COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Strasbourg, 16 May 2016 T-PD-BUR(2015)12Rev

BUREAU OF THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(T-PD-BUR)

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

Directorate General of Human Rights and Rule of Law

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.

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.

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.