COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Strasbourg, 20 September / septembre 2016

T-PD(2016)06MosRev

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.

* * *

BELGIUM / BELGIQUE

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.

Comment [VV6]: Nous mettrions davantage en évidence l'émergence du phénomène du Big Data et la nécessité de proposer une manière adéquate d'appliquer les principes de protection des données plutôt que les divergences entre les législations nationales.

Comment [VV7]: Remarque générale: ce projet de lignes directrices cite des articles tant de la Convention 108 modernisée en projet que de la Convention 108. Le projet de recommandation "santé" ne fait quant à lui aucune référence à un article cité en particulier (de la Convention 108) et ne renvoie en aucune façon au projet de Convention 108 modernisée. **Ne faudrait-il pas adopter une ligne identique dans les projets de nouveaux textes et évaluier l'opportunité de la référence à la Convention 108 modernisée (pas encore adoptée)**

Comment [VV8]: Le texte utilise parfois "shall", parfois "should": à harmoniser ?

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).

Comment [VV9]: Il s'agit de deux secteurs qui relève plutôt du domaine public (même si financial couvre les 2). Ne faudrait-il pas aussi viser des applications "Big Data" par le secteur privé ?

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:

h) 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.

i) 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).

j) 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).

k) 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.

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

m) 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.

n) 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.

Comment [VV10]: Ces implications devraient être explicitées dans l'exposé des motifs

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:

5) Identify the risks

6) 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

Comment [VV11]: A partir du moment où le document part de l'idée que c'est l'impact du Big Data qu'il faut examiner /évaluer, cet impact n'est pas nécessairement négatif. La relation "risque / impact" pourrait-elle être explicitée dans l'exposé des motifs ?

7) Provide adequate solutions by-design to mitigate these risks

8) 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 [VV12]: Cette disposition n'est pas acceptable. Elle est formulée telle un article de Convention alors qu'il s'agit ici de lignes directrices / de recommandations. Il ne peut y avoir de limitation de responsabilité ipso facto mais bien une prise en compte de l'attitude du responsable de traitement (respect de l'article 2.5.) dans le cadre de l'appréciation de la responsabilité.

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.

Comment [VV13]: Le principe de légitimité doit être ajouté ici. Il ne figure pas dans les lignes directrices. Le principe de finalité ne se confond pas avec celui-ci.

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 [VV14]: Le principe d'absence d'incompatibilité du traitement ultérieur ne vaut pas uniquement lorsque la base de légitimité du traitement primaire est le consentement.

Comment [VV15]: il ne suffit pas de prévoir un droit d'opposition aux traitements ultérieurs "incompatibles". Ces traitements ne sont pas admis. le GDPR de l'UE modifie cette approche de l'analyse du rôle du consentement dans le cadre des traitements ultérieurs mais la Convention 108 en l'état permet-elle une telle approche ?

Comment [VV16]: L'exigence d'absence d'incompatibilité ne dépend pas du risque plus élevé du traitement ultérieur par rapport au traitement initial.

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 [VV17]: Comme suggéré par l'EDPS, il serait préférable de parler ici de l'utilisation de techniques d'anonymisation plutôt que de données anonymes.

Comment [VV18]: Ceci ne suffit pas pour parler d'anonymisation.

Comment [VV19]: Ne s'agit-il dès lors pas plutôt de données codées-pseudonymisées plutôt que de données anonymes ?

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 [VV20]: Cet aspect devrait être renforcé compte tenu de l'interdiction de principe des décisions individuelles automatisées.

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 [MA21]: 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 [MA22]: 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 [MA23]: « 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 [MA24]: 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 [MA25]: A clarifier pour éviter un problème de cohérence avec l'article 22 du règlement 2016/679, dans la mesure où le paragraphe 1[er] 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 [MA26]: 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.

* * *

GERMANY / ALLEMAGNE

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 [BMG27]: The second sentence goes beyond Art. 9 (1) of the General Data Protection Regulation and does not make it possible to clearly differentiate between "normal" and special personal data, because - especially in the field of Big Data - it is possible to deduce sensitive information if every-day data is combined with other data. Together with other data, the purchase of a video game, for example, could provide information on the health of the data subject. According to this definition, this would therefore have to be considered a special piece of personal information.

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.

Comment [BMG28]: All in all, IV 1.3 is very vague. Even though the guidelines are rather general, it would be desirable (in terms of applicability) to have more specific information on "data controllers", "ad hoc ethical committees" and their goals in this context.

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.

Comment [WU29]: It is necessary to state that, to protect national security, it is not necessary to carry out a risk-assessment when processing Big Data pursuant to Art. 5 (4) and Art. 8 of the Convention: Art. 9 (1) (a) provides for an exception to Articles 5 (4), 7bis (1) and 8 to protect national security. A paragraph specifying exception possibilities should be included where suitable.

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:

9) Identify the risks

10) 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

11) Provide adequate solutions by-design to mitigate these risks

12) 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 and archiving purposes in the public interest, 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

Comment [WU30]: It is necessary to state that, to protect national security, it is not necessary to carry out a risk-assessment when processing Big Data pursuant to Art. 5 (4) and Art. 8 of the Convention: Art. 9 (1) (a) provides for an exception to Articles 5 (4), 7bis (1) and 8 to protect national security. A paragraph specifying exception possibilities should be included where suitable.

Comment [WU31]: It is necessary to state that, to protect national security, it is not necessary to carry out a risk-assessment when processing Big Data pursuant to Art. 5 (4) and Art. 8 of the Convention: Art. 9 (1) (a) provides for an exception to Articles 5 (4), 7bis (1) and 8 to protect national security. A paragraph specifying exception possibilities should be included where suitable.

Comment [BMG32]: Goes beyond Art. 35 of the General Data Protection Regulation.

Comment [BMG33]: "Free and meaningful and informed consent" is a criterion that, according to data and consumer protection authorities, many applications do not meet at the moment. Explanatory texts regarding consent are too complicated and too long and are therefore rarely read in practice. Another special problem is the fact that the use of simple applications often goes hand in hand with the transmission of data and information although this is by no means necessary for the application to function and has nothing to do with the purpose of the application. This applies to health and lifestyle apps, but also to other app types. However, if all apps - or at least widely used apps or apps for which there is no alternative -impose such conditions, it is doubtful whether the users have actually given their voluntary consent. In IV 5.4 ("imbalance of power"), this problem is addressed, but should be further specified.

To make sure that, when it comes to data processing and transmission, users give their consent on a truly voluntary basis, it would be necessary to introduce a rule ...

Comment [WU34]: It is necessary to state that, to protect national security, it is not necessary to carry out a risk-assessment when processing Big Data pursuant to Art. 5 (4) and Art. 8 of the Convention: Art. 9 (1) (a) provides for an exception to Articles 5 (4), 7bis (1) and 8 to protect national security. A paragraph specifying exception possibilities should be included where suitable.

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 a~~n~~ clear imbalance of power between the data subject and the Data Controllers or Data Processors. The Data Controller shall provide proof that this clear imbalance does not exist or does not affect the consent given by the data subject.

5.5 Consent to data collection, storage, usage or transfer exceeding the degree necessary for the functioning and the specific purposes of an application must not be required for the use of any application.

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, 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 and archiving purposes in the public

Comment [BMG35]: According to Art. 35 of the General Data Protection Regulation, the data subject is not informed about the result of the risk assessment.

Comment [BMG36]: Pursuant to Article 7 (3), fourth sentence, of the General Data Protection Regulation, it must be just as easy to withdraw one's consent as it is to give one's consent.

Comment [BMG37]: Recital 43 of the General Data Protection Regulation: "clear imbalance"

Comment [WU38]: BMAS: This also applies to employment relationships.

Comment [BMG39]: Exclusion of tying arrangements is necessary, according to Art. 7 (4) of the General Data Protection Regulation in conjunction with recital 43 (proposed wording). Alternatively:

Recital 43, second sentence, of the General Data Protection Regulation: „Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on t ...

Comment [BMG40]: Not in line with the General Data Protection Regulation: The scope is limited to personal data, Art. 2 (1) of the General Data Protection Regulation. Data rendered anonymous are not ...

Comment [BMG41]: Recital 26 of the General Data Protection Regulation is more comprehensive: To ascertain whether means are reasonably likely to be used to identify the natural person, ...

Comment [WU42]: We suggest that the following paragraph be included (it is similar to recital 71 of the General Data Protection Regulation): *"In order to ensure fair and* ...

Comment [BMG43]: In the second paragraph of recital 71, the General Data Protection Regulation considers the context of data processing essential ("taking into account the specific circumstance ...

Comment [WU44]: It is necessary to add that, in the field of national security, the Convention does not contain the obligation to provide the data subject with a detailed motivation drafted by a human ...

Comment [BMG45]: According to this wording, decisions can be made solely on the basis of Big Data even if they affect individual rights. However, pursuant to Art. 22 (1) of the General Data Protection ...

interest

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 and archiving purposes in the public interest., ~~they should exclude any risk of infringement of the rights and fundamental freedoms of data subjects.~~

9.2 These ~~D~~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.

Comment [WU46]: 9.1 is not compatible with the draft Convention. It exceeds the requirements mentioned in Art. 11 of the draft when stating that exceptions "should exclude any risk of infringement of the rights and fundamental freedoms of data subjects." The requirements regarding exceptions arise directly from the Convention and are explained in 9.2-3. This phrase should therefore be deleted.

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.

PORTUGAL

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:

o) 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.

p) 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).

q) 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).

r) Personal Data: any information relating to an identified or identifiable data subject including the one used to take decisions affecting an individual belonging to a group based on group profiling information.

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

t) 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.

u) 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 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 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 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:

13) Identify the risks

14) 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

15)

Observation: What does that mean? The use of the expression "by design" can be mistaken with the idea of "privacy by design". Privacy by design solutions are to be researched and built by the Industry, not by the controllers.Somewhere in this text could be included the idea of a permanent contructive dialogue between controllers and DPAs (mainly) with the Industry geared towards the development of better personal data protection friendly technologies.

16) 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.

I do not agree. Sensitive data can, and in some very specific and justified situations must, be used in full respect for security, strict need, and other limits. This is valid either the sensitive data has been expressly collected from the data subject or with his/her express and specific informed consent OR in the cases, where it is inferred using big data or by simply using profiles. Unless one want to decide that “personal data” inferred is not personal 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.

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.

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.

THE NETHERLANDS / PAYS-BAS

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

General comment of the Netherlands:

- The purpose of the guideline should be to provide advice and to stimulate best practices to the users of Big data in order to achieve better data protection for individuals. The guidelines should not provide new norms (compared to the modernized C108) for data protection in relation to Big data. This aspect should be reviewed in the whole text (examples are given).
- A general comment, partly in relation to the first comment, is that the language of the guideline gives the impression that the guideline is legally binding. Although many of the guidelines deserve strong support, we propose that the 'shall' in the entire text be replaced by 'may', 'could' or 'should'.
- The guideline has to be in conformity with the requirements in the GDPR and the EU-Directive on data protection.
- The balance between opportunities and risks of the use of Big data could be slightly changed (described) to the advantage of the opportunities (for instance in innovation).
- Do not oblige countries to establish an ethical commission, this should be left to the Parties to C108. It is an example of a good practice (and the creation of obligations are not to be expected in a *guideline*).

I. Introduction

These guidelines take into account specific nature of Big data processing, with regard to data protection and have been drafted on the basis of the revised Convention 108.. They are primarily addressed to rule-makers, data controllers and data processors, as defined in section III.

Comment [HJ47]: This text is not about differences between parties, we think.

Comment [HJ48]: Not regulation in general, as implied by this word.

Comment [HJ49]: Please check the text against the background of the revised C108.

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:

v) 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.

w) 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).

x) 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).

y) 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.

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

aa) 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.

Comment [HJ50]: This guideline clearly goes beyond the scope of article 6 and 9 (1) of the current and the revised Convention. This guideline is therefore not acceptable.

bb) 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 should adopt a proportionate 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:

17) Identify the risks

18) 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

19) Provide adequate solutions by-design to mitigate these risks

20) Monitor the adoption and the efficacy of the solutions provided

2.6 The Risk-assessment Process should preferrably 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 archiving purposes in the public interest, scientific or historical research purposes or statistical 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 [HJ51]: We oprefer a proportionate rather than a precautionary approcah to data protection. It is important to robustly protect the rights of citizens, but it must be possible to do this without freezing innovation and responsible business use of data to create new products and services.

Comment [HJ52]: 2.3 neglects that it is according to the revised article 9(1) not necessary to carry out a risk-assessment when Big data is being processed to protect national security. Articles 5(4) and 8 of C108 are not applicable.

Comment [HJ53]: Who determines what adequate professional qualifications are, and we think this (obligatory) formulation will this bring administrative burden for SME.

Comment [HJ54]: We prefer a different wording here. It is a guideline, and ot a regulatory paper we are dealing with here. The text should not impact liability rules in the contracting Parties with C108.

Comment [HJ55]: See comment with regard to 2.3. the guideline neglects the exceptions in C108.

Comment [HJ56]: See comment with regard tio 2.3.

Comment [HJ57]: This goes clearly beyond the scope of the Convention and neglects the legitimate interest in secrecy (law enforcement, national security).

Comment [HJ58]: In conformity with the new article 9 (2) of C108 and the GDPR.

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 a clear imbalance of power between the data subject and the Data Controllers. The Data Controller shall provide proof that this clear imbalance does not exist or does not affect the consent given by the data subject.

Comment [HJ59]: The processor is not the person to be addressed, he is not responsiblebut executive.

6. Anonymization

6.1 In the Big Data context, the fact that data are being qualified as anonimous 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 [HJ60]: Since C108 does not contain specific rules on anonimisation and pseudonimisation, the guideline should not be used as an alternative instrument to add new rules to the convention. The 'shall' is not the right term here. We propose to strike this part from the guideline, and to address the issue for instance in an opinion to be taken up in T-PD.

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 significantly or produce legal effects affect individual rights, a

Comment [HJ61]: See article 22 (1) of the GDPR.

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 should 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 archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Comment [HJ62]: In conformity with the new article 9 (2) GDPR.

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 archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, they should exclude any risk of infringement of the rights and fundamental freedoms of data subjects.

Comment [HJ63]: In conformity with the new article 9 (2) GDPR.

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.

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?

* * *

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.

Comment [u64]: 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.

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.

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 [u65]: 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 [u66]: 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~~Anonymization 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.

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

Comment [A67]: 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 [u68]: (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 [u69]: It is not correct, legally speaking, to talk about anonymous data if a risk of re-identification exists.

Comment [u70]: For the same reason, it is inaccurate to talk about anonymised data. Because data are identifiable, they shall be protected against unlawful access.

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 COMITE EUROPEEN DE COOPERATION 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.

* * *

EUROPEAN COMMISSION / COMMISSION EUROPEENNE

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 Draft modernised Convention. 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 when personal data is processed in a "Big Data" context.

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

The complexity and impenetrability of Big Data applications should therefore prompt rule-makers to consider the notion of control as not circumscribed to mere individual control (). They should 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.

Comment [A71]: Which differences? What do you mean by "data protection regulation"? It would be unfortunate if these guidelines would refer to differences among the Parties, while the aim of the CoE is to achieve greater convergence between its members – as reflected, in particular, in the recently adopted draft modernised Convention 108 – based on a high level of protection of human rights and fundamental freedoms as well as a comprehensive and technologically neutral approach

Comment [A72]: Shouldn't this read better as a references to the new modernized convention (even if not yet agreed)? As they do on para 2 and in the rest of the text.

II. Scope

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

Given the nature of Big Data and of its uses, the application of some of the traditional principles of data processing (e.g. the principles of data minimization, purpose limitation, fairness and transparency and free, specific and informed 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.

Comment [A73]: Transparency ?!

The purpose of these guidelines is to define principles and practices to limit the risks for data subjects' rights related to the use of Big Data. These risks mainly concern the potential bias of data analysis, the underestimation of the social, legal and ethical implications of the use of Big Data for decision-making processes, and the limitations to an effective 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 in particular, data subjects' rights and data processing safeguards provided by the Convention and by the European Convention on Human Rights and Fundamental Freedoms.

III. Terminology used for the purpose of these guidelines:

cc) 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. In terms of personal data protection, the main issues refer precisely to the analysis of high volume and variety of data using software to extract new and 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.

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

ee) 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).

ff) Personal Data: any information relating to an identified or identifiable individual (data subject).

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

hh) 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.

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

jj) By design and by default solutions: appropriate technical and organisational measures designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of Convention 108;.

Comment [A74]: Data protection by design and default can be referred to as 'implementing appropriate technical and organisational measures ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.'

IV. Principles and guidelines

1. Ethical and socially aware use of data

1.1 The fair balance between all interests concerned shall be reflected at all stages of the processing of personal data, and in particular where information is used for predictive purposes in decision-making processes. In this case Data Controllers and Data Processors shall adequately take into account the broader ethical and social implications of Big Data while ensuring full respect of data subjects' rights and full compliance with data protection obligations as set forth by Convention 108.

1.2 Personal data processing should not be in conflict with the ethical values commonly accepted in the relevant community or communities and cannot prejudice societal values and norms, including the protection of human rights. While defining prescriptive ethical guidance may be problematic, due to the influence of contextual factors, common guiding ethical values can be found in international charters of human rights and fundamental freedoms, such as the European Convention for the Protection of Human Rights and Fundamental Freedoms, the EU Charter of Fundamental Rights or the International Covenant on Civil and Political Rights.

1.3 If the examination of the likely impact of an intended processing 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.

Comment [A75]: With whom as members?

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 Big Data and its impact on individuals and society to ensure the protection of the personal data and taking into account the rights and freedoms of the data subjects and legitimate interests of other persons concerned.

2.3 Pursuant to Article 5.1 and 2 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 protection of those rights and freedoms against 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, ethical, societal and legal 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 an examination of the likely impact of an intended processing in order to:

21) Identify and evaluate the risks of each processing activity involving Big Data and its potential negative outcome to the right to the protection of personal data.

22) Develop and provide adequate solutions by design and by default to mitigate these risks;

23) Monitor the adoption and the effectiveness of the solutions provided;

2.6 The examination of the risks of the processing shall be carried out by persons with adequate professional qualifications and knowledge to evaluate the different impacts, including the legal, organisational, social, ethical and technical 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 examination of the risks and in the design of data processing.

Comment [A76]: Who decides when fundamental rights are being affected and involvement of different stakeholders is needed?

2.8 Data controllers shall regularly review the results of the assessment of the risks.

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 examination of the risks of the processing.

2.11 The Parties may take into account where establishing the liability of Data Controllers for damage caused by the risks referred to in paragraph 2.5, of the measures implemented by Data Controllers to process Personal Data according to the provisions of this article.

3. Legitimacy of data processing and quality of data

Comment [A77]: Interchange section 2 and 3 for better understanding.

3.1 Given the transformative nature of the use of Big Data, and in order to comply with the requirement of free, specific and informed consent and the principles of purpose limitation, fairness and transparency pursuant to Article 5 of the Convention 108 and Article 5 of the Draft modernised Convention, Data Controllers should also identify the potential impact on individuals of the different uses of data.

3.2 In a context of big data analytics the principles of fairness and transparency become even more relevant. Data controllers must provide to data subjects information on the processing they are going to undertake, the rights data subjects hold, and such information must be provided in a clear manner.

Pursuant to Article 7bis. of the Draft modernised Convention, the controller shall inform data subjects of:

a. the controller's identity and habitual residence or establishment;

b. the legal basis and the purposes of the intended processing;

c. the recipients or categories of recipients of the personal data, if any; and

d. the means of exercising the rights set out in Article 9;

as well as any necessary additional information in order to ensure fair and transparent processing of the personal data. Where the personal data are not collected from the data subjects, the controller shall nonetheless not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

If data subjects are not informed in a clear manner about the processing of their personal data, they could be deprived de facto of the possibility of exercising their rights to access and rectification.

3.3 Where data gathered are further processed for archiving purposes in the public interest, scientific or historical research purposes , they shall be subject to appropriate safeguards, compatible with those purposes. In some of those 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 examination of the likely impact of an intended processing , Data Controllers and where applicable Data Processors shall adopt adequate by-design solutions at the different stages of the processing of Big Data.

4.2 Data Controllers and where applicable 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 where applicable Data Processors shall test, prior to the processing, the adequacy of the by-design solutions adopted on a limited amount of data by means of simulations. This should 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 stage.

Comment [A78]: What do you mean by 'means of simulations'? Is it expected that the solution be tested with 'test data' before it goes live or is it expected that once the solution is live, data controllers and providers run a test with a sample of real data?

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, free, specific and informed consent shall be based on the information provided to the data subject pursuant to Article 5 and Article 7bis of the Draft modernised Convention. This information shall be comprehensive of the outcome of the assessment of the risks and likely impacts on data subjects' rights and might also be provided by means of an interface which simulates the effects of the processing 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 where applicable 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 The concept of compatible use of personal data should not hamper the transparency, legal certainty, predictability or fairness of the processing. Personal data should not be further processed in a way that the data subject might consider unexpected, inappropriate or otherwise objectionable.

5.4 Consent is not freely given if there is an imbalance of power between the data subject and the Data Controllers. The Data Controller shall have the burden of 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 always exclude the application of the principles concerning data protection, due to the risk of re-identification. A set of data that, at a certain point, is not considered personal data (in the sense that it cannot be related to any identified or identifiable individual) might later on actually be linked up with a concrete person by the correlation with other sets of data.

6.2 Anonymization may combine technical measures (e.g. aggregation of data) 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, continuous and regular re-assessment of risks that takes into account new technological developments and discoveries with regard to anonymization, and the costs of implementation of the available anonymizing technologies.

6.4 Sustainable anonymization

Risk of re-identification through large data-sets in the context of big data

Comment [A79]: Further details are needed to understand how this contributes.

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

7.1 The use of Big Data shall preserve the autonomy of human intervention 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 reasoning. Big Data may be used for profiling and result in the adoption of decisions of a potentially discriminatory nature, based on automated processing. , Pursuant to Article 8 (a) of the Draft modernised Convention, data subjects have the right not to be subject to decisions significantly affecting them based solely on automated processing of data without having their views taken into consideration. Furthermore, given the recurrent use by Big Data analytics of opaque algorithms for processing data it is worth noting that Article 8 (c) of the Draft modernised Convention gives data subjects the right to obtain on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to them.

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 assessment of the risks involved in processing shall take into account the effects on re-identification of the data subject and the resulting impact on his or her rights and freedoms by 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 archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, they should exclude any recognisable 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.

INTERNATIONAL CHAMBER OF COMMERCE (ICC) / CHAMBRE INTERNATIONALE DU COMMERCE (CIC)

POLICY AND BUSINESS PRACTICES

ICC comments on Council of Europe big data guidelines

ICC is the world business organization and works to further the development of an open world economy with the firm conviction that international commercial exchanges are conducive to both greater global prosperity and peace among nations. Consisting of over six million companies, chambers of commerce and business associations in more than 130 countries, ICC has vast experience providing business expertise to policy makers and regulators in Europe and globally and holds observer status at the Council of Europe.

A number of issues in the Council of Europe *"Draft guidelines on the protection of individuals with regard to the processing of personal data in a world of big data"* have created a level of concern across ICC's membership and we thank the Council of Europe for the opportunity to share global business comments for consideration.

The Council of Europe has correctly identified the challenge of applying existing, even recently revised policies to fast changing technologies. While the focus of the Guidelines in protecting the fundamental right of privacy is laudable, the approach taken is unbalanced and may cost many of the benefits new technologies bring to foster and advance equally important and protected fundamental rights such as health. The concept of balance was effectively captured in a remark made by a French entrepreneur at an Organisation for Economic Cooperation and Development (OECD) Foresight Forum on big data: "You absolutely need to be responsible for your use of big data, but you equally must be responsible for your failure to use big data." The Council of Europe analysis of big data in the Guidelines focuses solely on the protection of privacy and does not reflect the societal benefits which may be lost by not considering more flexible methods of application of privacy protection.

There is no suggestion that effective protection of privacy should be diminished, but how privacy can be effectively protected should have some flexibility according to context and potential for societal benefit. It is therefore important that a future orientated document considers these factors. Council of Europe 108 Convention, the OECD Privacy Guidelines and other founding privacy documents consider parallel and complementary objectives: the protection of privacy and the ability to use information for societal benefit. The recent revision of the OECD Privacy Guidelines maintained the importance and currency of the foundation principles, but recognized the need for new and flexible, context-based implementation guidance of the principles in relation to new technologies and innovative uses of data.

Existing tenets of privacy may indeed be challenged by new technology. Big data analytics, especially in health, may be able to generate innovative and lifesaving solutions by analyzing data across silos and purposes of collection. Similarly more data may better inform results and lead to new correlations that can target disease or find cures. Research and insights through rich data sets can inform decision-making and improve citizens' lives with innovative services and product development. Finally re-use of historic data for new research may be essential to generate the longitudinal data sets needed for future-oriented research. These benefits challenge established models of consent, purpose specification, data minimization and data retention.

The draft guidelines could expand and highlight reference to historical, statistical and scientific purposes within research purposes. The Guidelines as drafted merely reiterate the established principles without taking into account whether there might be ways to preserve privacy while still attaining the potential societal benefits that could ensue. This dialogue is taking place beyond what the former Information and Privacy Commissioner for the Canadian province of Ontario and Executive Director of the Privacy and Big Data Institute at Ryerson University Ann Cavoukian referred to as the “Zero Sum”; the fallacious assumption that one chooses either privacy or innovation. The Council of Europe is well positioned to be a leading voice in this exploration but both sides the preservation of privacy and promotion of innovation must be considered and promoted.

The Guidelines reference ethical considerations. For the past three years discussion on societal ethics has played an increasing role in the privacy debate. Guidance on ethics in big data is being developed in many forums such as the Oxford Ethics Institute and the Information Accountability Foundation. National and international research codes of ethics are also providing ethical frameworks for carrying out market, opinion and social research. Ethics has also been a concept of long application in the health arena where ethical research protocols and ethics review boards have existed for years. Much work is being undertaken in the health arena to find ways to both protect privacy and expand the potential benefits of health research. For example, the OECD is finalizing a council recommendation supporting the joint work between the Health Committee and Committee on Digital Economy Policy and in Asia Pacific Economic Cooperation (APEC) as joint work between the Life Sciences Forum, the Electronic Commerce Steering Group and its Data Privacy Sub Group. Therefore any guidance being developed should be duly informed by this work.

The Guidelines also suggest the need for risk assessment and highlight difficulties in ensuring it is context appropriate. The Guidelines however develop a risk mitigation approach as opposed to true risk management which comprises a more comprehensive risk-benefit analysis. The former merely identifies risk and seeks to eliminate it. A more comprehensive risk benefit approach would: 1.) identify both potential risk and potential benefit, 2.) develop a management approach that would minimize risk while trying to preserve benefit and 3.) analyze residual risk to determine if it was acceptable. It is through these types of analysis that health professionals have made decisions about accessing data to prevent the breakout of epidemics etc. The current guidelines should adopt such a broader analysis. This would also be a step towards preserving beneficial applications and guarantee that care is taken across mitigation strategies to confirm that the avenue chosen is effective, while assuring least harm to beneficial societal uses of big data.

The Guidelines also highlight the need for greater transparency in big data analytics and their potential for negative consequences to individuals. There is no question that this is an important topic that needs to be addressed. ICC welcomes the recognition that these technologies may be of great importance to business and may be highly confidential and proprietary. The current phrasing of “secret to the extent protected by law” is not broad enough to cover these technologies as some are protected in a contract or using trade secrets protection which is less uniformly recognized. ICC suggests that the ability of authorities to access the protected data should be further qualified with requirements of notification, necessity, and obligations to protect the security and confidentiality of the information that are consistent with their established investigative and enforcement functions.

The specifics related to consent and other established privacy principles, should continue to validate the relevance of those principles, but encourage continued dialogue on innovative solutions that can preserve privacy and while still allowing uses of technology to create substantial societal benefit.

ICC remains available to work with the Council of Europe as it continues to define practical, optimally effective guidance on the protection personal data and reap the full societal benefits of big data.

About The International Chamber of Commerce (ICC)

The International Chamber of Commerce (ICC) is the world's largest business organization with a network of over 6.5 million members in more than 130 countries. We work to promote international trade, responsible business conduct and a global approach to regulation through a unique mix of advocacy and standard setting activities—together with market-leading dispute resolution services. Our members include many of the world's largest companies, SMEs, business associations and local chambers of commerce.

www.iccwbo.org

@iccwbo