anonymous data. We therefore believe that p. 6.1 needs to be redrafted. The risk of re-identification should of course be taken seriously, but recommendations to mitigate this risk are given in 6.2 and 6.3.

7

Section 7 provides stricter standards than the Draft Convention as regards automatic decisions and should be adapted to the level of protection in the convention.

9

The Guidelines reduces the room for exemptions in the Draft Convention significantly. The Guidelines should be aligned with the convention.

10

The Guidelines is not the proper place to introduce requirements for the national curriculum. Instead, the Guidelines could emphasize the importance of digital literacy as a means of mitigating privacy risks and therefore encourage digital literacy education.

UNITED KINGDOM/ ROYAUME UNI

UK's response on the Draft Opinion on the Data protection implications of the processing of personal data in a world of Big Data

Introduction

The Bureau of the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD-BUR) have requested comments on the Draft guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (T-PD-BUR (2015) 12rev).

UK's response

Chapter 2.1 – The UK would like to see a proportionate rather than a precautionary approach to data protection regulation. We agree it is important to robustly protect the rights of citizens, but it is possible to do this whilst not also having to stifle responsible business use of data to create new products and services. Any legislation also needs to be designed to keep up with the fast-moving pace of new technological advancements in big data processing.

Chapter 2.6 – The UK believes this may be difficult to achieve in practice. Who would determine what are 'adequate professional qualifications', and would this create difficulties for some small businesses?

Chapter 5.4 – The UK believes the guidance raises practical issues. It is difficult to see how a data controller would be able to provide proof that there is not an imbalance of power between themselves and the data subject. We join Switzerland in questioning whether this imbalance of power actually exists in most business-consumer or business-to-business relationships?

* * *

EDPS / CEPD

I. Introduction

These guidelines take into account the differences existing among the Parties, with regard to data protection regulation and have been drafted on the basis of the Convention 108, in the light of its ongoing process of modernisation. They are primarily addressed to rule-makers, data controllers and data processors, as defined in section III.

The Preamble of the Draft modernised Convention focuses on the protection of "personal autonomy based on a person's right to control his or her personal data and the processing of such data". The nature of this right to control should be carefully addressed with regard to the use of Big Data.

Control requires awareness of the use of data and real freedom of choice. These conditions, which are essential to the protection of fundamental rights, can be met through different legal solutions. These solutions should be tailored according to the given social and technological context, taking into account a lack of knowledge on the part of individuals.

The complexity and obscurity of Big Data applications should therefore prompt rule-makers to consider the notion of control as not circumscribed to mere individual control (e.g. notice and consent). They shall adopt a broader idea of control over the use of data, according to which individual control evolves in a more complex process of multiple-impact assessment of the risks related to the use of data.

II. Scope

The present Guidelines recommend measures which Parties, Data Controllers and Data Processors shall take to prevent the potential negative impact of the use of Big Data on human dignity, human rights and fundamental individual and collective freedoms, mainly with regard to data protection.

Given the nature of Big Data, the application of some of the traditional principles of data processing (e.g. minimization principle, purpose specification, meaningful consent, etc.) may be challenging in this technological scenario. These guidelines therefore suggest a tailored application of the principles of the Convention 108, to make them more effective in practice in the Big Data context.

The purpose of these guidelines is to define principles and practices to limit the risk related to the use of Big Data. These risks mainly concern the potential bias of data analysis, the underestimation of the social and ethical implications of the use of Big Data for decision-making processes, and the marginalization of a real and conscious involvement by individuals in these processes.

Since these guidelines concern Big Data in general and not sector-specific applications, they provide general and high-level guidance, which may be complemented by further guidelines on the protection of individuals within specific fields of application of Big Data (e.g. healthcare, financial sector).

Nothing in the present Guidelines shall be interpreted as precluding or limiting the provisions of the Convention 108 and the safeguards for the data subject recognised by the Convention.

Comment [u12]: I'm not sure about idea to start by flagging differences among members with regard to data protection, especially now that an EU regulation approximates the legal framework and that convention 108, as mentioned, is being modernised. I think it gives the wrong introductory message.

III. Terminology used for the purpose of these guidelines:

a) Big Data: there are many definitions of Big Data, which differ depending on the specific discipline. Most of them focus on the growing technological ability to collect, process and extract predictive knowledge from great volume, velocity, and variety of data. Nevertheless, in terms of data protection, the main issues do not only concern the volume, velocity, and variety of processed data, but also the analysis of the data using software to extract predictive knowledge for decision-making purposes. For the purposes of these guidelines, therefore, the definition of Big Data encompasses both Big Data and Big Data analytics.

b) Draft modernised Convention: the Draft modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (consolidated text revised in January 2016).

c) Parties: the parties who have ratified, accepted or approved the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 28.1.1981).

d) Personal Data: any information relating to an identified or identifiable data subject. Personal data are also any information used to take decisions affecting an individual belonging to a group based on group profiling information.

e) Risk-assessment Process: the process of risk-assessment as described below in section IV.2.

f) Sensitive Data: data belonging to the categories of Article 6 of the Convention 108. Data that do not directly reveal sensitive information, but may provide such information when further processed or combined with other data, are considered sensitive data.

g) Supervisory Authority: an independent authority which is established by a Party pursuant to Article 13 (2) of the Convention 108.

IV. Principles and guidelines

1. Ethical and socially aware use of data

1.1 According to the principle of the fair balance between all interests concerned in the processing of personal information, where information is used for predictive purposes in decision-making processes, Data Controllers and Data Processors shall adequately take into account the broader ethical and social implications of Big Data to ensure the full respect for data protection obligations set forth by Convention 108 and to safeguard fundamental rights.

1.2 Data use cannot be in conflict with the ethical values commonly accepted in the relevant community or communities or prejudice societal interests, including the protection of human rights. While defining prescriptive ethical guidance may be problematic, due to the influence of contextual factors, the common guiding ethical values can be found in international charters of human rights and fundamental freedoms, such as the Convention for the Protection of Human Rights and Fundamental Freedoms.

1.3 If the Risk-assessment Process highlights a high impact of the use of Big Data on ethical values, data controllers may establish an ad hoc ethical committee to identify the specific ethical values that shall be safeguarded in the use of data.

2. Preventive policies and risk-assessment

2.1 Given the increasing complexity of data processing and the transformative use of Big Data, the Parties shall adopt a precautionary approach in regulating data protection in this field.

2.2 Data controllers shall adopt preventive policies concerning the risks of the use of data and its impact on individuals and society.

2.3 Pursuant to Article 5.1 and Article 8bis (2) of the Draft modernised Convention, a risk-assessment of the potential impact of data processing on fundamental rights and freedoms is necessary to balance the different interests affected by the use of Big Data.

2.4 Since the use of Big Data may affect not only individual privacy and data protection, but also the collective dimension of these rights, preventive policies and risk-assessment shall consider the social and ethical impact of the use of Big Data, including with regard to the right to equal treatment and to not be discriminated.

2.5 Data controllers shall conduct a Risk-assessment Process in order to:

1) Identify the risks
2) Evaluate the risks of each specific Big Data application and its potential negative outcome on individuals' rights and freedoms, in particular the right to the protection of personal data and the right to non-discrimination, taking into account the social and ethical impacts
3) Provide adequate solutions by-design to mitigate these risks
4) Monitor the adoption and the efficacy of the solutions provided

2.6 The Risk-assessment Process shall be carried out by persons with adequate professional qualifications and knowledge to evaluate the different impacts, including the social and ethical dimensions.

2.7 With regard to the use of Big Data which may affect fundamental rights, the Parties shall encourage the involvement of the different stakeholders in the Risk-assessment Process and in the design of data processing.

2.8 Data controllers shall regularly review the results of the Risk-assessment Process.

2.9 Data controllers shall document the assessment and the solutions referred to in paragraph 2.5.

2.10 Supervisory Authorities should provide recommendations to data controllers on the state-of-the-art of data processing security methods and guidelines on the Risk-assessment Process.

2.11 The Parties may introduce some limitations to the liability of Data Controllers for damage caused by the risks referred to in paragraph 2.5, when Data Controllers have processed Personal Data according to the provisions of this article.

Comment [u13]: We strongly oppose this wording.
This is not a regulatory document and it should not foresee any possibility for parties to derogate from liability principles a set in the legal framework.
The text could only recommend that measures taken by the data controller to mitigate risks are taken into account in evaluating the sanction, where the margin of evaluation exists. It should not impact liability rules.

3. Purpose specification and transparency

3.1 Given the transformative nature of the use of Big Data, the purposes of data processing to be considered explicit, ~~and~~ specified and legitimate, pursuant to Article 5 (b) of the Convention 108 and Article 5.4 (b) of the Draft modernised Convention, should also identify the potential impact on individuals of the different uses of data.

Comment [u14]: There is a confusion between purpose specification and balance of interest/legitimacy, which are two different concepts. Legitimacy should at least be added here.

3.2 Pursuant to Article 7bis. (1) of the Draft modernised Convention, the results of the Risk-assessment Process shall be made publicly available, without prejudice to secrecy safeguarded by law. In the presence of such secrecy, Data Controllers shall provide any sensitive information in a separate annex to the risk-assessment report. This annex should not be public, but may be accessed by Supervisory Authorities.

3.3 Where the data gathered are further processed for historical, statistical and scientific purposes, they shall be stored in a form that permits identification of the data subjects for no longer than is necessary. In some of these cases, appropriate safeguards may include restriction to access and/or public availability of data where, according to the law, there is no public or individual legitimate interest to access such information.

4. By-design approach

4.1 On the basis of the Risk-assessment Process, Data Controllers and Data Processors shall adopt adequate by-design solutions at the different stages of the processing of Big Data.

4.2 Data Controllers and Data Processors shall carefully consider the design of their data analysis, in order to avoid potential hidden data biases, in both the collection and analysis stages, and minimize the presence of redundant or marginal data.

4.3 When it is technically feasible, Data Controllers and Data Processors shall test the adequacy of the by-design solutions adopted on a limited amount of data by means of simulations, before their use on a larger scale. This would make it possible to assess the potential bias of the use of different parameters in analysing data and provide evidence to minimise the use of information and mitigate the potential negative outcomes identified in the Risk-assessment Process.

4.4 Regarding the use of sensitive data, by-design solutions shall be adopted to avoid non-sensitive data being used to infer sensitive information and, if so used, to extend the same safeguards to these data as adopted for sensitive data.

5. Consent

5.1 Given the complexity of the use of Big Data, meaningful consent shall be based on the information provided to data subject pursuant to Article 7bis of the Draft modernised Convention. This information shall be comprehensive of the outcome of the Risk-assessment Process and might also be provided by means of an interface which simulates the effects of the use of data and its potential impact on the data subject, in a learn-from-experience approach.

5.2 When data have been collected on the basis of data subject's consent, they cannot be processed in a manner incompatible with the initial purposes. Data Controllers and Data Processors shall provide easy and user-friendly technical ways for data subjects to ~~withdraw their~~provide their consent for such further processing, or, where this is sufficient,~~and~~ to oppose data processing incompatible with the initial purposes.

5.3 Pursuant to Article 5 (b) of the Convention 108, compatibility is assessed on the basis of the nature of the purpose(s) followed, and taking into account the reasonable expectations of the data subject. A data processing activity is considered as incompatible, for instance, when the use of data exposes data subjects to risks greater, or other than, those contemplated by the initial purposes.

5.4 Consent is not freely given if there is an imbalance of power between the data subject and the Data Controllers or Data Processors. The Data Controller shall provide proof that this imbalance does not exist or does not affect the consent given by the data subject.

6. Use of a~~A~~nonymization techniques

6.1 In the Big Data context, the fact that efforts have been made to anonymise the data ~~anonymous nature of the data processed~~ does not exclude, in general, the application of the principles concerning data protection, due to the risk of re-identification.

6.2 Anonymization techniques may combine technical measures with legal or contractual obligations not to attempt to re-identify the data.

6.3 On the basis of the risk of re-identification, the Data Controller shall demonstrate and document the adequacy of the measures adopted to ~~anonymize~~ keep the data secure. This assessment of the risk of re-identification shall take into account both the nature of the data and the costs of implementation of the available anonymizing technologies.

Comment [A15]: Under EU law, in many cases opt-in (consent) is required and objection is not sufficient.
Practically speaking this means the processing cannot take place as long as the individual has not taken a positive action.
This is much more protective and it is justified in a context of processing for incompatible purpose, where the intrusion in the rights is greater.

Comment [u16]: (in)compatibility is not only related to risk (danger of an assessment only based on such an approach).
But risk can be an element of the assessment.

Comment [u17]: It is not correct, legally speaking, to talk about anonymous data if a risk of re-identification exists.

Comment [u18]: For the same reason, it is inaccurate to talk about anonymised data. Because data are identifiable, they shall be protected against unlawful access.

7. Role of the human factor in Big Data-supported decisions

7.1 The use of Big Data shall preserve the autonomy of the human factor in the decision-making process.

7.2 Decisions based on the results provided by Big Data analytics shall take into account all the circumstances concerning the data and shall not be based on merely decontextualized information or data processing results.

7.3 Where decisions based on Big Data might affect individual rights, a human decision-maker shall provide the data subject with detailed motivation.

7.4 On the basis of reasonable arguments, the human decision-maker should be allowed the freedom to disagree with the recommendations provided using Big Data.

7.5 Where direct or indirect discrimination based on Big Data recommendations is suspected, Data Controllers and Data Processors shall demonstrate the absence of this discrimination.

7.6 The subjects that are affected by a decision based on Big Data have the right to challenge this decision before a competent authority.

8. Open data

8.1 Given the availability of Big Data analytics, public and private entities shall carefully consider their open data policies concerning personal data. When Data Controllers adopt open data policies, the Risk-assessment Process shall take into account the effects of merging and mining different data belonging to different open data sets.

9. Derogations for historical, statistical and scientific purposes

9.1 Where the Parties provide specific derogations to the provisions of Articles 7-bis and 8 of the Draft modernised Convention with respect to data processing for historical, statistical and scientific purposes, they should exclude any risk of infringement of the rights and fundamental freedoms of data subjects.

9.2 Derogations shall be limited to the extent strictly necessary and not be applied unless expressly provided for by the law.

9.3 Derogations cannot prejudice fundamental rights, the principle of non-discrimination, and the right of data subjects to challenge before a competent authority decisions taken on the basis of automated data processing.

10. Education

10.1 To help citizens understand the implications of the use of information and personal data in the Big Data context, the Parties shall recognize digital literacy as an essential educational skill, and incorporate it in the standard curriculum.

* * *

Commentaires du Comité européen de coopération juridique (CDCJ)

4. GUIDELINES ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA IN A WORLD OF BIG DATA
LIGNES DIRECTRICES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL DANS UN MONDE DE DONNEES MASSIVES
document T-PD-BUR(2015)12Rev

Commentaire de la Belgique

Le texte « données massives / big data » est globalement acceptable. Il appartiendra à nos experts au T-PD de formuler les commentaires nécessaires.

Commentaires de la Suisse

- Ch. 5.4 : nous craignons que cette guideline ne pose d'énormes problèmes de praticabilité. Dans la plupart des cas, il y a un déséquilibre entre la personne concernée et le responsable de traitement (les rapports contractuels sont rarement équilibrés). Doit-on par conséquent considérer que le consentement n'est jamais donné librement ? Si on prend au sérieux cette disposition, c'est à ce résultat qu'on arrive. Et comment le responsable de traitement peut-il démontrer que le consentement a été donné librement, sauf à limiter considérablement la liberté contractuelle ?

- Ch. 7.4 et 7.5 : ces lignes directrices vont très loin et reviennent à introduire une direction générale de discriminer de manière directe ou indirecte dans les relations entre les particuliers ainsi qu'une forme de renversement du fardeau de la preuve, que l'on ne connaît (ou moins en droit suisse) que dans des domaines très limités. Quant à la personne physique habilitée à prendre la décision, comment garantir son droit d'être en désaccord ? Dans les rapports de subordination du contrat de travail, cela va être difficile pour un employé d'être en désaccord. Là aussi, nous voyons de gros problèmes pratiques.

* * *