Strasbourg, 27 September / septembre 2021 T-PD-BUR(2021)2rev2MOS

**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
À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL**

***

Compilation of Comments on Draft Guidelines on Digital Identity

Compilation des commentaires sur le Projet des Lignes directrices relatives à l'Identité numérique

TABLE OF CONTENT / TABLE DES MATIERES

GERMANY / ALLEMAGNE

Digital Identity

3. Principles for the protection of personal data and fundamental rights and freedoms – human dignity

When considering the processing of personal data for fulfilling the objectives of NIDS, it is crucial to reflect on the Preamble to Convention 108+ and the necessity to "*secure the human dignity and the protection of the human rights and fundamental freedoms of every individual*~~begin with Article 1 of Convention 108+ and that requires **respect** for an individual's **human rights** and **fundamental freedoms** and in particular their **right to privacy**.~~." ~~Of equal importance is the~~The Preamble in the Explanatory Report ~~–~~to Convention 108+ ~~which~~ further states that "***human dignity*** *requires that safeguards be put in place when processing personal data, in order for individuals* ***not to be treated as mere objects***."[1] Because of their unchangeable nature the increasing incorporation of biometrics into NIDS, carries the risk of making people and their actions too easy to record, which could pose a threat to their rights and freedoms. ~~The increasing incorporation of biometrics into NIDS, making people machine readable carries the risk of reducing people to an object removed from considerations of human dignity and other adverse effects on their rights and freedoms.~~

3.2 Fairness and Transparency

Article 5(4)(a) and (b) and Article 8 of Convention 108+ require that ~~the processing of an individual's~~ data about individual is ~~done~~ processed in a manner that is fair and transparent to individuals.

~~. Fairness and transparency are also necessary to ensure the legitimacy of processing.~~

~~The legitimacy of processing of personal data and special categories of personal data is dependent not only NIDS being laid down in law, but also~~This includes not only ~~-~~ensuring that the scope and purpose of ~~such~~ NIDS law is foreseeable and accessible, but also ~~. It is also dependent on ensuring that the processing of data is transparent and fair to individuals and groups to which individuals may be a part of, and that appropriate safeguards are established to ensure respect for, and the protection of, the rights and freedoms of individuals *and* groups impacted by NIDS.~~

that ~~i~~Individuals ~~-~~data subjects ~~and groups~~ must be informed in a concise, transparent, intelligible and easily accessible form so that they are able to clearly understand:

[1] Convention 108+, Explanatory Report, Preamble, Paragraph 9, Page 16 https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Commented [A1]: General remark:
The Guidelines should be streamlined further. The use of citations and certain sources should be reviewed taking into account the nature of "guidelines".

Furthermore, the scope of the Guidelines should be discussed as it goes beyond data protection principles in quite a few instances.

It might be helpful to identify different use cases as it makes quite a difference who (private entities or the government) uses what categories of data.

Commented [A2]: We suggest a different wording as it is rather drastic for Guidelines. While the increasing incorporation of biometrics has more risks, it's purpose is not to "make people machine readable".

Commented [A3]: What is meant by groups? Isn't it all about data subjects?

Commented [A4]: It might be useful to differentiate between what data subjects must be informed on according to Conv. 108+ and what they should be informed on but that goes beyond the scope of the convention.

- what personal data and special categories of personal data such as biometric data will be processed and for what explicit and specific purposes.

(...)

- whether the provision of data to establish a national digital identity is voluntary or mandatory, and the consequences of not providing data to establish a national digital identity (NID).

(...)

- whether ~~national digital identity (~~NID~~)~~ data, such as a national identification number (NIN), will be shared with or accessible to other national identity dependent schemes or be required for such schemes and why. For example, whether national identity will be required to obtain a mobile sim card or to access education or healthcare services and what national identity data will be recorded as a result.
- whether a NIN will be bound to other unique identifiers (and the lawful bass for this) such as a mobile phone number, a mobile sim card electronic identity number,[2] or electronic equipment number of a mobile phone,[3] for example ~~and which may facilitate State interference with human rights such as the right to freedom of movement and association or the right to freedom of expression for.~~

(...)

One way to further ensure full transparency on the use of the NID data or a NIN could be the implementation of new digital tools, like a data cockpit that shows all transmission relying on either the NID data or a NIN. Such a data cockpit could be made easily accessible for the individual via digital means and would also be fairly easy to implement by the policy maker, since it would only reuse the already established digital infrastructure by the NID / NIN itself.

Commented [A5]: This section concerns the information necessary for the data subject to understand and not certain dangers.

Commented [A6]:

3.3 Specific and legitimate purpose(s) and purpose limitation

Prior to the implementation of NIDS, it is important that national policy and law on NIDS explicitly ~~define~~ specify the legitimate and permitted purposes for which personal data and special categories of data (such as biometric data) ~~are *n*~~*and the categories of data that*~~*ecessary*~~can be processed ~~and the precise data deemed *necessary* to fulfil those purposes.~~ This is necessary to meet the ~~requirement~~ conditions for legitimate processing and purpose limitation of Article 5(4)(b) of Convention 108+ and to prevent data being processed for imprecise or vague or incompatible purposes. It is ~~and~~ also necessary to meet the design obligations contained in Article 10 of Convention 108+.[4]

Commented [A7]:

[2] For example the international mobile subscriber identity (IMSI) that uniquely identifies every SIM card on a mobile network https://en.wikipedia.org/wiki/International_mobile_subscriber_identity

[3] For example, the International Mobile Equipment Identity number (IMEI) that uniquely identifies a mobile phone on a mobile network https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

[4] Paragraph 89 of the Explanatory Report to Convention 108+ Article 10 – Additional Obligations, requires "that data protection requirements are integrated as early as possible, that is, ideally at the stage of architecture and system design, in data processing operations through technical and organisational measures (data protection by design)."

(…)

In accordance with the principles of legitimacy, fairness and transparency personal data and special categories of personal data processed under NIDS, should not be processed in a way that would be unexpected, ~~inappropriate~~inappropriate, or otherwise objectionable by data subjects. Laws establishing such data processing should be~~Any processing that has such consequences must be clearly established in law and~~ subject to assessment of any potential adverse impact on the human rights of individuals and groups.

The secondary use of national identification numbers and other data collected for the purposes of national digital identity should be prohibited except for purposes clearly provided for in law.

Commented [A8]: Any law must also follow these principles

Commented [A9]: This could be clarified: What is meant by this? The data processed for establishing an identity? The use of the identity? By companies? By the state?

3.4 Data Quality – Accurate, adequate, relevant and not excessive

Accurate

(…)

Ensuring the accuracy of data processed in NIDS is crucial. This is especially so when NIDS require the registration of biometrics~~. and where~~a B~~b~~iometric data may link to other identity-based systems such as facial recognition where – depending on the use – errors might have serious consequences for the individuals concerned~~.~~ Or where NIDS may deny individuals access to crucial services such as mobile connectivity, or health care or education, or migration because of inaccurately recorded data.

Commented [A10]:

(…)

Adequate, relevant and not excessive (data minimisation)

Only the minimum data necessary must be processed to fulfil an identified and legitimate specific purpose or purposes. To achieve this~~, s above, you~~ the ~~must first define the purpose, and~~purpose must first be defined and ~~and ensure~~ an appropriate legitimate basis must be ensured– which for NIDS should be specified in law.

Commented [A11]:

3.5 Data Retention

(…)

~~as~~ Data ~~long as necessary to fulfil a specific justified and legitimate purpose and~~ should be deleted or rendered anonymous when the specific purpose of processing has been achieved ~~and/or the data are no longer required~~. This must include consideration of data processed in systems ~~integrated~~ that are integrated ~~into~~ with NIDS or ~~on which~~that NIDS draw data from

Commented [A12]: This may be one situation in which personal data must be erased. But what about other constellations such as legal obligations, the objection of a data subject, etc..?

Commented [A13]: This criterion is completely vague and should be deleted. Rather, personal data should be deleted as soon as the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed.

(see also wording of Art. 5 lit. e) of modernized Convention: *"preserved in a form which permits identification of data subjects* ***for no longer than is necessary for the purposes for which those data are processed****.")*

~~depend or that otherwise depend on NIDS~~. For example, facial recognition systems or mandatory SIM registration systems or border control systems.

3.6 Security of processing

(…)

It is vital that controllers ~~ensure~~ implement appropriate ~~*appropriate*~~ *technical* and *organisational* measures ~~are implemented~~ to ~~protect~~ safeguard data ~~held~~ and the fundamental rights and freedoms of individuals~~in national identity systems and other identity related systems they interconnect to~~. A lack of appropriate security constitutes an unlawful data processing and may, for example, lead the theft and/or unauthorised access to or disclosure of data. This may lead to harms such as harassment, persecution, fraud or identity impersonation. It is also important to consider that once compromised – stolen for example - biometric data cannot be replaced, or that stolen biometric templates can be repurposed.

~~A compromise of one system may compromise others.~~

'Appropriate' measures' ~~security~~include:

- ensuring ~~data minimisation~~ in the design and operation of systems, that, by default, only personal data which are necessary for each specific purpose of the processing are processed. ~~— you should process only the minimum data necessary to achieve a specific and legitimate purpose~~. Consider that if you do not collect data then it cannot be compromised or be used to compromise an individual's fundamental rights and freedoms.

(...)

3.7 Profiling and automated decisions making

(...)

Profiling (including automated decisions) should be prohibited within national digital identity systems and associated systems, unless expressly provided for in law. Any such permitted purposes should be subject to an obligation to conduct a prior human rights impact assessment. Individuals should also be given rights over profiling and automated decision making, and any exceptions to such rights must be clearly determined in accordance with Article 11 of Convention108+. Article 11 requires that exceptions must be provided for by law (that is accessible and foreseeable) and that must respect the essence of fundamental rights and freedoms, and pursue a legitimate aim considered a necessary and proportionate measure in a democratic society.

Commented [A14]: To underline, that the issue of data security is a precondition for the lawful processing of personal data.

Commented [A15]: This is a core data protection principle which should not be listed here since it is not particularly linked with the issue of data security and must be guaranteed at any time – regardless of the nature, scope and context of processing.

Additionally, some rather editorial changes

Commented [A16]: This part seems to contradict the previous statement of the UK Information Commissioner's Office

3.8 Human Rights by Design and Human Rights Impact Assessments

(…)

Human Rights Impact Assessments and Human Rights by Design

Commented [A17]: This section should be further discussed with the Bureau as this goes beyond the scope of the Convention and criticizes an DPIA as insufficient.

3.9 Accountability

(...)

However, a human rights based approach extends the principle of accountability beyond the obligation to demonstrate compliance with data protection principles to regulators, but to ensure accountability in a transparent manner, throughout key stages of NIDS, beginning with the development of policy, to stakeholder engagement, to the development of law, through to the conduct of HRIAs and to designing for human rights in NIDS.[5]

Commented [A18]: See above

3.10 Right of individuals

(…)

Subject to *limitations set out in law*, the rights of individuals include:

(...)

- the right to access their personal data and to obtain a copy of personal data being processed, free of charge and ~~at reasonable intervals~~ the right to have inaccurate data corrected (free of charge)
- the right to have their data erased (free of charge) where the processing of their data is contrary to the provisions of applicable data protection law/national digital identity law
- the right to restrict the processing of their data
- the right to object to the processing of their personal data
- the right not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration ~~to profiling and/or automated decision making except where clearly provided for in national digital identity law~~
- the right to lodge a complaint with a supervisory authority
- the right to judicial and non-judicial remedies (as provided by Article 12 of Convention 108+)

Commented [A19]: According to Art. 9 lit.e) of Convention 108+, this is not a precondition and should be deleted.

Commented [A20]: See wording Art. 9 lit. a) Convention 108+

[5] See footnote 64 and

4. Recommendations for policy and decision- ~~policy~~ makers

(...)

Policy makers and decision makers should:

(...)

- ensure that the adoption of appropriate safeguards is a requirement in policy and law including that special categories of data require additional safeguards
- consider the implementation of digital transparency tools

Commented [A21]:

(...)

5. Recommendations for controllers

(...)

Controllers should:

- establish an appropriate governance framework and assign responsibilities for data protection, privacy and human rights
- consider appointing a data protection officer with appropriate, knowledge and understanding
- ensure appropriate staff are adequately trained in data protection and privacy and the impact of the collection and use of data on broader human rights[6]
- adopt effective policies and measures to ensure data are processed only on an appropriate legal basis, and to ensure transparency, data quality and other key data protection principles and that individuals are provided with all the relevant information, including ~~made aware of~~ their rights so that they ~~and~~ can easily exercise them

Commented [A22]: Insertion

(...)

[6] The Council of Europe HELP course on Data Protection and Privacy Rights provides a good introduction https://rm.coe.int/help-course-brief-data-protection-and-privacy-rights/16809cd3a7

UNITED KINGDOM : ICO / ROYAUME-UNI: ICO

3. Principles for the protection of personal data and fundamental rights and freedoms – human dignity

3.6 Security of processing

(…)

It is vital that controllers implement appropriate *technical* and *organisational* measures to safeguard data and the fundamental rights and freedoms of individuals. A lack of appropriate security may, for example, lead the theft and/or unauthorised access to or disclosure of data. This may lead to harms such as harassment, persecution, fraud or identity impersonation. It is also important to consider that once compromised – stolen for example - biometric data cannot be replaced, or that stolen biometric templates can be repurposed.

'Appropriate measures' include:

- ensuring data minimisation in the design and operation of systems – you should process only the minimum data necessary to achieve a specific and legitimate purpose. Consider that if you do not collect data then it cannot be compromised or be used to compromise an individual's fundamental rights and freedoms.
- assessing the sensitivity of the data involved and the potential adverse consequences for individuals and groups and adopting measures to mitigate possible risks to individuals.

Commented [A23]: "may include"

3.8 Human Rights by Design and Human Rights Impact Assessments

(...)

As discussed previously, NIDS may be a combination of public and private arrangements and technologies. Pursuant to the recommendation of the Committee of Ministers of the Council of Europe[7] parties to Convention108+ should require businesses to "*apply and carry our human rights due diligence ... including project-specific human rights impact assessments, as appropriate …*" The obligation to carry out diligence and human rights impact assessments applies equally to the public sector when considering the adoption of NIDS.

Commented [A24]: We'd suggest keeping the previous wording 'encourage or require' which is closer to the Recommendation's text.

Commented [A25]: I am not sure we can use the word 'obligation'. We could stick to the wording of the Recommendation and use *'requirement to carry out human rights due diligence as appropriate as contained in the afore-mentioned Recommendation'*.

(...)

[7] Council of Europe. Recommendation CM/Rec (2016)3 of the Committee of Ministers to member States on human rights and business https://rm.coe.int/human-rights-and-business-recommendation-cm-rec-2016-3-of-the-committe/16806f2032

Stakeholder engagement

(…)

This guidance suggests that the following key stakeholders are crucial to consult in the context of national digital identity schemes. It is not an exhaustive list of stakeholders but includes:

- **Government**
  - Key government departments, agencies and ministries with responsibility for:
    - Information Communications Technology
    - Digital Agenda and Economy
    - Health Care
    - Education
    - Birth registration/civil population registration
    - National Identity
    - Border Control and Immigration
    - National Security and Law Enforcement
    - Social Protection
    - Indigenous Affairs
    - Refugees
    - Procurement
    - Data Protection
    - Human Rights

Commented [A26]: A lesser point: We wonder whether this list could be summarised in the main body of the Guidelines and whether the full list would best be moved to an annex.

Human Rights Impact Assessments and Human Rights by Design

Data protection frameworks such as Convention108+ or the GDPR, require consideration of risks to the interests, ~~rights~~rights, and fundamental freedoms of individuals and to safeguard against such risks ~~to these~~, through a range of ~~governance~~ measures ~~and design~~, including conducting a data protection impact assessment (DPIA) that focusses on 'risk' processing operations. But such frameworks may not sufficiently ~~elaborate~~ identify~~on~~ what those~~those~~ interests, rights and freedoms are in practice and restrict assessments to what is defined and articulated in law ~~or the circumstances in which risks may materialise and harms occur~~.

~~These guidelines~~Drawing on the concept of a DPIA these guidelines adopt ~~a~~ the more inclusive term of Human Rights Impact Assessment ('HRIA). F~~, that f~~rom the outset term HRIA forces thinking beyond rules-based data protection compliance to consideration of rights ~~beyond privacy~~ that may be impacted by NIDS, that need to be designed for (in policy, technology and practice). A HRIA is a more human centred approach that puts individuals and communities, and their needs, concerns, and perceived risks at its centre .

(…)

Commented [A27]: We'd really recommend to remove all passages that criticise DPIAs. If the author wants to promote HRIAs then this is a decision to take by the whole Committee. But we see the risk that this passage criticises DPIAs or even the remit itself of privacy law.

We would simply propose to delete this sentence ('*But… in law*') as we think it could lead to confusion.

Commented [A28]: As mentioned above, we believe this text as drafted may risk being misunderstood and present a reductive view of the objectives and purpose of DP law.

DP law, as described in Article 1 C108+ but also UK GDPR considers fundamental rights and freedoms (for example when considering sensitive/special data, risks of harms to individuals, rights and remedies). This is also recognised in the 1st sentence of this paragraph.

The Committee can promote the use of HRIAs as it sees fit. However, we are concerned that the current approach risks putting DP law in a less positive light without wanting to do so.

In conclusion: we suggest deleting this addition '*thinking.. compliance to'* as well as remove 'beyond privacy' in the same sentence in keeping with the comments above (2nd deletion made in the text for clarity).

Commented [A29]: Same as before – suggest deleting 'more'.

A HRIA approach forces policy makers and controllers to ~~think beyond rules based 'data protection' requirements to considerations of~~consider whether a programme may exclude categories of ~~individuals, or~~individuals or lead to discrimination for example. A HRIA at the policy level alone can assist in assessing the proportionality of a proposal. For example, whether a perceived benefit to be gained is outweighed by the severity of the harm to individuals and subsequently the legitimacy of the processing.[8] A DPIA approach does not require nor facilitate such an approach. As Mantelero argues, "*A human rights-centred assessment ... offers a better answer to the demand for a more comprehensive assessment, including not only data protection … but also the effects of data use on other fundamental rights and freedoms*."[9]

4. Recommendations for policy and decision- ~~policy~~ makers

Policy makers, whether members of parliament, legislators or government officials or policy advisors have a vital role to play in setting societal values and legal approaches and standards that should apply to national identity schemes.

Policy makers and decision makers should:

(…)

- establish an independent oversight function with powers of audit and corrective enforcement measures

5. Recommendations for controllers

(...)

Controllers should:

(...)

- develop and adopt human rights impact assessment and human rights by design methodology, building on, but going beyond, data protection impact assessments. to ensure for example, that individuals do not experience exclusion or discrimination

6. Recommendations for the identity industry – manufacturers, service providers and developers

A movement and industry has emerged that promotes 'legal identity' as a fundamental human right.[10] Manufacturers of equipment, providers of services and developers of software used in national identity systems should seek to meet key data protection principles of Convention 108+ to ensure respect for an individual's human rights and freedoms. Identity industry entities may be impacted by virtue that the controllers and processors who they provide equipment and services to,

[8] See for example, considerations of benefit versus harm deliberated in the Supreme Court of Jamaica ruing in Robinson – v- The Attorney General of Jamaica and the Jamaica Digital ID programme and test of proportionality and legitimacy of processing https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

[9] See footnote 58

[10] Thales 'Legal identity, a fundamental human right'. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/legal-identity

Commented [A30]: We would like to see the deletion of the sentence '*A DPIA approach does not require nor facilitate such an approach'.*

DPIAs are a useful tool in many situations including digital identity and so we'd prefer to delete negative commentary.

This is how ICO Guidance currently reads for DPIAs which are mandatory in certain circumstances as per the UK GDPR (and the approach holds true for many other parties, we believe):
[A] DPIA must:
•*describe the nature, scope, context and purposes of the processing;*
•*assess necessity,* ***proportionality*** *and compliance measures;*

Commented [A31]: I am not sure what is meant by this?

Commented [A32]: ICO Guidance reads that these exercises (DPIAs and other assessments – these could include human rights IAs) can be combined, so long as the final assessment encompasses all the requirements of a DPIA. [We think this point is implied so far but it is important to make it clearer]

So we ask to add this here:

Where a DPIA is legally required the final assessment should in any case encompass all the requirements of a DPIA.

Commented [A33]: Lesser point: Think this is meant to read 'within industry'.
I am not sure what this sentence leads us to conclude and wonder whether we should focus on the next sentences.

are required to comply with applicable data protection law – and are obligated to design the processing of data in ways that considers and prevents or minimises risks to the human rights and freedoms of individuals. Or such entities may themselves process data to test hardware and software for example.

7. Recommendations for Supervisory Data Protection Authorities

(…)

SAs should consider building on data protection and privacy impact assessment approaches to create a human rights impact assessment methodology. A HRIA approach moves beyond a data protection compliance mindset, to include stakeholder engagement and participation in considering the interests of individuals and groups that data protection law and DPIAs do not make provision for. A HRIA also helps to identify concerns and needs and perceived risks of rights holders that a DPIA does not address.

(…)

8. Glossary

(…)

HRIA: means a human rights impact assessment. A process by which NIDS – from a policy proposal, to draft law, to its implementation and operation – are assessed for potential adverse effects on rights holders as individuals and communities.

Commented [A34]: Guidelines often choose one term either 'Data Protection Authorities' or 'Supervisory Authorities'

Commented [A35]: The DPA's competence lies in the data protection area (rather than encompassing all human rights).

Commented [A36]: Here I am suggesting to add 'In the context of these Guidelines….'. Otherwise in my understanding of this, this could be read as meaning that any HRIA is specific to digital identity.