~~9~~ 30 September 2022 T-
PD(2021)~~2rev8~~2rev9

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

CONVENTION 108

National Digital Identity

Draft Guidelines

TABLE OF CONTENTS

1. Introduction

Many countries have adopted national identity schemes that process a range of personal data including special categories of data about individuals in order, principally, to certify the authenticity of an individual's 'legal identity' before the law and vis-à-vis the state. The concept of 'legal identity' has developed from Article 6 of the Universal Declaration of Human Rights which provides that "Everyone has the **right** to recognition everywhere as a person before the law."

Historically, national identity schemes began as 'analogue' identity systems that relied on the limited data recorded in civil (birth, marriage, death) registration systems. Such national identity schemes were and may still be based on issuing a foundational identification 'document' (such as an identity card) by which a person may prove their identity before the law and vis-à-vis the state', and by which individuals may be granted access to public services (such as social welfare protections) or by which they could assert their rights.

Increasingly, analogue national identity schemes are being digitalised to include the electronic processing of personal data often accompanied by authentication via biometric data such as fingerprints and iris scans. These digitised national identity schemes may additionally ingest or link to demographic and biometric data and identifiers collected in other sector specific systems such as healthcare, social welfare or even mobile sim card registration or mobile device identity databases. National digital identity schemes seek to represent the [civil or] legal status of an individual and may affect and influence many aspects of a person's private life, including the private sphere of their digital activities. For example, a national digital identity may be used in the commercial sector, to provide identity assurance services or where a national digital identity is tied to a mobile number or device identifier in the private sector.

A key justification for digitising 'legal identity' and creating national digital identity schemes and systems (NIDS), is that they ensure and guarantee legal security and certainty but could also facilitate easier access to social and economic rights and entitlements and provide broader societal protections, such as personal and societal security. It is also suggested they offer benefits such as interoperability within and across borders, that they improve the accuracy and availability of data, and improve government decision making and the provision of public services and social protection measures.

While NIDS may bring significant benefits and protections in multiple contexts, and allow individuals to obtain and assert important rights, they may also have adverse consequences for the human rights of individuals *and* communities and groups of individuals. 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 even the misuse or theft of one's identity.

Further privacy risks for individuals arise due to the multitude of actors involved in the management of digital identity, including identity providers, service providers and third parties allowed to develop or use national digital ID systems, and to the fact that the use of digital identities by individuals can be tracked thereby allowing intrusive forms of surveillance and profiling.

‘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 and communities). Developments have also led to the linking 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 national digital identity systems into other systems, such as vehicle surveillance schemes[1], facial recognition[2] or facial verification schemes.

The Preamble in the Explanatory Report to Convention 108+ 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***.”[3] The increasing incorporation of biometrics into NIDS, that make people ‘machine readable’ carries the risk of reducing people to a mere object removed from considerations of human dignity and other adverse consequences for their human rights and fundamental freedoms.

NIDS can interfere with and have significant implications for human rights and fundamental freedoms and in particular the rights to privacy and protection of personal data which can be even greater in cases where biometric data are processed. Therefore, it is highly recommended that a domestic data protection law, aligned with Convention 108+, is first established to provide a foundational legitimate basis for rules and safeguards. A domestic data protection law should inform and be a prerequisite to the introduction of a NIDS.

Furthermore, given the potential for adverse impacts on human rights, NIDS should take a human right centred approach ~~also when dealing with data protection~~ and should explicitly integrate human rights considerations as anchored in international human rights law into the policy, design, implementation, and operation of national digital identity schemes and systems. These guidelines therefore support a privacy and human rights by design approach that includes the need for stakeholder engagement in identifying and assessing possible adverse impacts of NIDS on the interests and human rights and fundamental 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. This approach is also consistent with a former UN Special Rapporteur who in 2007 asserted that ‘‘*Human rights impact assessment is the process of predicting the potential consequences of a proposed policy, programme or project on the enjoyment of human rights*.”[4]

Legal and civil society challenges, whether from the UK, Kenya or Jamaica, 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, if NIDS are to succeed and establish necessary trust.

[1] ~~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~~

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

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

[4] Report of the Special Rapporteur on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health https://undocs.org/A/62/214

A human right centred impact assessment, reflecting Article 1 and Article 10 of Convention 108+, also engages rights holders in not only promoting the transparency of NIDS policy and practice, but in identifying their interests and perceived risks or actual risks experienced by rights holders and the potential adverse impact of NIDS on individuals and communities that would otherwise remain invisible. Engaging rights holders via such an approach, can help to ensure that the processing of personal data adequately respects individual and other applicable rights, that it is ultimately fair and transparent, while also strengthening awareness of rights. Stakeholder engagement may be considered an appropriate and necessary safeguard against risks to the interests, rights, and fundamental freedoms of individuals.

2. Scope and Purpose

2.1 These guidelines are general in scope, applying to the public and private sectors and to [civil or] legal identity that national digital identity schemes seek to represent. Nothing in these guidelines should be interpreted as excluding or limiting the provisions of the European Convention on Human Rights or of the Council of Europe Convention ETS No. 108 for the Protection of individuals with regard to automatic processing of personal data ('Convention 108'). There are also other specific instruments that may be equally relevant in the context of national digital identity schemes such as the *Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling*: or *Guidelines on facial recognition*[5]. These guidelines take into account and seek to apply the principles and other key provisions and safeguards of the Council of Europe Protocol CETS No 223 amending Convention 108 ("Convention 108+")[6] to the development and implementation of national digital identity schemes and systems (NIDS).

2.2 Drawing in particular on Article 10 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 but appropriately examine, consider and mitigate their potential adverse impacts on human rights and fundamental freedoms enshrined in relevant international instruments. It is intended that the guidelines will help ensure that NIDS respect and protect human rights and fundamental freedoms, from the policy phase through the design phase and all aspects of data processing.

2.3 The guidelines promote an objective assessment of all interests at stake including the benefits of such systems against the interference they might represent with human rights and fundamental freedoms of individuals, in supporting legitimate policy objectives while minimising risks to individuals, groups, and communities of individuals.

[5] https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751
[6] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

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

When considering the processing of personal data for fulfilling the objectives of NIDS, it is crucial to reflect on the Preamble and Article 1 of Convention 108+ and the need to secure human dignity, and to respect and secure human rights and fundamental freedoms of every individual.

Adopting a precautionary approach [and 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 particular, they emphasise the need for fair and transparent processing of personal data including by providing a strengthened protection to special categories of data such as biometric data.

Policy making, and the design, implementation and operation of national digital identity schemes should therefore help ensure NIDS do not adversely affect people's human dignity and other human rights and fundamental freedoms and that individuals are not reduced to 'mere objects'.

3.1 Legitimacy of processing

According to Article 5 of Convention 108+, personal data may only be processed on the basis of consent, or some other legitimate basis laid down by domestic law,. Article 6 of Convention 108+ further requires that the processing of special categories of data such as data revealing a person's ethnicity (often used in NIDS) or such as biometric data uniquely identifying a person, must be subject to appropriate safeguards enshrined in domestic law, complementing those of the Convention.

Taken into account the relationship between the state, citizens and other data subjects, it should be kept in mind that because of the imbalance of power between the controller and the data subject, consent could not be considered, in principle, as an appropriate legal basis for the processing of personal data by public authorities. Where, in individual cases however, the processing of data is based on consent as provided by Article 5(2) of Convention 108+, such consent must be freely given, informed, explicit and limited to a specific purpose. Consent must represent the free expression of an intentional choice by an individual. It must be taken into account that an imbalance of power between the controller and the data subject can also occur in relationships within the private sector (e.g. the employer - employee relationship). Therefore, in relationships between citizens and third parties allowed to develop or use national digital ID systems, care must be taken to ensure high standards to ensure the free will of individuals in expressing consent

-Personal data processing in NIDS must be necessary and proportionate and must have a specific legal basis laid down in domestic law and its implementation should be preceded by an impact assessment. NIDS must serve a legitimate purpose, such as the certification of the authenticity of a natural person legal identity in line with the country's constitution and applicable international law, rather than for expediency or being justified as 'desirable'. The law needs to define in an easily accessible and understandable form the scope of NIDS and the specific purposes of the processing of personal data including special categories

of data proposed under NIDS. It is recommended that the law is accompanied by an impact assessment which covers possible impacts on human rights and fundamental freedoms of individuals and groups, and which is made public prior to any processing of data. This must include an assessment of appropriate safeguards to limit and mitigate risks to the rights to privacy and to the protection of personal data.

Due to their intrusiveness and the potential in terms of surveillance over the activities carried out by the data subjects, the use of digital identity systems that serve to certify the authenticity of an individual's 'legal identity' before the law and vis-à-vis the State should not be made compulsory, and less intrusive alternatives should be ensured to individuals to have access to services.

3.2 Fairness and Transparency

Transparency is a core data protection principle as described by Article 5 paragraph (4)(a) of Convention 108+. It is of the utmost importance in helping individuals understand not only what of their data will be processed and why, but also of the implications of its use and of potential risks to their privacy and broader human rights and freedoms. Transparency is also key in ensuring people are aware of their rights and how they can exercise them. Based on the principle of fairness and because individuals will have especially high expectations of security of their information significant safeguards must be established to protect personal data against outsider threat and to prevent breach of assets and information.

In order to comply with this principle, NIDS should observe Article 8 of Convention 108+ as further explained by paragraphs 67 to 70 of the Explanatory Report to Convention 108+ which set out what information must be provided to individuals to ensure appropriate levels of transparency. The information can be made available at different levels or in layers (i.e. general information on the website, more detailed information in the enrolment form, etc.) provided that it contributes to the efficiency of receiving appropriate information and to the overall understandability of data processing foreseen under the NIDS. The information must be provided in an easily accessible form, preferably through digital device that allows the tracking of the personal data of respective individuals within the NIDS, and be legible, understandable, and appropriate to specific groups of individuals (for example individuals who may be blind or have low literacy). The information to be provided includes:

- providing individuals with the identity and habitual residence or establishment of the controller and how to contact them (individuals must know who is responsible for the collection and subsequent processing of their data and for respecting and complying with their rights, for example).communicating what categories of personal will be processed and for what explicit and specific purposes, including that their data will be used, or are intended to be used, in the context of profiling;[7]
- the legal basis relied on to process the data as per Article 5 and 6 of Convention 108+;
- the recipients to whom data will be disclosed or made available (for example, other public authorities or agencies);

[7] Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, adopted by the Committee of Ministers on 3 November 2021, 4.1.a)

- the existence of data protection rights afforded by Convention 108+ and how to exercise them, such as how to easily have inaccurately recorded data corrected and how to update their records (which should be free of charge);
- how to obtain redress.

Further information is recommended such as:

- whether the provision of data to establish a national digital identity is voluntary or, if no exemptions are applicable, mandatory (and if so, which law is relied on), 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 a 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);
- whether national digital identity (NID) data, such as a national identification number (NIN), will be shared with or accessible to other national identity dependent schemes or be required for such schemes and why. For example, whether national identity will be required to obtain a mobile sim card or to access education or healthcare services and what national identity data will be processed as a result;
- whether a NIN will be bound to other unique identifiers (and the lawful basis for this) such as a mobile phone number, a mobile sim card electronic identity number,[8] or electronic equipment number of a mobile phone,[9] 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 example;
- the basis for exclusion from NIDS (for example lack of proof of birth).

information related to the design and implementation of the systems and the operations applied for personal data processing, particularly where automated systems are used.

~~It is important that when NIDS lawfully require the processing of biometric data for authentication purposes and if they pass the necessity and proportionality test or any similar balancing test used in the domestic legal framework producing the same effect, an alternative means of inclusion is provided for those individuals who are unable to provide biometrics or whose biometrics are unreadable or whose biometrics become unreadable. This will help ensure fairness and prevent exclusion.~~

Fairness also requires that communications about NIDS and the processing of personal data are appropriate and intelligible to the diverse communities that NIDS are meant to serve.[10]

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 specify the legitimate and permitted purposes for which the processing of personal data, including special categories of data (such as biometric data uniquely identifying an

[8] ~~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~~
[9] ~~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~~
[10] See for example, paragraph 68 of the Explanatory report on Article 8 of Convention 108+.

individual) are considered lawful. It is to be recalled that those intended instances of processing involving personal data should also be *necessary* and proportionate to fulfil those purposes according to Point 3. This is necessary to meet the conditions for legitimate processing and purpose limitation of Article 5(4)(b) of Convention 108+ and to prevent data being processed for imprecise, vague or incompatible purposes. It is also necessary to meet the design obligations contained in Article 10 of Convention 108+.[11]

Controllers and other entities *providing* hardware, software and services that enable NIDS, should by design and ongoing measures, ensure that only those data necessary for a purpose specified under NIDS law or other appropriate legislation shall be processed. Where processing becomes incompatible with the specified and legitimate purpose, the data should not be processed further and should be deleted. It should be further noted that even if the personal data processing is carried out for the legitimate purposes, NIDS-related data should not be retained longer than is necessary and should be subject to applicable retention and disposition policies and procedures.

The subsequent 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 and if appropriate safeguards have been put in place.

As different attributes (such as civil identity, date of birth, address and more articulated ones), can provide a detailed picture of an individual's intimate sphere they can only be introduced in digital identity schemes if they are necessary and proportionate to the legitimate aim pursued.

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

Accurate

It is essential that measures are adopted to ensure the accuracy of any personal data processed, and that inaccurate personal data can be corrected or deleted in an efficient and timely manner notably to avoid significant adverse consequences for individuals' human rights and fundamental freedoms, such as exclusion from services or social protection measures, discrimination, incorrect criminal charges or false arrest and imprisonment for example.

When NIDS require the registration of biometrics and where biometric data may link to other identity-based systems such as facial recognition it is important to emphasise that according to the Guidelines on facial recognition[12] "*the use of facial recognition for the sole purpose of determining a person's skin colour, religious or other beliefs, sex, racial or ethnic origin, age, health or social condition should be prohibited unless appropriate safeguards are provided for by law to avoid any risk of discrimination*". It is worth noting that the mere presence of safeguards does not on its own justify the use of facial recognition technologies for the purpose described. Other considerations should factor into deciding whether to proceed with such a use-case, including the necessity of the technology, the proportionality

[11] 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).*"

[12] https://rm.coe.int/guidelines-facial-recognition-web-a5-2750-3427-6868-1/1680a31751

of the deployment given user needs and objectives, and the degree to which the technology poses a risk of harm or other adverse impact (e.g., identified via HRIAs).

The use of biometric data in NIDS requires additional measures to ensure the accuracy of biometric data acquired, enrolled and matched as well as during the performance of those aspects of NIDS that require a person to present their biometrics for proof of identity or authentication.[13] It also requires measures to reduce bias and inaccuracies in biometric identity techniques and technologies and to enhance fairness.[14] It is imperative that testing for 'accuracy' is a core requirement of a human rights by design approach and a condition to be fulfilled before the purchase and implementation of biometric identity technologies.

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. It should be noted here too that attributes which are not strictly necessary to such purposes (namely to identify the individual and allow the access to services) should be avoided. To achieve this, the purpose must first be defined, and an appropriate legal basis ensured – 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. Personal data should not be shared unjustifiably. The processing of personal data that would result in a disproportionate interference with the right to privacy and in connection with it with other human rights and fundamental freedoms of individuals and groups would be considered excessive under Convention 108+ and constitute an unlawful processing of personal data.[15]

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 information that is sufficient to meet a specified purpose in order to prevent the misuse or incompatible uses of biometric templates.

Data quality must form part of a cycle of continuing assessment and evaluation and adaption to findings and events.

Good data quality management practices can promote interoperability across systems/institutions/jurisdictions and 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.[16]

3.5 Data Retention

[13] 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

[14] 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

[15] Article 5 – Legitimacy of data processing and quality of data of the Explanatory Report to Convention 108+ paragraph 52

[16] 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

The retention of personal data of data must be proportionate and necessary for the specified and legitimate purposes pursued. Special attention should be paid to the retention of special categories of data, such as biometric data.

Data should be deleted or only preserved in a from that permits identification of an individual for no longer than it is necessary for the specific purpose for which the data are processed. This must include consideration of data processed in systems that are integrated with NIDS or that NIDS draw data from; for example, facial recognition systems or mandatory mobile SIM card registration systems or border control systems. It should be noted that common disposition standards could be highly beneficial in the elaboration of which supervisory authorities could play a leading role.

Moreover, 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.

3.6 Security of processing

NIDS involve the processing of (often sensitive) personal data at *population scale* and may even contain data on specific vulnerable and at-risk groups. A failure to ensure the security of data and systems can have serious adverse consequences for the human rights and fundamental freedoms of individuals, groups and communities of individuals.

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

The protection against third-party tracking of device information using a NIDS system should also be prevented.

'Appropriate measures' include:

- ensuring in the design and operation of systems, that by default only those personal data which are necessary for each specific purpose are processed;
- assessing the sensitivity of the data involved and the potential adverse effects for individuals and groups and adopting measures that are appropriate to mitigate possible adverse risks;
- adopting and implementing policies and procedures to investigate and manage security incidents that may have adverse impacts for individuals and for reporting such incidents to individuals and data protection supervisory authorities;
- adopting and implementing policies, procedures, and physical and technical measures to control access to systems and the data they hold or provide access to;
- encrypting data in transit and at rest and ensuring only trusted devices may access NIDS data;
- adopting and implementing procedures to investigate and address security weaknesses and to ensure 'security' measures are kept under regular review;
- providing internal and external processes for the confidential reporting of security vulnerabilities;[17]
- regularly testing the effectiveness of existing security measures and maintaining a log of such tests and actions taken/to be taken to address failings that might compromise the data and rights and freedoms of individuals;
- consider how to prevent the misuse of NIDS data and systems where these have been compromised and can be used to intentionally harm individuals, groups, and communities of individuals. Contingency plans should be in place to avoid disruptions to a critical or other services relying on national identity-related systems in the event of a compromise. These plans should identify backup systems and processes that can be activated to support impacted service operations.
- provide the data subject with specific tools to prevent identity theft (e.g., verification of accesses and of use of the identity).

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

- third party tracking can be mitigated with additional security barriers in the application to prevent the leak of information. As an extra precaution, a more in-depth information on issues such as applicable liability waiver shall also be made available upon access for individuals to inform them on the legal regime or contractual agreements concerning the data controller's legal responsibility in the case of third-party security breaches.

Another matter to consider for national supervisory authorities that provide or approve mobile apps to access to NIDS and related services, is not just the security of those apps, but whether they contain third party tracking code 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, if misused, may facilitate the profiling and electronic surveillance of individuals with the potential for significant adverse consequences for human rights.[18] 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.[19]

The creation and issuing of a unique, global permanent National Identity Number (NIN) should be avoided to help prevent profiling and associated risks, such as the monitoring of internet/digital activities of data subjects. Service or application specific NINs that are underpinned by appropriate safeguards are therefore preferable

Profiling (as described by the Recommendation on profiling[20]) should be avoided within national digital identity systems and associated systems unless expressly provided for by law. Any measures intended to enable profiling should be subject to an obligation to conduct a prior human rights impact assessment of individual and collective risks that profiling may present. Individuals should also be given access in line with Article 9 of Convention 108+ to rights-based measures (e.g., opt-out, redress, explanation) where profiling and automated decision making is used, and any exceptions to such rights must be clearly determined in accordance with Article 11 of Convention108+ [and be compatible with Article 8 of the European Convention on Human Rights].

3.8 Human Rights and Privacy by Design and Human Rights Centred Impact Assessments

Policy and design decision making of national digital identity schemes may adversely impact the interests, privacy and other human rights and fundamental freedoms of individuals, groups, and communities. 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*

[18] As eloquently deliberated in legal cases such as the ruling of the Supreme Court of Jamaica https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

[19] Recommendation CM/Rec(2021)8 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling: https://search.coe.int/cm/pages/result_details.aspx?ObjectId=0900001680a46147

[20] *idem*

manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms."

Of further note is the recommendation of the Committee of Ministers of the Council of Europe[21] ~~that parties to Convention108+ should require businesses to~~which stipulates that "*Member States should apply such measures as may be necessary to encourage or, where appropriate, require that: – business enterprises domiciled within their jurisdiction apply human rights due diligence throughout their operations; – business enterprises conducting substantial activities within their jurisdiction carry out human rights due diligence in respect of such activities; including project-specific human rights impact assessments, as appropriate to the size of the business enterprise and the nature and context of the operation~~apply and carry out human rights due diligence ... including project-specific human rights impact assessments, as appropriate~~.*" As NIDS may be a combination of public and private arrangements and **technologies the** obligation to carry out due diligence and human rights impact assessments should apply equally to the public and private sector when considering the adoption of NIDS.

Also of note is the Recommendation of the Committee of Ministers[22] on the human rights impacts of algorithmic systems which furthermore recommends that human rights impact assessments should be mandatory for all algorithmic systems that have high risks to human rights and that "*States should ensure that they, as well as any private actors engaged to work with them or on their behalf, **regularly and consultatively conduct human rights impact assessments prior** to public procurement, during development, at regular milestones, and throughout their context-specific deployment to identify risks of rights-adverse outcomes.*" It seems to be of high importance that mitigation measures corresponding to the risks identified are also to be put in place. The use of categorisation of risk of an algorithmic system based on criteria of reversibility and expected duration: (i.e., automated decisions with little to no impact are reversible and brief, while those with a very high impact are irreversible and perpetual) as applicable already in some jurisdictions could also be considered to enhance trust and improve transparency.

Based on the above, and given that national digital identity schemes may incorporate algorithmic systems and decision making, these guidelines seek to ensure a privacy and human rights-based approach to national digital identity

This human rights centred approach also requires identifying and engaging stakeholders (stakeholder engagement), and in particular affected rights holders. This will help identify not only risks to NIDS but also to the interests and human rights and fundamental freedoms 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

Stakeholder engagement is crucial to identifying, considering and mitigating risks to rights holders that national (digital) identity schemes (NIDs) may give rise to. Stakeholder

[21] 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

[22] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems, adopted 8 April 2020 https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154

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.[23] 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.

An obligation to undertake stakeholder engagement is consistent with Article 10 and in particular paragraph 90 of the Explanatory Report to Convention 108+ that allows for additional obligations to take into consideration the risks at stake for the interests, rights and fundamental freedoms of 'data subjects. Such risks may remain invisible without effective stakeholder engagement. Stakeholder engagement is recommended as an appropriate and necessary safeguard against risks to the interests, rights, and fundamental freedoms of individuals.

Annex A to this guidance suggests key stakeholders considered crucial to consult within the context of national digital identity schemes. Annex B to this guidance provides an example stakeholder engagement approach.

These guidelines, suggest adopting a human rights centred impact assessment to reflect to Article 1 of Convention 108+ and also Article 10 of Convention 108+. The approach seeks to integrate human rights considerations into the policy, design, implementation, and operation of NIDS. Such an approach ensures that data protection tools and instruments contribute to the wider consideration and protection of individuals' human rights and fundamental freedoms. This approach helps to proactively and explicitly identify and consider the potential for adverse impacts of data processing in the context of NIDS on a broad range of human rights beyond privacy, consistent with Article 1 of Convention 108+.

The approach includes the requirement for controllers to examine the likely impact of the intended data processing on the rights and fundamental freedoms of individuals *prior* to the commencement of such processing. Controllers are further required to design data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

This approach also incorporates the need to consider the moral, ethical and social values[24] of human rights given by international human rights instruments such as the European Convention on Human Rights (ECHR)[25] and the Universal Declaration of Human Rights[26]. Such an approach forces policy makers and controllers to consider whether a programme may exclude categories of individuals or lead to discrimination for example. At the policy level alone, this approach can assist in assessing the proportionality of a proposal and even pre-

[23] 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

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

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

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

empt adverse impacts. 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.[27]

Resources linked in this document may help policy makers, regulators, controllers, and providers of identity technologies understand key components of a human rights centred impact assessment approach.[28] International standards on identity registration schemes – 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.[29]

3.9 Accountability

A key requirement of Convention 108+[30] and modernised data protection laws is that 'controllers' and where applicable, processors 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.

Moreover accountability (as described in this section), as well as guaranteeing the right of individuals (Section 3.10), are paramount for ensuring the protection of personal data and the protection of human rights. The inclusion and maintenance of these guidelines as well as to ensure a continuous transparency and regular threat and risk assessment are essential for the legitimisation of NIDS.

In this respect it is suggested that applicable organisations should apply the accountability principle throughout key stages of NIDS and 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 upon;
- 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;

[27] 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
[28] 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 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
[29] For example, the International Standards organisation has developed frameworks and standards on identity management, identity proofing, biometric identity assurance such as ISO/IEC24760-1 '**Information technology — Security techniques — A framework for identity management'**. See https://www.iso.org/home.html
[30] Article 10

- 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 by evaluating existing or previous instances of data processing, leveraging documentation and other relevant evidence concerning a NIDS;
- 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 them;
- 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 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 with the inclusion of all stakeholders (e.g., universities, NGOs, government organisations, industry experts).

3.10 Right of individuals

Article 9 of Convention 108+ gives individuals a number of rights over the processing of their personal data. The rights must be established in law and apply 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[31] *only* when provided for in law, constituting a necessary and proportionate measure in a democratic society for specific and legitimate public interest purposes defined in law, and always respecting the essence of fundamental rights and freedoms.

Individuals must be informed 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 legal 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, the use of automated systems to process their data, particularly in cases involving legally significant decisions;
    - 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;

[31] Article 11 Convention 2018+

- the right to have inaccurate data corrected (free of charge and without excessive delay);
- the right to have their data erased (free of charge) where the processing of their data is contrary to the provisions of applicable law (such as data protection law/national digital identity law);
- the right to restrict the processing of their data;
- the right to object to the processing of their personal data;
- the right not to be subject to a decision significantly affecting them based solely on the automated processing of their data without having their views taken into consideration;
- 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+).
- the right of data subjects of automated decisions to explanations describing how a decision was reached and providing relevant information about the system and related data inputs and outputs

4. Recommendations for policy and decision-makers

Policy makers, whether members of parliament, legislators, 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 digital identity schemes.

Policy makers and decision makers should:

- ensure that the goal of NIDS is rooted in the constitution and applicable international law, well-defined, evidence-based, and proportionate and necessary for the legitimate purpose pursued;
- adopt a human-rights centred national policy;
- consider ~~to integrate~~integrating into national legislation a human rights impact assessment (HRIA) ~~approach~~ that extends the data protection impact assessment (DPIA) to explicitly integrate further human rights considerations into the policy, design, implementation, and operation of national digital identity schemes and systems (NIDS).
- establish regulatory forums by which ~~they~~ data protection regulators and other supervisory authorities that have a role in NIDS can come together to ensure effective compliance, address risks, and develop best practice.
- ensure that policy and the development of law are informed by stakeholder engagement and participation and that stakeholders have an opportunity to contribute to and review policy and law prior to adoption;
- publish the results of stakeholder engagement;
- specify in law, that the processing of personal data and special categories of data in particular, shall only be allowed for specific and legitimate purposes and on a specific legal basis;
- specify that consent to data processing shall only serve as a legal basis where all conditions for consent are met and in particular, where the free will of individuals is ensured;
- ensure that the adoption of appropriate safeguards is a requirement in policy and law including that special categories of data require the adoption of additional safeguards;
- require that NIDS are subject to cyber security and resilience assessments and obligations given their role in becoming part of critical national infrastructure and services;

- require human rights centred impact assessments and the regular monitoring of human rights impacts of NIDS on rights holders - from policy development, to law, to design, implementation, and operation of NIDS;
- support the development of a privacy and human rights by design methodology and guidance reflecting Article 10 of Convention 108+ and best practice;
- ensure that national identity law includes an obligation requiring transparency of processing and rights (as described above), 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;
- establish an independent oversight function with powers of audit and corrective enforcement measures;
- plan for the mitigation of harms arising from the compromise of NIDS, such as the theft of data, denial of service attacks and other forms of cybercrime as defined by the Council of Europe Convention ETS No. 185 on cybercrime (Budapest Convention) and its additional Protocols[32], the appropriation of national identity systems to intentionally cause harm to individuals or categories of individuals;
- criminalise possible attacks against and by means of computers in relation ~~the misuse of data collected and further processed for the purposes~~ of NIDS in line with the Budapest Convention. For example, the selling of data or misuse of data for financial benefits.

5. Recommendations for controllers

Controllers as defined in Article 2 of Convention 108+ – whether a public or private entity – should follow the guidance set out in this document. However, this guidance does not replace applicable data protection law and which controllers must comply with when processing personal data and special categories of data such as biometric data uniquely identifying an individual. They must have due regard for risks to the rights and freedoms of individuals and be able to demonstrate that their processing complies with applicable data protection/privacy laws.

Controllers should:

- consider appointing a data protection officer with appropriate knowledge and understanding of data protection law (and in particular its application to NIDS);
- ensure appropriate staff are adequately trained in data protection and privacy and the impact of the collection and use of data on broader human rights;
- adopt effective policies and measures to ensure data are processed only on an appropriate legal basis, and to ensure data quality, transparency, and other key data protection principles in particular that individuals are provided with all relevant information, including about their rights so they can easily exercise them;
- adopt data policies and measures supporting the lifecycle management and governance of data of which the ongoing evaluation and maintenance of data quality is part
- ensure where consent is relied on as a legal basis, that it takes place only with the free will of individuals and that it appropriately allows individuals to remain in control of their data throughout the various processing activities;
- develop and adopt human rights centred impact assessment and privacy and human rights by design methodology, to prevent exclusion or discrimination or other unlawful adverse consequences;

[32] Full list (coe.int)

- provide a point of contact by which individuals may raise concerns or questions about the collection and further processing of their data;
- implement effective technical and organisational measures to safeguard against risks to individuals;
- ensure that data sharing between controllers may only take place based on appropriate legal grounds and subject to appropriate data protection standards as described in these guidelines;
- ensure appropriate access controls are maintained in view of NIDS-related data, particularly in view of personal and special categories of data that restrict access to national identity systems and specific records, to authorised individuals and devices, and maintain a record of such access;
- prevent the profiling of individuals unless expressly provided for in law and when appropriate safeguards have been put in place;
- ~~It is important that~~ help ensuring fairness and preventing exclusion when NIDS lawfully require the processing of biometric data for authentication purposes ~~and if they pass the necessity and proportionality test or any similar balancing test used in the domestic legal framework producing the same effect,~~ an alternative means of inclusion ~~is~~should be provided for those individuals who are unable to provide biometrics or whose biometrics are unreadable or whose biometrics become unreadable. ~~This will help ensure fairness and prevent exclusion.~~

6. Recommendations for manufacturers, service providers and developers

Manufacturers of equipment, service providers and developers of software used in national identity systems should adopt key data protection principles of Convention 108+ to ensure respect for an individual's human rights and fundamental freedoms. These commercial entities may be impacted by virtue that the controllers and processors who they provide equipment and services to, are required to comply with applicable data protection law – and are obliged to design the processing of data in ways that consider and prevent or minimise risks to the interests, human rights, and fundamental freedoms of individuals. Or such entities may themselves process data to test hardware and software for example.

To enable controllers and processors to comply with Convention108+ such entities should ensure that the hardware, software and services they provide in support of National Identity Systems are designed to ensure data quality, purpose limitation, data minimisation; that data are not retained for longer than necessary for a specified purpose; that data are erased appropriately; that data are processed only on a specified legal basis and that systems provide for the exercise of rights by individuals (including the right of correction, access or erasure).

Article 5 of Convention 108+ requires that data shall be:

- processed accurately and kept up to date. This means that National Identity Systems must be designed to ensure a change of name can take place – caused by deed poll or marriage for example - or for the correction of an inaccurately recorded name, or a change in a person's biometrics that make unusable a current biometric template;
- adequate, relevant, and not excessive. This means that National Identity Systems must be designed to process only the minimum data necessary to fulfil a purpose

specified in law, and that the data and the processing operation must be fit for purpose – e.g., adequate, and relevant to fulfil a legitimate purpose.

Article 6 of Convention 108+ applies to processing of special categories of data such as biometric data uniquely identifying an individual or data about a person's racial or ethnic origin. Article 6 requires that appropriate safeguards are enshrined in law to protect against risks to the interests, rights, and freedoms of individuals. Article 10 of Convention 108+ further requires that data protection requirements (and appropriate safeguards) are integrated as early as possible, "*ideally at the stage of architecture and system design in data processing operations*."[33]

Manufacturers of equipment, providers of services and developers of software used in National Identity Systems should take steps to meet the requirements of these guidelines and Convention 108+ and applicable national data protection law.

7. Recommendations for Supervisory Data Protection Authorities

First and foremost, supervisory authorities (SAs) should play an effective and active role in supporting enforcement of national and other applicable data protection laws in line with Chapter IV of Convention 108+.

Article 15(3) of Convention 108+ imposes an obligation on states to ensure SAs are consulted on proposals for any legislative measure or administrative measure involving the processing of personal data. Policy makers and legislators should therefore ensure that SAs are consulted as key stakeholders, beginning with the formulation of national policy on NIDS, and throughout the legislative process.

Linked to the right of an SA to be consulted on measures such as NIDS, an SA also has the authority to issue an opinion on data processing operations that present risks to the rights and freedoms of individuals that NIDS may present. An SA should consider issuing such opinions on any consultation pursuant to Article 15 of Convention 108+ on any aspect of proposals to introduce or amend a NIDS where the proposed processing presents risks to rights and fundamental freedoms.

Article 15 also imposes obligations on SAs to promote public awareness of their activities – this should include the SA's engagement and specific activities related to NIDS and include periodical reports. This is consistent with the crucial role of an SA as advocate for data protection and privacy, in ensuring that National Digital Identity Schemes and Systems incorporate Convention 108+ provisions and applicable national data protection law. SAs are in positions of authority and have expertise that impacted rights holders do not have and by which they can help ensure the interests of rights holders are duly considered in NIDS – from policy to practice.

[33] Paragraph 89 to the Explanatory Report of Convention 105+

Supervisory authorities can work with key stakeholder groups on raising awareness of key considerations of the impact of NIDS on human rights and freedoms of appropriate measures to reduce risks to them. SAs can contribute to policy, law and the development of guidance or legally binding codes of practice.

SAs should be invited to be part in any decision considering a human rights impact assessment (HRIA) approach that extends the data protection impact assessment (DPIA) to explicitly integrate human rights considerations into the policy, design, implementation, and operation of national digital identity schemes and systems (NIDS).

Data Protection Authorities should consider ~~establishing~~ participating in regulatory forums by which they and other supervisory authorities that have a role in NIDS can come together to ensure effective compliance, address risks, and develop best practice.

It is also recommended that the independent external oversight of NIDS is ensured by SAs or they are involved in it in an appropriate way.

8. Glossary

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: Data resulting from a specific technical processing ~~data~~ concerning the physical, biological or physiological characteristics of an individual which allows his/hers unique identification or authentication.

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.

Convention 108+: the Protocol (CETS No 223) amending the Convention for the protection of individuals with regard to the processing of personal data (Convention ETS No 108)

HRbD: means privacy and human rights by design. Ensuring respect for, and the protection of, human rights from policy, to regulation, to technology design, to the processing of personal data.

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 **uniquely identifiable** in given contexts.

National Digital Identity Schemes/System (NIDS): a combination of policy, law, and technology by which a person's 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 to a person assigned a legal identity and by which an individual can be uniquely identified by reference to verified attributes 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: refers to any form of automated processing of personal data, including use of machine learning systems, consisting in the use of data to evaluate certain personal 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 complementing those of Convention 108+.

Supervisory Authority: an authority established as per Article 15 of Convention 108+ for ensuring compliance with the provisions of the Convention.

Annex A - Suggested list of Stakeholders
This list is not exhaustive but includes:

- **Government**
  - Key government departments, agencies and ministries with responsibility for:
    - Information Communications Technology
    - Digital policy
    - Digital Agenda and Economy
    - Health Care
    - Education
    - Birth registration/civil population registration
    - National Identity
    - Border Control and Immigration
    - National Security and Law Enforcement
    - Social Protection
    - Indigenous Affairs
    - Refugees
    - Procurement
    - Data Protection
    - Human Rights
    - Discrimination Issues
- **Parliament**
  - Committees with a human rights and technology, digital economy, identity focus
- **National regulatory bodies** that have a human rights related mandate and responsibilities
  - Data Protection Authorities (Privacy, data, and information commissioners)
  - Human rights or equalities commissions[34] or commissioners
  - Biometric Commissioners
  - Surveillance Commissioners
  - National Identity Commission
  - Telecommunications Authorities
- **Judiciary/Redress**

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

- Ombudsman with human rights/social justice mandates/responsibilities[35]
- Bar associations
- Community based organisations that support the resolution of human rights redress

- **Rights holders and representatives**
  - Community representatives
  - Civil society / Human rights organisations[36]
  - Citizens councils

- **Business sector**
  - ID vendors – hardware and software
  - Industry associations
  - Mobile operators[37]
  - 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[38]
- **International Actors**
  - Humanitarian organisations
  - World Bank
  - UN organisations [39]
  - International Telecommunications Union (ITU)
  - Organisation for Economic Co-operation and Development (OECD)
  - African Union
  - African Commission for Human Rights
  - Council of Europe

[35] 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

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

[37] 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

[38] 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/

[39] 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

- EU[40]

Annex B – Example stakeholder engagement approach

The following tables have been adapted directly from the Danish Institute for Human Rights 'Stakeholder Engagement Practitioner Supplement'[41] 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.			

[40] 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

[41] 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)*
		Patients/students where services require proof of NID. Mobile phone subscribers that require proof of NID.			
	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.			

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)*
	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			
	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			

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)*
		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'.			
	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.			

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)*
	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.	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.

TABLE B: Examples of steps to take prior to engaging directly with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
	• 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.	
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. • 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).	• consider the numbers of individuals to engage, their positions within communities and what 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.

TABLE B: Examples of steps to take prior to engaging directly with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
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.
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

TABLE B: Examples of steps to take prior to engaging directly with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
		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 • 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	**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. 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.

TABLE C: Examples of steps to take during the interview or meeting with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
	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.	
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.	
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 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.

TABLE C: Examples of steps to take during the interview or meeting with stakeholders		
Steps	**Process**	**Areas for further attention and considerations**
	• 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)	
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. • 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.