19 March 2021 T-PD-BUR(2021)2rev

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

CONVENTION 108

Digital Identity

Draft Guidelines

Directorate General of Human Rights and Rule of Law

TABLE OF CONTENTS

1. Introduction

Policy agendas and initiatives among governments, international organisations and the private sector in many parts of the world are driving the reconceptualization of 'a person's legal identity[1] as a de facto 'national digital ID'. Reinforcing these developments, we also see the commercial advocacy and the commodification of a 'legal [digital] identity' as a 'fundamental human right' by private sector identity stakeholders.[2] This reconceptualization of a legal identity as a 'national digital ID' has spurred the development of national digital identity schemes (NIDS) that have in many cases become a prerequisite to access basic services and rights in many countries.

A key justification for national identity schemes is that they fulfil a fundamental human right to a 'legal identity'.[3] That NIDs facilitate access to social and economic rights and entitlements and provide broader societal protections, such as personal and societal security. While a national digital identity scheme may bring significant benefits and protections in multiple contexts, and allow individuals to obtain and assert important rights, it 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 a human rights based approach built on human rights by design and that incorporates assessments of the impact on human rights beyond data protection and privacy. Human rights values should underpin NIDs.

Of note, is that there is no universally agreed definition of 'legal identity' or 'digital identity', and likewise, there is no agreed definition of a 'national digital identity'. 'National digital identity' appears inadequately defined in policy, law and practice such that national digital identity schemes may not appropriately consider, provide for or safeguard against risks to the fundamental rights and freedoms of individuals (and groups).[4]

National digital identity schemes involve the electronic capture of a range of attributes about an individual so an individual is uniquely identifiable within a population and given contexts. NIDS are rapidly evolving and increasingly seek to incorporate biometrics such as fingerprints and iris scans, digital device identifiers or even digital behavioural attributes as a means of creating and verifying a 'digital identity.[5] In 2011, the Council of Europe adopted Resolution

[1] The concept of 'legal identity' has developed from Article 6 of the Universal Declaration of Human Rights that "Everyone has the **right** to recognition everywhere as a person before the law." This has been given impetus by the drive to achieve the UN Sustainable Development Goal (UN-SDG) 16.9 that calls for the provision of "*legal identity for all, including birth registration*" by 2030 https://sustainabledevelopment.un.org/sdg16 See also, Manby, B (2020) *The Sustainable Development Goals and 'legal identity for all': 'first, do no harm'* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3783299

[2] Mastercard joins ID2020 Alliance https://mastercardcontentexchange.com/newsroom/press-releases/2020/may/mastercard-joins-id2020-alliance/

[3] Case law of the European Court of Human Rights has variously found a person's identity to include an individual's ethnicity as an "*important element of [their] private life"* https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0 or that identity can "*embrace multiple aspects of a person's identity, such as gender identification and sexual orientation, name or elements relating to a person's right to their image*" and that is may also include a right to a name and a right to identity documents. The ECHR has also found that the use of biometric data and DNA profiles to infer ethic origin may violate a person's right to ethnic identity under Article 8 of the ECHR – see https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

[4] See for example, *Robinson – v- The Attorney General of Jamaica* https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf or Namati, (2019) *Case Filed to Stop New Digital ID Register in* Kenya https://namati.org/news-stories/case-filed-stop-new-digital-id-system-kenya/

[5] See Access Now, (2018) National Digital Identity Programmes: What's Next https://www.accessnow.org/cms/assets/uploads/2018/03/Digital-Identity-Paper-digital-version-Mar20.pdf and Digital Identity Trends – 5 forces that are shaping 2020 https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/trends and Kloppenburg and Ploeg, (2018) *Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences* https://www.tandfonline.com/doi/full/10.1080/09505431.2018.1519534

1797 raising concern that such technologies may put at risk key human rights and called for an assessment of such risks and the adoption of measures to address them.[6] Developments have also led to the linking of or integration of identity schemes such as mandatory biometric based mobile SIM card registration into national digital identity policy and systems, and to the potential to link and integrate in to other systems, such as vehicle surveillance schemes[7] or facial recognition[8] or facial verification schemes.[9] Such developments add to the potential risks and harms that may arise from 'national digital identity' schemes that do not appropriately consider their impact on a person's human rights and fundamental freedoms.

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.[10] 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*,"[11] 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.

Given the above, these guidelines support a human rights by design approach that includes the need for stakeholder engagement in identifying and assessing possible adverse impacts of NIDS on the fundamental rights and freedoms of individuals *and* groups. The approach requires parties to appropriately consider the needs, concerns and risks of NIDS as identified by communities and/or their representatives. As Beduschi argues, "*digital identity platforms will only effectively contribute to the protection of human rights if they comply with [international human rights law], adequately mitigate … risks ... and promote high standards of privacy and data protection*,"[12] as consistent with case law on the European Convention on Human Rights for example.[13]

2. Scope and Purpose

2.1 These guidelines are general in scope, applying to the public and private sectors and seek to apply the principles and other key provisions of the Council of Europe Convention for the Protection of Individuals with regard to the Processing of Personal Data ("Convention 108+")[14] to the development and implementation of national digital identity schemes.

[6] Council of Europe, Resolution 1797 (2011) The need for a global consideration of the human rights implications of biometrics http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=17968&lang=en

[7] Schemes that may also include facial recognition. See Harper, J (2018) *The New National ID Systems* https://www.cato.org/policy-analysis/new-national-id-systems#real-id-and-e-verify

[8] https://www.unwantedwitness.org/ugandas-facial-recognition-technology-threatens-privacy/

[9] https://www.bbc.co.uk/news/business-54266602

[10] 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

[11] 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

[12] Beduschi, A (2019) Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights https://journals.sagepub.com/doi/pdf/10.1177/2053951719855091

[13] See for example, references to identity in this *Guide on Article 8 of the European Convention on Human Rights*, published by the European Court of Human Rights (2020) https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf and in this Guide to the Case-Law of the of the European Court of Human Rights, Data Protection (2020) https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0

[14] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168076c65bf

2.2 Drawing in particular on Article 10(2) of Convention 108, the guidelines establish a set of reference measures that policy makers and other stakeholders can apply to national digital identity schemes, to help ensure such schemes do not undermine human rights and fundamental freedoms. It is intended that the guidelines will help foster a human rights centred approach to help ensure NIDS are designed from the outset to respect and protect fundamental rights and freedoms, not just of individuals but of groups also.

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 and in particular, the need for strengthened protection of the use of special categories of data such as biometric data. This requires an objective assessment of the benefits versus interference with fundamental human rights, supporting justified policy objectives while minimising risks to individuals *and* to groups.

2.4 The guidelines do not replace measures required in law to safeguard against risks to the interests, rights and fundamental freedoms of individuals and nothing in these in guidelines shall be interpreted as precluding or limiting the provisions of the European Convention on Human Rights and of Convention 108+[15].

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

When considering the processing of personal data for fulfilling the objectives of NIDS, it is crucial to 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 Preamble to Convention 108+ which 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***."[16]

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, and the design, implementation and operation of national digital identity schemes. People must not become mere objects represented by their digitized identities.

3.1 Legitimacy of processing

As provided by Article 5 of Convention 108+ the processing of personal data (and special categories of data) must have a legitimate basis laid down by law, such as a domestic data protection law or some other law or regulation.[17] Article 6 of Convention 108+ further requires that the processing of special categories of data such as biometric data or data revealing a person's ethnicity (often used in NIDS), must be subject to appropriate safeguards enshrined in domestic law.

[15] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
[16] Convention 108+, Preamble, Paragraph 9, Page 16 https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
[17] https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf

NIDS interfere with and have significant implications for fundamental rights and freedoms and in particular the right to privacy and data protection. Therefore, an omnibus domestic data protection law, aligned with Convention 108+, should *first be established* to provide a foundational legitimate basis and rules and safeguards. A domestic data protection law should inform and be a prerequisite to the introduction of a NIDS.

A NIDS must separately have a legitimate basis laid down in domestic law and only after an appropriate assessment has been conducted.[18] NIDS must serve genuine objectives of a pressing social need that are considered necessary *and* proportionate in a democratic society, rather than for expediency or being justified as 'desirable'. This requires that the scope of NIDS and the specific purposes of the processing of personal data and special categories of data proposed under NIDS is subject to an assessment of their impact on the human rights and freedoms of individuals (and groups). Including an assessment of appropriate safeguards to limit and mitigate risks to rights and freedoms.

3.2 Fairness and Transparency

Article 5(4)(a) and Article 8 of Convention 108+ require that the processing of an individual's data is done in a manner that is fair and transparent. 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 ensuring the scope and purpose of such law is foreseeable and accessible. 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.

Individuals 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 specific purposes
    - this should include whether NID data, such as a 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,[19] or electronic equipment number of a mobile phone,[20] 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.

[18] https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf
[19] 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
[20] 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

- 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 NID.
- the contexts in which the subsequent presentation of proof of a NID is a mandatory or voluntary requirement and the consequences of refusing to provide a NID (for example denial of access to services or the obtaining of a mobile phone).
- rights and how to exercise them
- how to easily have inaccurately recorded data corrected and how to update their records (free of charge)
- the basis for exclusion from NIDS (for example lack of proof of birth)
- how to obtain redress

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[21] or whose biometrics are unreadable[22] or who biometrics become unreadable.[23] This will help ensure *fairness* and *prevent exclusion*.

Fairness also requires that communications about NIDS and the processing of personal data and special categories of data are appropriate and intelligible to the diverse communities that NIDS are meant to serve.[24]

3.3 Specific and legitimate purpose(s)

Prior to the implementation of NIDS, it is important that national policy and law on NIDS explicitly define 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 of Article 5(4)(b) of Convention 108+ and also the design obligations contained in Article 10 of Convention 108+.[25]

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.

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 or otherwise objectionable by data subjects. Any processing that has such consequences must be clearly established in law

[21] 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
[22] See for example, Drahansky et al, (2012) *Influence of Skin Diseases on Fingerprint Recognition* https://www.hindawi.com/journals/bmri/2012/626148/
[23] 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
[24] See for example, paragraph 68 of the Explanatory report on Article 8 of Convention 108+ (page 23).
[25] 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)."

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.

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

Accurate

Inaccurate data can have significant adverse consequences for people's human rights. It can lead to incorrect suspicion of criminal activities or other offences in law and/or to false arrest and imprisonment for example. It can lead to exclusion from services or social protection measures. It can lead to discrimination. For these reasons it is crucial that measures are adopted to ensure the accuracy of any personal data or special categories data processed, and that inaccurate personal data can be corrected or deleted in a timely manner.

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.

The use of biometric data in NIDS requires additional measures to ensure the accuracy of biometric data acquired, enrolled and matched and during the performance of those aspects of NIDS that require a person to present their biometrics for proof of identity or authentication.[26] It also requires measures to reduce bias and inaccuracies in biometric identity techniques and technologies and to enhance fairness.[27] It is imperative that testing for 'accuracy' is a core requirement of a human rights by design approach and pre-purchase and implementation of biometric identity technologies.

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'[28]). 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 database. A person's national identity number and/or

[26] See for example, Council of Europe Guidelines on Facial Recognition, (2021) https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 and guidance on *Biometric recognition and authentication systems* from the UK National Cyber Security Centre, https://www.ncsc.gov.uk/collection/biometrics/measuring-performance

[27] UK Government Office for Science, (2018) Biometrics: a guide https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf

[28] 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

biometrics will be bound to a range of unique identifiers such as a person's mobile number or the unique identifiers of their devices.[29] 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.

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 must first define the purpose, and ensure an appropriate legitimate basis – which for NIDS should be specified in law.

The data must be proportionate and sufficient to meet the identified and specific purposes and not excessive for those purposes. The processing of personal data or special categories of data that would result in a disproportionate interference with the fundamental rights and freedoms of individuals and groups would be considered excessive under Convention 108+.[30]

Measures must be taken to ensure that biometric data captured from individuals to create a biometric template for the purposes of identification and authentication (as authorised by NIDS law), must contain only that information sufficient to meet a specified purposes in order to prevent the misuse or incompatible uses of biometric templates.

The processing of data for the purposes of NIDS must always be justified and necessary to meet a specific purpose laid down in law. Determining what data is necessary and the quality of data necessary to fulfil a legitimate specified purpose for NIDS, should be the subject of prior assessment beginning with policy, and continuing into law, design and practice and be in part, informed by stakeholder engagement as discussed below. Data quality must form part of a cycle of continuing assessment and evaluation and adaption to findings and events. This obligations and requirements must also include other systems that form dependencies of NIDS – such as mandatory SIM registration, refugee identification schemes, facial recognition surveillance schemes and so on.

Good data quality management practices can help prevent adverse impacts on the rights and freedoms of individuals and groups and also assist in preventing and/or removing duplications in registered identities and effective management of services dependent on such identities.[31]

[29] See footnotes 19 & 20.
[30] Article 5 – Legitimacy of data processing and quality of data of the Explanatory Report to Convention 108+ paragraph 52
[31] UN World Food Programme, (2021) Report of the External Auditor on the management of information on beneficiaries, draft decision, Paragraph 52, http://www.fao.org/3/nf601en/nf601en.pdf

3.5 Data Retention

Personal data and special categories of data must only be retained for as long as necessary to fulfil a specific justified and legitimate purpose and should be deleted or rendered anonymous when the purpose of processing has been achieved. This must include consideration of data processed in systems integrated into NIDS or on which NIDS depend or that otherwise depend on NIDS. For example, facial recognition systems or mandatory SIM registration systems or border control systems.

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.

3.6 Security of processing

NIDS involve the processing of (often sensitive) data at *population scale* and may even contain data on specific vulnerable and at risk groups. NIDS may interconnect to or otherwise include other identity based systems such as migration and law enforcement databases, or mandatory sim card registration databases that are important to also consider.[32] It is vital that controllers ensure appropriate technical and organisational measures are implemented to protect data held in national identity systems and other identity related systems they interconnect to. A compromise of one system may compromise others.

'Appropriate' security requires an assessment of the sensitivity of the data involved and the potential adverse consequences for individuals and groups and for their fundamental rights and freedoms. A lack of appropriate security may include the theft and/or unauthorised disclosure of data. These may lead to harms such as harassment, persecution, fraud, identity impersonation.

It is also important to consider that once compromised – stolen for example - biometric data that cannot be replaced, or that the theft of biometric templates can be repurposed.

The principle of data minimisation is an important consideration in the context of security. If you do not collect data then it cannot be compromised.

Appropriate measures may include;

- policies and procedures to investigate and manage security incidents that may have adverse impacts for individuals and their fundamental rights and freedoms and procedures for reporting such incidents to individuals and data protection supervisory authorities.
- policies, procedures and physical and technical measures to control access to systems and the personal data they hold or provide access to.

[32] Casagran, C (2021), *Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU*, Human Rights Law Review, Volume 21, Issue 2, June 2021, Pages 433–457, https://academic.oup.com/hrlr/article/21/2/433/6131329

- procedures to investigate and address security weaknesses.[33]
- providing internal and external processes for the confidential reporting of security vulnerabilities.[34]
- regularly testing the security of existing security measures and maintaining a log of these and actions taken/to be taken to address failings that might compromise the data and rights and freedoms of individuals.

Another matter to consider for authorities providing mobile apps to enable access to NIDS, is not just the security of those apps, but whether the apps may contain third party tracking code embedded that collects device and other identifiers or behavioural data, that may compromise the privacy and rights of individuals.

3.7 Profiling and automated decisions making

National identity systems may facilitate the profiling and electronic surveillance of individuals with the potential for significant adverse consequences for human rights, as eloquently deliberated in legal cases such as the ruling of the Supreme Court of Jamaica.[35] This may especially arise when NIDS interconnect with systems introduced to facilitate the surveillance of individuals or groups and that may be contrary to the right to respect for private life in accordance with international human rights instruments.[36] Profiling may "*expose individuals to particularly high risks of discrimination and attacks on their personal rights and dignity*," and may lead to the violation of human rights.[37]

The UK data protection authority also recognises the risks of profiling. Writing on the UK government's proposal for a trusted digital identity system,[38], the UK Information Commissioner's Office argues 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*."[39] 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.

[33] For example, in 2017, researchers informed the Estonian authorities of a 'flaw' in chip of the Estonia digital identity card affecting approximately 7500,000 identity cards issued since 2014. It was reported that the flaw could allow the decryption of private data on the affected digital identity cards. https://news.err.ee/644250/gemalto-rep-estonian-authorities-notified-of-id-card-flaw-in-june This incident also reportedly led to the Estonian authorities suing the private sector chip manufacturer for Euro 152 million https://www.reuters.com/article/estonia-gemalto-idUSL8N1WD5JZ Also see the e-Estonia response 'What we learned from the eID security risk? https://e-estonia.com/card-security-risk/

[34] See for example, the UK National Cyber Security Centre, Vulnerability Reporting, https://www.ncsc.gov.uk/information/vulnerability-reporting

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

[36] Declaration of the Committee of Ministers of the Council of Europe on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, adopted 11 June 2013 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068460d and also referenced in Council of Europe Guidelines on Facial Recognition, (2021) https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3

[37] Council of Europe Recommendation CM/Rec(2010)13 and explanatory memorandum on *'The protection of individuals with regard to automatic processing of personal data in the context of profiling'*. https://rm.coe.int/16807096c3

[38] https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework

[39] 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

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.

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[40] may require controllers to adopt 'data protection by design and default' and like laws such as the Mauritius Data Protection Act 2017[41], 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.

As discussed previously, NIDS may be a combination of public and private arrangements and technologies and support. It is important to consider the recommendation of the Committee of Ministers of the Council of Europe[42] calling for Member States to encourage or require businesses to "*apply and carry our human rights due diligence ... including project-specific human rights impact assessments, as appropriate …*" These guidelines are consistent with the legal objectives of Convention 108+ and domestic data protection laws and the goal of the above recommendation of ensuring appropriate due diligence. The obligation to carry out diligence and human rights impact assessments applies equally to the public sector when considering the adoption of NIDS.

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 approach national digital identity. The human rights based process should begin with identifying and engaging stakeholders (stakeholder engagement), and in particular affected rights holders. This will help identify risks to NIDS themselves but also to the human rights of those who NIDS will impact. NIDS can only be designed to avoid or minimise adverse human rights impacts if such impacts are identified and considered.

Stakeholder engagement

[40] https://ec.europa.eu/info/law/law-topic/data-protection_en
[41] See Section 34 https://dataprotection.govmu.org/Documents/The%20Law/Act%20No.%2020%20-%20The%20Data%20Protection%20Act%202017.pdf
[42] 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 is crucial to identifying, 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,[43] Kenya[44] or Jamaica,[45] 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.[46] 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.[47]

A good example of stakeholder engagement can be found in the UK. The Ada Lovelace Institute recently created the Citizens Biometrics Council (CBC) to publicly "*deliberate on the use of biometric technologies like facial recognition"* including concerns over identity, bias and discrimination that biometric data may give rise to. A subsequent report[48] of the recommendations and findings of the CBC argues that "*continued consultation with, and representation of, a diverse cross-section of society is fundamental to ensuring that biometric technologies are only deployed in a way that is trustworthy, responsible and acceptable.*" This is true of NIDS if they are to be seen as legitimate, trustworthy and that respects and safeguards fundamental rights and freedoms, especially NIDs that incorporate biometrics. Effective stakeholder consultation should be viewed as foundational policy and legal requirement of identity based schemes that by their nature interfere with the right to privacy and that may create risks to other rights and freedoms. Stakeholder consultation should be a key component of impact assessments and design.

The Danish Institute for Human Rights (DIHR) has produced a helpful document on stakeholder engagement as a supplement to its human rights impact assessment guidance.[49] While guidance on stakeholder engagement and human rights appears to have

[43] 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/

[44] 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

[45] 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

[46] 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

[47] 2021, Satterthwaite, M. *Critical legal empowerment for human rights* https://www.openglobalrights.org/critical-legal-empowerment-for-human-rights/?lang=English

[48] Report of the recommendations and findings of the *public deliberation on biometrics technology, policy and governance* (2021) https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Citizens_Biometrics_Council_final_report.pdf

[49] Human Rights Impact Assessment Guidance and toolbox: Stakeholder engagement practitioner supplement https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/stakeholder_engagement/stakeholder_engagement_prac_sup_final_jan2016.pdf

its roots in extractive industries,[50] and/or the corporate sector,[51] guidance such as that from the DIHR, can help provide a basis on which to consider effective stakeholder engagement in the context of NIDs.

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:
    - ICT
    - digital economy
    - health care
    - education
    - birth registration/civil population registration
    - national identity
    - border control
    - national security/law enforcement
    - social protection
    - indigenous affairs
    - refugees
    - procurement
    - data protection
    - human rights
- **Parliament**
  - Committees with a human rights and technology, digital economy, identity focus
- **National regulatory bodies** that have a human rights related mandate/responsibilities
  - Data Protection Authorities
  - Human rights or equalities commissions[52]
  - Biometric Commissioners
  - Surveillance Commissioners
  - National Identity Commission
  - Telecommunications Authorities
- **Judiciary/Redress**
  - Ombudsman with human rights/social justice mandates/responsibilities[53]
  - Bar associations
  - Community based organisations that support the resolution of human rights redress
- **Rights holders and representatives**
  - Community representatives
  - Civil society / Human rights organisations[54]
  - Citizens councils

[50] See for example https://www.oecd.org/daf/inv/mne/OECD-Guidance-Extractives-Sector-Stakeholder-Engagement.pdf

[51] see https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[52] For example, the Chancellor of Justice of Estonia https://www.oiguskantsler.ee/en

[53] See for example, Equinet – European Network of Equality Bodies https://equineteurope.org/author/greece_ombudsman/ or the European Network of Ombudsmen https://www.ombudsman.europa.eu/en/european-network-of-ombudsmen/about/en See also footnote 4

[54] For example, organisations such as Namati and the legal empowerment network https://namati.org/network/

- **Business sector**
  - ID vendors – hardware and software
  - Industry associations
  - Mobile operators[55]
  - Financial services/mobile money agents
- **Academia / Research**
  - academics with a national digital identity /human rights focus
  - institutions with a focus on national digital identity /human rights[56]
- **International Actors**
  - Humanitarian organisations
  - World Bank
  - UN organisations [57]
  - International Telecommunications Union (ITU)
  - Organisation for Economic Co-operation and Development (OECD)
  - African Union
  - Africa Commission for Human Rights
  - Council of Europe
  - EU[58]

Esteves et al, write that "*equality and non-discrimination, participation and inclusion, and accountability and transparency constitute the key principles underpinning a human rights-based approach. Non-discrimination means that various groups of rights-holders – especially vulnerable people, women, children, Indigenous peoples, and other marginalised groups – require special attention to be able to enjoy their human rights*."[59] National digital identity schemes require such inclusive and participatory stakeholder engagement and accountability.

Human Rights Impact Assessments and Human Rights by Design

Data protection frameworks require consideration of risks to the interests, rights and fundamental freedoms of individuals and to safeguard against risks to these, through a range of governance measures and design. But such frameworks may not sufficiently elaborate on what those interests, rights and freedoms are or the circumstances in which risks may materialise and harms occur. These guidelines adopt a more inclusive term of Human Rights Impact Assessment ('HRIA), that from the outset forces consideration of rights beyond privacy that may be impacted by NIDS, that need to be designed for (in policy, technology and practice).

[55] Mobile operators may be required to collect and or verify personal and biometric data and national identity details for any person seeking to buy a mobile SIM card and record this against SIM card identifiers, device identifiers and mobile numbers. See for example GSMA, 2021, *Access to Mobile Services and Proof Identity* (2021) https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf

[56] For example, Strathmore University, Kenya & its Centre for Intellectual Property and Information Technology Law and Digital Identity research programme https://cipit.strathmore.edu/our-id-experience/ or the Identities Research Project https://www.identitiesproject.com/ or The Centre for Internet Studies, India, 'Digital Identities: Design and Uses' https://digitalid.design/

[57] See for example the UN Refugee Agency, Registration and Identity Management https://www.unhcr.org/registration.html Or UNDP https://unstats.un.org/legal-identity-agenda/meetings/2021/UNLIA-FutureTech/docs/Agenda.pdf

[58] See for example, the EU-AU Digital Economy Task Force that considers digital identity services as an enabler of the digital economy https://digital-strategy.ec.europa.eu/en/policies/africa or the recent agreement between the EU and the Members of the Organisation of the African, Caribbean and Pacific States. Article 70(3) of the agreement requires parties to "develop robust, secure and inclusive identification systems to ensure the provision of a legal identity for every citizen, including by strengthening the system of civil registration and vital statistics (CRVS). https://ec.europa.eu/international-partnerships/system/files/negotiated-agreement-text-initialled-by-eu-oacps-chief-negotiators-20210415_en.pdf

[59] Esteves et al (2017) Adapting social impact assessment to address a project's human rights impacts and risks https://www.sciencedirect.com/science/article/abs/pii/S0195925517300070

A HRIA incorporates the need to consider the moral and social values[60] of fundamental human rights given by international human rights law such as the European Convention on Human Rights (ECHR),[61] the Universal Declaration of Human Rights,[62] the EU Charter of Fundamental Rights,[63] or the constitutions of countries. A HRIA more broadly requires inclusive participation of impacted rights holders and consideration of the impact on their interests, rights and freedoms of policies and laws that seek to impose national digital identity schemes.

A HRIA approach forces policy makers and controllers to think beyond rules based 'data protection' requirements to considerations of whether a programme may exclude categories of 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.[64] 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*."[65]

A HRIA helps to strengthen transparency, legitimacy and accountability. A HRIA goes beyond an assessment that seeks to achieve compliance with law to one that puts individuals and communities, and their needs, concerns and perceived risks at its centre. A HRIA requires transparency about how NID will be used broadly, the systems it interacts with and the purposes and reasoning, and due consideration of the possible adverse human rights impacts and their mitigations.

But a HRIA must not be a tick box exercise. As Götzmann argues, a HRIA, must go "*beyond mere consultation or a technical add-on to project design [and] rather than stakeholder consultation being just one of the impact assessment stages [a] HRIA needs to make provisions for the inclusive participation of rights-holders at critical points throughout the whole assessment process*."[66]

There is no single, right way to conduct a HRIA. But resources linked in this document can help policy makers, regulators, controllers and providers of identity technologies understand key components of a HRIA.[67] International standards on identity management – while not explicitly addressing human rights – may help establish a methodical approach to creating a framework for identity management, that can be adopted to include broader human rights.[68]

---

[60] Mantelero, A (2018) *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment https://www.sciencedirect.com/science/article/pii/S0267364918302012*

[61] https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=

[62] https://www.un.org/sites/un2.un.org/files/udhr.pdf

[63] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[64] 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

[65] See footnote 58

[66] Götzmann, N (2016), *Human Rights Impact Assessment of Business Activities: Key Criteria for Establishing a Meaningful Practice* https://www.cambridge.org/core/journals/business-and-human-rights-journal/article/human-rights-impact-assessment-of-business-activities-key-criteria-for-establishing-a-meaningful-practice/D964B80AC12F33C0FBEE4EF6A2F323C4

[67] See in particular, the Danish Institute for Human Rights, and guidance (2020) on Human rights impact assessment of digital activities https://www.humanrights.dk/publications/human-rights-impact-assessment-digital-activities and especially comparisons between a DPIA and a HRI (page 38) https://www.humanrights.dk/sites/humanrights.dk/files/media/document/A%20HRIA%20of%20Digital%20Activities%20-%20Introduction_ENG_accessible.pdf. Also see (2020) The Tech Sector and National Action Plans on Business and Human Rights https://www.humanrights.dk/sites/humanrights.dk/files/media/document/The%20Tech%20Sector%20and%20National%20Action%20Plans%20on%20Business%20and%20Human%20Rights_2020_accessible.pdf and PIA guidance from the French Data Protection Authority, the CNIL, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

[68] For example, the International Standards organisation has developed frameworks and standards on identity management, identity proofing, biometric identity assurance. See https://www.iso.org/home.html

3.9 Accountability

A key requirement of Convention 108+[69] and modernised data protection laws is that 'controllers' must be able to demonstrate that the processing of data under their control complies with the principles and obligations as set out in those instruments.

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.[70]

Applicable organisations should:

- document and publish their commitment to a human rights based approach
- document and publish a plan for ensuring human rights impacts are considered at each stage of NIDS - from policy to stakeholder engagement, to law, to HRIAs, to design, to the operation of NIDS
- document and publish the outcome of stakeholder engagement and the results of HRIAs and how these will be considered and acted on
- develop policies, procedures and practices that demonstrate how human rights impacts are addressed (from data protection, to privacy, to ensuring non-discrimination for example)
- develop and implement awareness and training programmes on human rights and data protection and privacy in particular
- establish audit procedures to ensure not only compliance with obligations set out in data protection and NIDS law, but also avoid and mitigate adverse impacts to human rights
- ensure all parties in the delivery and operation of NIDS meet key applicable requirements, and in particular key principles of data protection
- establish policies and procedures to meet the rights of individuals and publish these
- publish clear process of individual or community (group) complaints and redress mechanisms
- ensure that the impact on human rights and the need to design for human rights is a requirement of the procurement process. Organisations providing hardware, software or support services for example, must be required to attest to how they will address human rights, including conducting HRIAs in support of contracts to support NIDS.
- establish clear governance structures, including ethics committees, to ensure not only compliance with law but also human rights due diligence takes place.
- consider independent reviews from a human rights impact assessment perspective

3.10 Right of individuals

Article 9 of Convention 108+ gives individuals a number of rights over the processing of their personal data and special categories of data. The rights must be established in law and apply

[69] Article 10
[70] See footnote 64 and

to NIDS and any interconnected or inter-dependent services that demand proof of legal identity or NID, or NIN etc.,

The rights given by Convention 108+ and by international human rights law such as the ECHR, may be restricted[71] *only* when provided for in law, that constitute a necessary and proportionate measure in a democratic society for specific and legitimate purposes in law, and that must always respect the essence of fundamental rights and freedoms.

Individuals must be advised of their rights and any limitations and contexts in which limitations may apply. The rights of individuals apply irrespective of the individual's citizenship, nationality or residency status. It is crucial that NIDS are designed in a manner that enables the exercise of individual rights.

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

- the right to be informed about why their data are required, what it will be used for (purposes), the lawful basis relied on (for example, consent or to meet a legal obligation), the period for which data will be kept, and which parties their data be shared with or given access to.
    - It is important that individuals are informed in clear and simple and culturally appropriate ways and sufficiently to ensure the processing is fair to individuals.
- 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 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+)

4. Recommendations for policy makers

[for discussion]

5. Recommendations for controllers

[for discussion]

6. Recommendations for the identity industry

[for discussion]

7. Recommendations for Supervisory Authorities

[for discussion]

[71] Article 11 Convention 2018+

8. Glossary

Attribute: a characteristic or property that is ascribed to a person, such as their name, gender, date of birth, parent's names, biometrics, and even a mobile phone number.

Authentication – the process of verifying the identity of an individual and that they are who they claim to be. This could be by examining an individual's birth documents or passport for example.

Biometric data: physiological or behavioural characteristics that can be used to uniquely identify an individual.

Centralised national identity system: one in which identity data is held in and controlled by one system and that provides proof of identity and authentication of identity.

Controller: means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing.

Federated identity system: relies on data held by different public authorities and private sector entities that facilitate the use of identity attributes between systems based on trusted authorised relationships. Data may be used to prove and authenticate a person's identity in a specific context.

Foundational identity system: a multipurpose population wide system that seeks to create an official government legal identity. Such systems seek to ensure an individual is uniquely identifiable within a national population. A foundational identity may support functional identities.

Functional identity system serves a specific and often sectoral purpose, such for the management of individual taxes or the provision of national healthcare or a driver's licence, or even voters' registration.

Identification – the process of establishing a person's identity based on verifiable attributes.

Identifier: a unique number or sequence of characters assigned to an individual so they are uniquely identifiable within a given identity management system.

Identity: an attribute or combination of attributes that uniquely identifies an individual.

National digital identity (NID): The processing of attributes about an individual so that the individual is a **uniquely identifiable** individual in given contexts.

National Digital Identity Schemes/System (NIDS): A combination of policy, law and technology by which a person's personal data and special categories of personal data are captured to establish and digitally represent, verify and manage a person's legal identity across public (and private) services identified in national policy and law

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.

Profiling: means the automated processing of personal data or special categories of data in order to evaluate aspects relating to an individual (or groups of individuals), in particular relating to an individual's ethnicity or religion, behaviour, location or movements.

Special Categories of data: as per Article 6 of Convention 108+, this includes genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; and personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life and which require appropriate safeguards that must be enshrined in law.

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

Annex A – Example stakeholder engagement approach

The following tables have been adapted directly from the Danish Institute for Human Rights 'Stakeholder Engagement Practitioner Supplement'[72] produced as part of their human rights impact assessment guidance and toolbox. The tables and suggestions are intended as an aid to considering key elements of stakeholder approach.

TABLE A: Stakeholder identification					
Stakeholder group	**Specific types of stakeholders**	**Entity and general characteristics** *Examples provided*	**Relationship with the national identity sponsor/or other stakeholders**	**Views / influence on the NIDs**	**Type of engagement e.g.** *when and how (in person, remote)*
Rights-holders/representatives	**Potentially impacted categories of communities**	This could include those lacking proof of citizenship/ or recognised legal identity; ethnic groups; refugees, asylum seekers and those with an inability to have their biometrics read or whose biometrics degrade over time.			
	Citizens/Consumers	Birth registration/CRVS services. Patients/students where services require proof of NID. Mobile phone subscribers that require proof of NID.			

[72] See https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/stakeholder_engagement/stakeholder_engagement_prac_sup_final_jan2016.pdf

TABLE A: Stakeholder identification					
Stakeholder group	**Specific types of stakeholders**	**Entity and general characteristics** *Examples provided*	**Relationship with the national identity sponsor/or other stakeholders**	**Views / influence on the NIDs**	**Type of engagement e.g.** *when and how (in person, remote)*
	Civil society organisations/ human rights defenders	Local/international non-governmental organisations, and community-based organisations such as community councils, human rights organisations, legal networks etc that represent affected communities and that may also facilitate redress/ombudsman roles.			
Duty-bearers	**Government actors**	National authorities, specific government agencies or departments, policymakers and regulators with direct responsibility at a policy, legal, technical, implementation and/or regulatory level for national digital identity schemes.			
	Parliamentary representatives/committees	Committees with a human rights/ technology, digital economy, identity focus.			
	Judiciary/Redress	Bar associations. Community based organisations that support the resolution of human rights redress			

TABLE A: Stakeholder identification					
Stakeholder group	**Specific types of stakeholders**	**Entity and general characteristics** *Examples provided*	**Relationship with the national identity sponsor/or other stakeholders**	**Views / influence on the NIDs**	**Type of engagement e.g.** *when and how (in person, remote)*
	Industry/ business sector	Providers of hardware/software for NIDS. Joint venture suppliers of NIDS. Supplementary businesses that may be mandated to record and/or verify national identity details – for example sim card registration. Industry associations engaged on NIDS.			
	Government Procurement	Procurement authorities and who should ensure that hardware and software can incorporate fundamental human rights and freedoms into the design and operation of NIDS. From data quality to data retention and erasure to the exercise of individual rights. The procurement process should require 'human rights by design assured'.			

TABLE A: Stakeholder identification					
Stakeholder group	**Specific types of stakeholders**	**Entity and general characteristics** *Examples provided*	**Relationship with the national identity sponsor/or other stakeholders**	**Views / influence on the NIDs**	**Type of engagement e.g.** *when and how (in person, remote)*
	International organisations	The World Bank, ICRC, UN agencies such as the UNDP, UNHCR etc.			
	National Human Rights Institutions (NHRIs)	Autonomous body with a constitutional or legislative mandate to promote and protect human rights, such as human rights commissions or ombudsman.			
	Experts & Researchers	National/legal digital identity experts including academics and researchers with a focus on human rights dimensions at the policy, legal and technology levels.			
	Media/journalists	State and private/community media/journalists to foster broader awareness and knowledge of NIDs and public consultations and encourage community engagement etc.			

TABLE B: Examples of steps to take prior to engaging directly with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
1. Establish a Human Rights Impact Assessment Team	A human rights impact assessment **team** should be established. The team must have clear objectives, and key roles and responsibilities agreed. The HRIA team should prepare a briefing that reflects the competencies, knowledge etc of specific targeted stakeholder groups and that clearly articulates: • the problem that a NIDS is meant to solve • the legal basis on which the NIDs is established. • linkages between NIDS and other services such as mobile SIM cards, health, education. social protection programmes, and the purpose and legal basis for these linkages. • the data that NIDS will collect, the purposes and who will have access to the data (and for what purposes) or who data will be shared with (and for what purposes), where data will be kept and how it will be kept secure and also safeguarded against abuse. • whether the NIDS is voluntary or mandatory and what data is voluntary of mandatory. Also, the contexts in which proof of NID will be required. • any financial costs to individuals. • the objective of seeking stakeholder views and how they will be considered. • how fundamental rights and freedoms will be protected. • a key point of contact by which stakeholder concerns over the consultation process can be communicated.	It may be necessary to train existing staff or hire stakeholder engagement experts that can ensure culturally appropriate techniques of engagement and inclusive participation. The team must also have an expert understanding of data protection, human rights and national digital identity.
2. Reach out to rights-holders	• identify local representatives and assess their experience of matters related to digital identity, data protection, human rights and facilitating community stakeholder engagement.	• consider the numbers of individuals to engage, their positions within communities and what

TABLE B: Examples of steps to take prior to engaging directly with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
	• identify preferred ways of communicating and participating. • enquire whether identified stakeholders are appropriately representative. • assess whether individuals or groups within communities are indirectly or directly excluded by the process (due to gender, socio-economic status, ethnicity, citizenship status etc).	would constitute a representative sample of views. • what is the preferred form and venue for face to face or virtual meetings. • consider if costs of participation may act as a barrier to engagement or lack of ICT equipment and connectivity may prevent participation. • are there any other barriers to engagement? Language? Cultural? Pollical? Fear? • Consider how best to ensure safe and inclusive engagement.
3. Determine the format, location, and time of the interviews/ meetings and factors that may act as a barrier to participation + privacy	• Consider one to one and group consultations and culturally appropriate techniques of engagement, to help to gather information. • How will engagement take place – face to face or virtual? • Consider those who feel for whatever reason unable to participate in proposed meetings – for example, marginalised individuals or groups or women only groups? • Consider culturally appropriate settings and timings. • Consider the provision of appropriate food and refreshments, and whether assistance may be needed to attend a venue. • Does a venue have appropriate facilities and is it a place where stakeholders will feel at ease? • Consider whether it is necessary collect personal data and if so, obtain consent and explain how they can change their mind and of other data rights.	• Do not take photographs unless people expressly consent and inform individuals beforehand whether photographs will be published (paper or online news media, websites, social media). • Consider whether providing personal data may act as a barrier and whether to not record or later redact personal data – ensuring transparency with participants.

TABLE B: Examples of steps to take prior to engaging directly with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
4. Assess the security context	• **Conduct thorough background research on the local security situation.** Consider risks for both the assessment team and the interviewed persons by conducting a risk analysis looking at threats, vulnerabilities and capacities. • **Consider risks to participation –** especially of marginalised / vulnerable groups, human rights defenders	• Consult with stakeholder representatives about actual or perceived security concerns for a chosen location • Consider if the need to take public transport is considered safe by participants • Consider if visiting the proposed meeting place is considered safe by specific groups? • Ensure responses from participants are secured appropriately – whether computerised or on paper • **Do not take photographs unless** people **expressly consent** and inform individuals beforehand whether photographs will be published (paper or online news media, websites, social media).

TABLE C: Examples of steps to take during the interview or meeting with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
1. Inform participants and capacity building	An agreed facilitator should clearly articulate: • the stakeholder process and its objective • the problem that a NIDS is meant to solve • the wish to understand and duly reflect on views, interests, needs and concerns of participants	**Build the capacity of rights-holders** by explaining the relationship between national digital identity, data protection and human rights and safeguards for rights and freedoms.

TABLE C: Examples of steps to take during the interview or meeting with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
	• explain how the data collected will be used – be transparent • explain rights over the use of personal data Avoid technical language and legalese unless appropriate to the stakeholder group (for example, industry, parliamentary science committee, ICT authority etc) Be respectful of and sensitive to participants. Be considerate of those who may be marginalised/vulnerable Be mindful or power relations and strive to sensitively include those who may appear reluctant to participate but do not exert pressure on such individuals or groups.	Also explain the role National identity and ID data will play in other areas of the lives of citizens /consumers. Such as whether proof of NID is required obtain a mobile SIM card, or access healthcare or education of social welfare and the implications of this. Provide a short data protection, NID and human rights 101 talk/presentation.
2. Ensure voluntary participation	• Ensure participation is informed and voluntary – based on peoples' consent. Provide culturally appropriate transparency notices that consider the literacy skills and languages of groups/individuals invited to participate. • Ensure people are aware of how they can withdraw their consent to participation • Inform people of their rights over their data – to have it destroyed for example if they so wish. • Validate your understanding of the discussion with interviewees at the end of an interview. Allow people to ask questions.	

TABLE C: Examples of steps to take during the interview or meeting with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
3. Respect participant´s privacy	• **Do not collect people's names and contact details unless they have given their informed consent** ○ ensure individuals are aware of how such data will be recorded, for how long, where it will be held, who would have access to it and why etc • Consider whether it's possible to allow anonymous participation or to participate privately • Consider any risks to individuals or groups to having their personal data recorded and/or their participation made public (some may fear being made visible)	Consider during the stakeholder planning stage, how you will respond to/assist individuals or groups if you become aware of serious **human rights abuses** during the consultations.
4. Ensure security and safety – do no harm	• Consider any developments immediately prior to the date of the proposed meetings & on the day that may impact the security of the facilitation team and stakeholder participants • Be prepared to stop the event if any group or individual feels unsafe	
5. Be respectful – communicate in a culturally appropriate manner	• Facilitate don't dominate discussions. • Listen and be open minded to enable the lived experiences of individuals and communities to surface. • Be respectful when considering the need to interrupt or address inappropriate behaviour or interventions. • Be mindful of power relations and inclusion. Strive to include those who are less eager to express themselves in the interviews.	•

TABLE C: Examples of steps to take during the interview or meeting with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
	• Consider appropriate breaks for refreshments etc	

In addition to the above, the impact assessment team should also consider how and when to report back to stakeholders and share findings and next steps, and communicate a plan for this.