



Strasbourg, 19 November / 19 novembre 2018

T-PD(2018)23Bil

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

**COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION
DES PERSONNES A L'EGARD DU TRAITEMENT AUTOMATISÉ
DES DONNÉES A CARACTÈRE PERSONNEL**

**COMPILATION OF COMMENTS ON THE DRAFT GUIDELINES ON ARTIFICIAL
INTELLIGENCE**

**COMPILATION DES COMMENTAIRES SUR LE PROJET DE LIGNES DIRECTRICES
SUR L'INTELLIGENCE ARTIFICIELLE**

Directorate General of Human Rights and the Rule of Law /

Direction Générale droits de l'Homme et Etat de droit

TABLE DES MATIERES

ESTONIA / ESTONIE	2
GERMANY / ALLEMAGNE	3
ITALY / ITALIE	5
LATVIA / LETTONIE	6
PORTUGAL / PORTUGAL	7
SWITZERLAND / SUISSE	8

ESTONIA / ESTONIE

We kindly submit for consideration the following in the Draft Guidelines on Artificial Intelligence regarding III. Guidance for policy makers 5. When AI applications may significantly impact on the rights and fundamental freedoms of data subjects, data controllers should consult the supervisory authorities to seek advice to mitigate this potential adverse impact.

We propose to the Committee to engage supervisory authorities in seeking for advice prior to the processing where a data-protection impact assessment indicates that processing operations may have significant impact on the rights and fundamental freedoms of data subjects which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation.

GERMANY / ALLEMAGNE

The present Guidelines provide a set of baseline measures which governments, AI developers, AI manufacturers, and AI service providers should follow to secure the human dignity and the human rights and fundamental freedoms of every individual, in particular with regard to personal data protection.¹

Nothing in the present Guidelines shall be interpreted as precluding or limiting the provisions of the European Convention on Human Rights and of Convention 108 as amended ("Convention 108+")².

I. General guidance

1. Responsibility towards individuals and society is the corollary of any AI development, taking the safeguard of fundamental rights as an absolute pre-requisite.
2. A fundamental rights-oriented perspective is to be adopted by AI development and AI applications, in particular when AI is used in the context of decision-making processes.
3. AI development relying on personal data must be based on the principles of Convention 108+. The key elements of this approach are: proportionality of data processing, responsibility, transparency and risk management.
4. A risk-aware approach is not a barrier to innovation, but a helpful and useful tool. The risks of datafication and the potentially adverse implications of data-driven solutions should be considered.
5. Individuals and communities should have the right to freely decide what role AI should play in analysing collective behaviour, influencing social dynamics, and in decision-making processes affecting entire groups of individuals.
6. In line with the guidance on risk assessment provided in the Guidelines on Big Data³, a wider view of the possible outcomes of data processing should be adopted to consider the impact of data use not only on fundamental rights but also on collective social and ethical values.
7. AI development and AI applications shall ensure full respect of the rights of data subjects enshrined in Convention 108.

II. Guidance for AI developers

1. The Committee of Convention 108 encourages AI developers to adopt a value-oriented design of their products and services, consistent with Convention 108+ and other relevant instruments of the Council of Europe.
2. AI developers have to assess the adverse consequences of AI applications on the fundamental rights and freedoms of data subjects. Considering such consequences, precautionary approach based on risk prevention policies have to be adopted.
3. AI developers have to adopt a by-design approach to avoid potential unintentional and hidden data biases, and the risk of discrimination or negative impacts on the rights and fundamental freedoms of data subjects, in all phases of the processing, including data collection and analysis stages.
4. In developing AI applications, it is important to adopt a design paradigm that critically assesses the nature and amount of data used. Such design paradigms aim at reducing redundant or marginal

¹ These Guidelines derive from and are built upon the Report on Artificial Intelligence ("Artificial Intelligence and Data Protection: Challenges and Possible Remedies") available at ...

² Amending Protocol CETS n°223 to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

³ Guidelines on big data adopted by the Committee of Convention 108 in January 2017, available at <https://rm.coe.int/CoERMPublicCommnSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a>.

data, starting with a restricted amount of training data, and then monitoring the model's accuracy as it is fed with new data. The use of synthetic data can be considered as one of the possible solutions to minimise personal data processed.

5. The risk of de-contextualised data (i.e. ignoring the contextual information characterising the specific situations where the proposed AI-based solutions should be applied) and de-contextualised algorithmic models (i.e. using AI models originally designed for different contexts or purposes) should be adequately considered in developing AI applications.
6. Committees of experts from a range of fields, as well as independent academic institutions, should be involved in AI development to provide a valuable support in designing rights-based and socially-oriented AI and to contribute to detect potential bias. Such committees play an important role in all areas where the respect for fundamental rights and freedoms is crucial, such as for instance AI designed to be used in a judicial or law enforcement context.
7. Participatory forms of risk assessment, based on the active engagement of the groups potentially affected by AI applications, should be considered.
8. Where technically feasible, AI developers should design their products and services in a manner that safeguards users' freedom of choice over the use of AI and provide alternatives to AI-equipped devices and services.
9. Data subjects are entitled to know the AI applications used and to obtain meaningful information about the logic involved in AI data processing operations, including the consequences of such a reasoning.

III. Guidance for policy makers

1. Public procurement procedures could impose specific duties of transparency and prior assessment of AI systems to service providers. Nevertheless, these duties must be in compliance with the requirement of an adequate protection of business secrets.
2. Trust of the public in AI products and services could be enhanced by increased AI developers' accountability and the adoption of risk assessment procedures.
3. Data protection supervisory authorities and data controllers should adopt forms of algorithm vigilance to better ensure compliance with data protection and human rights principles over the entire lifetime of AI applications.
4. Overconfidence in the reliable nature of the solutions provided by AI systems, and fears of potential liability when taking a different decision than the one suggested by AI systems risk altering the autonomy of human intervention in decision-making processes. It is thus crucial that the freedom of human decision makers not to rely on the result of the recommendations provided using AI be preserved.
5. When AI applications may significantly impact on the rights and fundamental freedoms of data subjects, data controllers should consult the supervisory authorities to seek advice to mitigate this potential adverse impact.
6. Countries having established independent bodies supervising specific sectors where AI applications operate or may operate, should strengthen the mutual cooperation between these bodies and their cooperation with data protection supervisory authorities.
- 7.

ITALY / ITALIE

On the first part "General Guidance": the suggestion is to add a last principle stating that " A.I. systems must allow users to have constant control over the purposes and related effects both on a collective and individual level"

On the last part "Guidance for Policy makers", here too, the suggestion is to add a final principle stating that " the adoption of international standards on ethics and respect of rights, freedoms and self-determination of individuals in developing AI applications should be promoted and enforced"

LATVIA / LETTONIE

The Data State Inspectorate of Latvia (further -the Inspectorate) welcomes the efforts made by Consultative Committee of the Convention 108 with regard to the draft Guidelines on Artificial intelligence that is due to be discussed and approved during the Plenary meeting of the Committee in Strasbourg, 20-22 November 2018. The Data State Inspectorate of Latvia has also noted your request to send our comments on Draft Guidelines on Artificial intelligence.

However, the Inspectorate has some concerns arising from the **Chapter III Guidance for policy makers, point No.3**, it states: *“Data protection supervisory authorities and data controllers should adopt forms of algorithm vigilance to better ensure compliance with data protection and human rights principles over the entire lifetime of AI applications”*.

As the abovementioned applies directly to the data supervisory authority, the clarification is required regarding the meaning “should adopt forms of algorithm vigilance”. According to the functions of the Inspectorate, we are not sure whether the notion “adopt forms of algorithm vigilance ” includes some other activities, or new obligations to be provided that are probably not in the scope of the Inspectorat’s actual functions, and which requires specific means or procedures to take in the future in a view to ensure that these forms of algorithm vigilance are in compliance with data protection requirements.

PORTUGAL / PORTUGAL

Main findings and policy suggestions

- AI development and AI applications must adopt a fundamental rights-oriented perspective
 - Responsibility towards individuals and society is the primary goal in AI development
 - A risk-aware approach is no a barrier to innovation, but an enabler. Governments and citizens should therefore consider the risks of datafication and the potentially adverse implications of data-driven solutions.
 - Data-centric AI development must be based on the principles of Convention 108. The key elements of this approach are: proportionality of data processing, responsibility, transparency, risk management, and participation.
 - Individuals and communities should have the right to freely decide what role AI should play in shaping social dynamics, collective behaviour, and decisions affecting entire groups of individuals.
 - A wider view of the possible outcomes of data processing in AI should be adopted to consider the impact of data use not only on fundamental rights but also on collective social and ethical values.
-
- In developing AI applications is important to adopt a design paradigm that critically assesses the nature and amount of data used.
 - AI developers should adopt a by-design approach to avoid potential hidden data biases and the risk of discrimination or negative impacts on the rights and fundamental freedoms of data subjects, both with regard to the collection and analysis stages
 - In developing and using AI applications the risk of de-contextualised data and de-contextualised algorithmic models should be adequately considered.
 - Committees of experts from a range of fields should be involved in AI development and use, to provide a valuable support in designing rights-based and socially-oriented algorithms.
 - Participatory forms of risk assessment, based on the active engagement of the groups potentially affected by AI applications, should be adopted.
 - AI solutions should preserve the autonomy of human intervention in decision-making processes and the freedom of human decision makers not to rely on the result of the recommendations provided using AI.
-
- Public procurement procedures could impose specific duties of transparency and prior assessment of AI systems to service providers.
 - Public trust in AI products and services could benefit from an increased AI developers' accountability and the adoption of risk assessment procedures.
 - Supervisory authorities and data controllers should adopt forms of algorithm vigilance to better ensure compliance with data protection and human rights principles over the entire lifetime of AI applications.

SWITZERLAND / SUISSE

Au point I.1., je propose la formulation suivante : “ ... taking the safeguard of human rights and fundamental freedoms, and in particular the rights to dignity and privacy as an absolute pre-requisite.”

Au point I.3., ne doit-on pas plutôt parler d' « accountability » que de « responsibility » ?

Au point I.5, postule-t-on vraiment un droit ou vise-t-on plutôt une injonction à associer les personnes et les groupements (la société civile) à participe au débat sur le recours à l'IA.

Au point I.6, remplacer « fundamental rights » par « human rights and fundamental freedoms ».

Au point I.7, remplacer « cannot » par “shall not”

Au point II.2, remplacer “fundamental rights and freedoms of data subjects” par “human rights and fundamental freedoms, in particular the rights to dignity and privacy of data subjects”

Au point II.4, je suggère de définir dans une note de bas de pas l'expression « synthetic data ».

Au point II.6, de quels comités d'experts parle-t-on ? Ne s'agit-il pas plutôt de comités d'éthique, lesquels devraient être indépendants ?

Au point II.7, ce point est probablement à mettre en relation avec le point I.5. Dans ce cas, il faudrait remplacer « groups » par « individuals and communities »

Au point II.9, ce point devrait être complété ou précédé par une principe selon lequel les personnes concernées doivent être informées qu'elles interagissent avec une application d'IA. It should be recommended/required to make AI-based interactions recognizable to humans. For example, the person chatting with a bot (audio or texting) should be informed about the AI-aspect of his communication. Voir aussi, le § 3.d. et 3.e. de la déclaration de Bruxelles du 23 octobre de la Conférence des commissaires à la protection des données et à la vie privée sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle.

Je propose de rajouter un point II.10 étendant le droit d'opposition de l'art. 9.1.d. Convention 108+ . Toute personne concernée devrait pouvoir s'opposer aux technologies qui ont une influence sur ses opinions et son développement personnel. Ce droit est à mettre aussi en lien avec le droit de ne pas être soumis à une décision automatisée.

Au chapitre III. Guidance for policy makers,

Je propose de rajouter une point concernant la sensibilisation et la formation / l'éducation, voir § 2.c. de la déclaration de Bruxelles du 23 octobre de la Conférence des commissaires à la protection des données et à la vie privée sur l'éthique et la protection des données dans le secteur de l'intelligence artificielle.

Au point III.1, la transparence doit aussi viser les algorithmes. En outre l'assesment / vérifiabilité des systèmes I.A, y.c. des algorithmes doit se faire non seulement préalablement, mais également ultérieurement de manière périodique.

Au point III. 5, ajouter “human” avant “rights and fundamental freedoms”.