Strasbourg, 19 October / octobre 2020 T-PD(2021)2rev3Mos

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 AUTOMATISÉDES DONNÉES A 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

T-PD(2021)2rev3Mos

TABLE OF CONTENTS / TABLE DES MATIERES

ITALY / ITALIE

1. Introduction

(…)

While ~~a national digital identity scheme~~NIDS may bring significant benefits and protections in multiple contexts, and allow individuals to obtain and assert important rights, ~~it~~ they may also have adverse consequences for individuals *and* groups. These consequences can range from discrimination and exclusion to marginalisation, to unwarranted profiling and surveillance, to a person's loss of control over their identity or the presentation of their identity by others. It follows, therefore, that NIDS should ~~follow~~ take a human ~~rights based~~rights-based approach built on human rights by design and that incorporates assessments of the impact on human rights that includes and goes beyond privacy and personal data protection ~~and privacy~~. Human rights values should underpin NID~~S~~s.

(…)

Those whom national digital identity schemes are meant to serve have a right to expect that such schemes will respect and safeguard their human rights and fundamental freedoms, and in particular the right to privacy pursuant to Article 8 of the European Convention of Human Rights and case law.[1] And as Judge Sykes argued in the national digital identity case of Robinson – v- The Attorney General of Jamaica, rights such as privacy "*are possessed by all persons simply by being human*,"[2] and therefore, national digital identity schemes should consider rights that flow from "being human" especially, for those who struggle to assert or who are otherwise denied a legal identity.

2. Scope and Purpose

2.3. Adopting a precautionary approach drawing on Article 5 and Article 6 of Convention ~~-~~108~~+~~, the guidelines emphasise the need for proportionality and necessity at the policy, design, implementation and operation of national digital identity systems. In ~~and in~~ particular, they emphasise the need for strengthened protection of the use of special categories of data such as biometric data. ~~This~~ The guidelines require~~s~~ an objective assessment of the benefits versus interference with ~~fundamental~~ rights and fundamental fredoms~~human rights~~, supporting justified policy objectives while minimising risks to individuals *and* to groups.

Commented [A1]: "the impact on human rights including privacy and personal data protection"

Commented [A2]: Although very interesting, I wonder whether it is appropriate for guidelines. This remark concerns all the other quotations or examples included in the text. Maybe we could think about restructuring the document and for example consider the first part (until page 20) as a "Report" or "background information" and then differentiate more clearly the Guidelines which would start on page 21 (now called Recommendations)

Commented [A3]: we can probably delete "on the use"

Commented [A4]: legitimate?

[1] European Court of Human Rights, (2019) Guide on Article of the European Convention on Human Rights https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

[2] Para. 175. Robinson – v- The Attorney General of Jamaica https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

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

(…)

Convention 108+ establishes key principles, obligations and rights that must apply when processing ~~of~~ personal data and special categories of data such as biometrics, and that are essential to incorporate into government policy making, and the design, implementation and operation of national digital identity schemes. People must not become mere objects represented by ~~their~~ digitized identities assigned by others.

Commented [A5]: some adjustments may render the sentence more readable

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~~ndividuals and groups must be able to clearly understand:

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

(...)

- the existence of rights and how to exercise them
- how to easily have inaccurately recorded data corrected and how to update their records (which should free of charge)
- the basis for exclusion from NIDS (for example lack of proof of birth)
- how to obtain redress

Commented [A6]: existence of data subject rights?

It is important that when NIDS require the processing of biometric data that an alternative means of inclusion is provided for those individuals who are unable to provide biometrics[3] or

Commented [A7]: unable and/or unwilling?

[3] See, The Wire (2017) *Unable to Verify Fingerprints or Iris, Aadhaar Denies Leprosy Patients Basic Services* https://thewire.in/government/unable-verify-fingerprints-iris-aadhaar-denies-leprosy-patients-basic-services

whose biometrics are unreadable[4] or who biometrics become unreadable.[5] This will help ensure *fairness* and *prevent exclusion*.

3.3 Specific and legitimate purpose(s) and purpose limitation

(…)

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. 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.

Commented [A8]: I wonder whether we may give the wrong impression that (any) law would solve the problem (although we refer to the need of HRIA)

(…)

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

Ensuring the accuracy of data processed in NIDS is crucial. This is especially so when NIDS require the registration of biometrics and where biometric data may link to other identity--based systems such as facial recognition. 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.

(…)

Establishing and maintaining the capability to keep data up to date is crucial. Individuals must have a simple means free of charge to update their information such as a change of name or address or contact details for example.

Data protection obligations to ensure accuracy in NIDS also requires the ability to disassociate identities. For example, a government may impose a legal requirement on individuals to register their NIN and/or biometric data with mobile operators in order to simply obtain a pre-paid mobile SIM card (known as 'mandatory SIM registration'6). Mobile operators may be required by law to verify such data against a NID database or to capture such data and register it on a NID

Commented [A9]: Aren't we giving the impression that we somehow encourage this practice?

[4] See for example, Drahansky et al, (2012) *Influence of Skin Diseases on Fingerprint Recognition* https://www.hindawi.com/journals/bmri/2012/626148/

[5] The global mobile trade association, the GSMA, reports that in Kenya, in a social protection programme, the elderly and those engaged in manual labour, were unable to provide proof of identity (called 'proof of life' in the programme) as their fingerprints were no longer readable by the biometric scanner. GSMA, (2020) *Opportunities for Improving Digital Identification in Social Cash Transfers* https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/04/SCT_Report_R_WebSingles.pdf

[6] GSMA, Access to Mobile Services and Proof of Identity 2021: Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf

database. A person's national identity number and/or biometrics will be bound to a range of unique identifiers such as a person's mobile number or the unique identifiers of their devices.7 When a person disposes of their mobile number or when a mobile operator cancels service to a number, the number may be recycled to another individual. Likewise, a person may dispose of their mobile phone – passing it on to a family member or selling it. Unique identifiers therefore will no longer be in the possession of and used by the person to whom they were originally bound. It is important to also consider that NIDS and associated mobile identities may also be tied to financial services identifiers through anti-money laundering (AML) or know your customer (KYC) regulation. Given that a justification for mandatory SIM registration and even AML and KYC is a 'need' to address national security and reduce crime, a failure to maintain accuracy of data in the binding of mobile identifiers to a person's national identity may further exacerbate existing and potential adverse consequences for a person's human rights.

Commented [A10]: Same as above

3.5 Data Retention

For example, a biometric template should be deleted if the template is no longer readable because of the degradation of the biometrics of the person from whom the biometric template was originally created, such that the template is unusable. Another example is the re-recording of biometric data such as fingerprints, facial or iris scans at regular intervals - in these cases, old biometric templates should be erased unless their continued retention can be justified and accompanied by appropriate safeguards.

Commented [A11]: "Moreover", better than "for example"

3.6 Security of processing

(…)

'Appropriate' measures' ~~security~~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.

(...)

- consider how you would deny access to and otherwise prevent the use of national identity systems and data, especially biometric data, during times of crises, where such data may be used to intentionally harm individuals.

Commented [A12]: strange wording. can we use the impersonal form?

Commented [A13]: As above?

Commented [A14]: this sentence is not crystal-clear

[7] See footnotes 19 & 20.

3.7 Profiling and automated decisions making

The UK data protection authority also recognises the risks of profiling. Writing on the UK government's proposal for a trusted digital identity system,8~~,~~ the UK Information Commissioner's Office argues that "it is important that all organisations involved in the framework, including Government and other public bodies, have a clear dividing line between the processing of data for digital identity verification purposes and all other purposes [and that] profiling data collected for digital identity purposes ... could be intrusive and involve organisations evaluating data both within the system and related to the system (such as how often and where they made an identity check) to build a picture of an individual. It is important that no organisations use data they collect for digital identity purposes for wider profiling."9 This is important commentary given the possible public-private nature of national digital identity systems or systems based on federated public-private national digital identity schemes that utilise personal data attributes held by the public and private sectors.

Commented [A15]: this part is probably too descriptive. See the general comment on page 4

3.8 Human Rights by Design and Human Rights Impact Assessments

Policy and design choices may adversely impact privacy and other fundamental rights and freedoms particularly with regards to national digital identity schemes. Article 10 of Convention 108+ requires that controllers and where applicable processors shall, "*prior to the commencement*" of data processing, "*examine the likely impact of intended data processing on the rights and fundamental freedoms of data subjects*" and "*shall design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms*." Likewise, data protection laws such as the EU General Data Protection Regulation[10] may require controllers to adopt 'data protection by design and default' and like laws such as the Mauritius Data Protection Act 2017[11], require data protection impact assessments prior to processing where it is likely to result in a high risk to the rights and freedoms of individuals.

Commented [A16]: same as above

(...)

Diverging from terms used in law and even Convention 108+, these guidelines use the term human rights impact assessments (HRIA) and human rights by design (HRbD) in order to ensure a human ~~rights based~~rights-based approach national digital identity. ~~The~~ This requires~~human rights based process should begin with~~ identifying and engaging stakeholders (stakeholder engagement), and in particular affected rights holders. This will help identify not only risks to NIDS ~~themselves~~ but also to the human rights of those who NIDS will impact. NIDS

Commented [A17]: I would not emphasise this, and on the contrary try to build the discourse on the provisions we have in 108, as discussed during the last Bureau meeting

[8] https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework
[9] The Information Commissioner's position paper on the UK Government's proposal for a trusted digital identity system (2021) https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf
[10] https://ec.europa.eu/info/law/law-topic/data-protection_en
[11] See Section 34 https://dataprotection.govmu.org/Documents/The%20Law/Act%20No.%2020%20-%20The%20Data%20Protection%20Act%202017.pdf

can only be designed to avoid or minimise adverse human rights impacts if such impacts are identified and considered.

Stakeholder engagement

Stakeholder engagement is crucial to identifying, ~~considering and~~considering and mitigating risks to rights holders that national (digital) identity schemes (NIDs) may give rise to. Legal and civil society challenges, whether from the UK,[12] Kenya[13] or Jamaica,[14] reveal the importance of understanding the impact and consequences of NIDs for rights holders, and the need to design and ensure accountability for human rights. Stakeholder engagement is crucial to facilitating dialogue about the problems that NIDs seek to solve, and to surfacing the interests, expectations, needs and concerns of affected rights holders and of benefits and risks as seen by them.[15] Such engagement gives a necessary voice to and helps empower affected rights holders reflecting their lived experiences and needs and may help establish trust in proposals.[16]

(…)

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~~.

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:

Commented [A18]: this part seems to better suit a report than guidelines (see general comment on page 4

Commented [A19]: I would not refer to GDPR

[12] The UK Identity Cards Act 2006 was repealed in 2010 following scrutiny and civil society campaigning. https://spyblog.org.uk/ssl/spyblog/identity-documents-bill/

[13] Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR https://www.khrc.or.ke/publications/214-judgement-on-niims-huduma-namba/file.html

[14] 2019, Robinson v. Attorney General of Jamaica, Supreme Court, Claim No. 2018HCV01788 https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

[15] See for example, the Engine Room, 2019, *What to look for in digital identity systems*: *A typology of stages* https://www.theengineroom.org/wp-content/uploads/2019/10/Digital-ID-Typology-The-Engine-Room-2019.pdf and *Caribou Digital, Identities: New practices in a connected age* (2017) https://www.identitiesproject.com/wp-content/uploads/2017/11/Identities-Report.pdf

[16] 2021, Satterthwaite, M. *Critical legal empowerment for human rights* https://www.openglobalrights.org/critical-legal-empowerment-for-human-rights/?lang=English

- ensure that the goal of NIDS is well-defined, evidence-based, and proportionate and necessary

(...)

- ensure that national identity law includes the right to know of the uses made of their national identity data, subject to any exceptions in accordance with Article 11 of Convention 108+
- ensure civil and judicial redress mechanisms are established by which individuals may pursue grievances and rights

(...)

8. Glossary

(...)

Supervisory Authority: an authority established for ensuring compliance with the provisions of domestic data protection law.

Commented [A20]: necessary for the legitimate purpose pursued

Commented [A21]: we could align the text to 108 language

Commented [A22]: reference to Article 15 of 108+

MEXICO

8. Glossary

National Identity Number (NIN): A unique number assigned by a NIDS that relates a person assigned a legal identity and by which an individual can be uniquely identified by reference to the verification of attributes linked to captured when creating a NID.

Personal data: is any information relating to an identified or identifiable individual (data subject). This includes information that can be used to 'individualise' or 'single out' one person from another, for example, by reference to a NIN or mobile phone number or device identifier.

Commented [A23]: It is suggested to add the notion of human rights and their relation to digital identity.

SWITZERLAND / SUISSE

Projet de lignes directrices sur l'identité numérique:

[…]

7. Recommandations à l'intention des les autorités de contrôle à la protection des données

[…]

Les autorités de contrôle devraient envisager, à partir des approches de l'évaluation d'impact sur la protection des données et la vie privée, de créer une méthodologie d'évaluation d'impact sur les droits de l'homme. Une approche de l'EIDH dépasse l'esprit de la conformité aux normes de la protection des données pour intégrer l'engagement et la participation en considérant les intérêts des personnes et des groupes que les lois sur la protection des données et l'AIPD ne prennent pas en compte. De même, une EIDH permet d'identifier les problèmes, les besoins et les risques perçus des détenteurs des droits, ce que n'aborde pas une AIPD.

Commentaire de la Suisse :

La Suisse partage l'avis émis lors de la séance du bureau de septembre 2021, à savoir que la création d'une méthodologie d'évaluation d'impact sur les droits de l'homme par les autorités de contrôle à la protection des données dépasserait leurs compétences. Ainsi, le chiffre 117 du rapport explicatif de la C108+ mentionne : *Cet article vise à assurer la protection effective des individus en demandant aux Parties de créer une ou plusieurs autorités de contrôle, indépendantes, impartiales et publiques, qui contribuent à la protection des droits et libertés des individus* ***à l'égard du traitement des données à caractère personnel***. La recommandation à l'intention des les autorités de contrôle à la protection des données devrait donc se limiter à l'AIPD et non à une EIDH.

URUGUAY

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

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~~I~~ndividuals and groups must be able to clearly understand:

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

Commented [A24]: And consent the use when it is needed

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 *necessary* 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+.[17]

Controllers and other entities providing hardware, software and services that enable NIDS, should work to ensure that from design to implementation and operation and data processing, that only those data necessary for a purpose specified under NIDS law or other appropriate legislation shall be processed. Data should not be used for purposes that are incompatible with those specified (NIDS) purposes.

Commented [A25]: Or to eliminate those data that it is not compatible with the purposes.

[17] 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)."