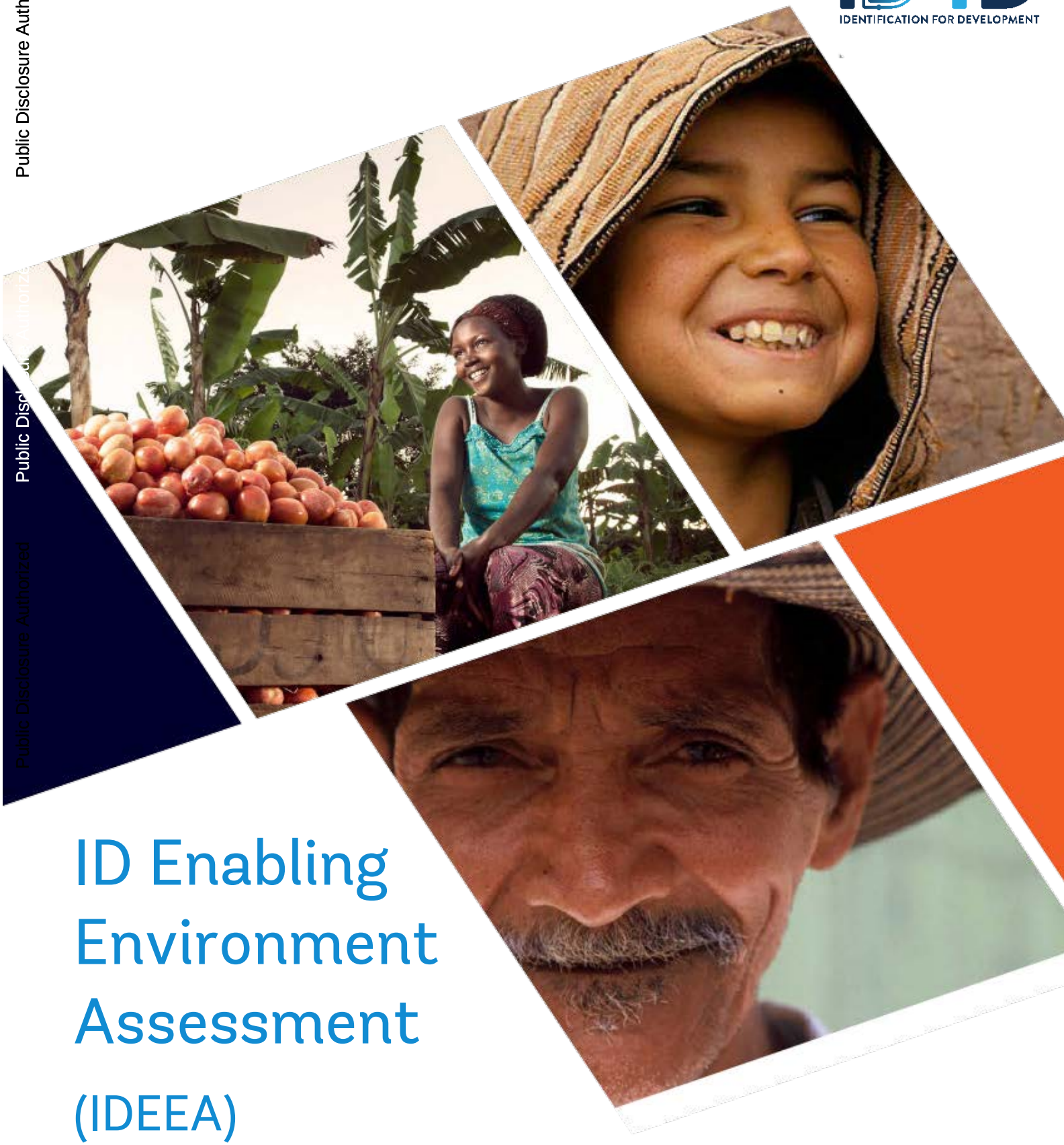
ID4D
IDENTIFICATION FOR DEVELOPMENT



ID Enabling Environment Assessment

(IDEEA)

GUIDANCE NOTE

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Photo credits: left photo by Stephan Gladieu/World Bank, top photo by Curt Carnemark/World Bank, and bottom photo by Scott Wallace / World Bank Collection.

Disclaimer

This ***Guidance Note*** is an explanatory commentary on the diagnostic tool ***ID Enabling Environment Assessment*** (IDEEA). These are designed together to support the review and analysis of a given country's legal and regulatory enabling environment for digital identification (ID) systems. Both the IDEAA and this Guidance Note are based on evolving international good practice. As diagnostic tools, they are not intended as a basis for legislation, but rather as a basis for broad, multi-stakeholder consultation on what a country may consider including in its legal and regulatory framework.

Both the IDEEA and this Guidance Note are "living" documents, which are intended to be updated from time to time. They reflect experience in a range of countries from different regions, with different legal systems and at different stages of economic development. They also take account existing literature (for example, on national ID, civil registration and vital statistics and citizenship, data protection and privacy, cyber-security, etc.), international conventions, norms and principles (including the Principles on Identification, available at: http://pubdocs.worldbank.org/en/200361509656712342/web-English-ID4D-IdentificationPrinciples.pdf).

This is version 2.0 of the IDEEA issued on 15 May 2019.

There is no guarantee that addressing all the issues raised in the IDEEA or this Guidance Note will result in a perfect or even workable legal and regulatory enabling framework for ID in a country – that will depend on many exogenous factors to be factored into a legislative strategy, which may be different from country to country. The information in this version of the Guidance Note is "as of" October 2018. All citations to laws or cases are for illustrative purposes, recognizing that these may be reversed, repealed, amended, etc., over time.

Contents

Introduction

This Guidance Note

Before rolling out any ID program, governments need to assess existing ID systems and registries and the relevant social, economic, legal and institutional context, a process that may be carried out with support from the World Bank or other development partners.

In World Bank supported engagements, the initial assessment of a country's identity ecosystem, comprising the set of existing ID systems and their interconnections within a country, often takes the form of an **ID4D Diagnostic**.[1] The ID4D Diagnostic is a process that reviews *foundational ID systems* created to provide general identification of the population for a wide variety of purposes. It also surveys key *functional ID systems* created to manage identification for a particular service or transaction, such as voting, tax administration or social programs.[2] (See the introductory text to Part I of this Guidance Note for further explanation of foundational and functional ID systems.) The ID4D Diagnostic involves desk review, field mission interviews and data collection, drafting of a report, and conduct of a validation workshop with stakeholders.

The **ID Enabling Environment Assessment (IDEEA)** builds on and is a supplementary tool to the ID4D Diagnostic. It is a due diligence questionnaire intended to facilitate a systematic assessment of a country's existing ID systems alongside an examination of its enabling laws and regulations, and institutions. It is designed to generate a country profile which may be used to identify areas where administrative and legal frameworks might be strengthened to support the development of digital ID.[3]

To ensure that the legal and regulatory review is carried out in context, the IDEEA includes a range of questions about the purpose, design, usage, institutions and cultural context surrounding a country's national ID and civil registration systems. It takes the form of a checklist requiring "yes or no" answers and other ratings, often to be supplemented by explanations.

This **Guidance Note** is an explanatory commentary on the IDEEA questionnaire. It provides background on the reasons why the questions are asked and guidance for those participating in the assessment on how to approach answering them. Its explanations and examples from international practice are also intended to allow persons in the country being assessed to benefit from the experience of other countries and wider international trends in digital ID, inclusion, privacy and data protection.

Sustainable Development Goals

Goal 16: "Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels"

Target 16.9: "by 2030 provide legal identity for all including free birth registrations"

The purposes of World Bank support

The review of any identification program should include an assessment of its main purposes and uses. ID programs should be designed to ensure that they serve productive purposes. Digital technologies facilitate positive outcomes such as economic opportunity and growth, increased transparency, reductions in fraud, enhanced efficient delivery of public services and the promotion of free movement of persons. But these outcomes are not inherent in digital systems and care must be taken to ensure that the digital ID systems are not used for inappropriate ends, such as promoting partisan political movements or broad surveillance of populations.

The target of Sustainable Development Goal 16.9 (to provide by 2030 "legal identity for all including free birth registrations") and developments in technology create the conditions in which Bank-financed ID programs can make a world of difference. Ensuring that "good practice" considerations are evaluated and included in each ID project will help ensure that Bank-financed digital ID projects fulfil a productive purpose and avoid political considerations.

[1] The ID4D Diagnostic assessment tool is the successor to the Identity Management System Analysis (IMSA). See World Bank Group, *Guidelines for ID4D Diagnostics*, 2018 at 1.

[2] World Bank Group, *Guidelines for ID4D Diagnostics*, 2018 at 2.

[3] World Bank Group, *Guidelines for ID4D Diagnostics*, 2018 at 2:

Key principles for digital ID

The IDEEA places significant emphasis on inclusion, privacy and data protection.[4] These issues are key to public trust and thus for successful deployment of, participation in and usage of national ID systems.[5] Trust that government will deal responsibly with personal data, and not intentionally or unintentionally use an ID system to exclude any person from exercising their rights or accessing services, is important to the success of a national identification scheme. If individuals feel that privacy is not protected or that the data about them is not safeguarded or that the ID system may be applied in a discriminatory manner, they may withhold data, supply inaccurate data or simply avoid participating.

The World Bank and over 20 key partners therefore developed a set of 10 principles on the themes of inclusion, design and governance that frame their work on digital ID and set them out in *Principles on Identification for Sustainable Development: Toward the Digital Age*. These are considered fundamental to maximizing the benefits of identification systems for sustainable development while mitigating many of the risks.[6]

The 10 principles are derived from and reinforced by international practice and principles that are widely agreed upon at international and national levels. Many of these principles are not only embedded in law and policy, but in codes of ethics of industry organizations and standard setting bodies.[7]

ID systems involve collection, storage and use of personal data. This means that data protection and privacy laws are particularly relevant. Such laws typically have provisions and principles specific to the collection, storage and use of personal data, requiring it to be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data.

Principles on Identification for Sustainable Development: Toward the Digital Age

INCLUSION: UNIVERSAL COVERAGE AND ACCESSIBILITY

1. Ensuring universal coverage for individuals from birth to death, free from discrimination.

2. Removing barriers to access and usage and disparities in the availability of information and technology.

DESIGN: ROBUST, SECURE, RESPONSIVE, AND SUSTAINABLE

3. Establishing a robust—unique, secure, and accurate—identity.

4. Creating a platform that is interoperable and responsive to the needs of various users.

5. Using open standards and ensuring vendor and technology neutrality.

6. Protecting user privacy and control through system design.

7. Planning for financial and operational sustainability without compromising accessibility.

GOVERNANCE: BUILDING TRUST BY PROTECTING PRIVACY AND USER RIGHTS

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.

9. Establishing clear institutional mandates and accountability.

10. Enforcing legal and trust frameworks though independent oversight and adjudication of grievances.

World Bank and endorsing agencies, 2017

The list above is drawn from Article 5 of the *2016 EU General Data Protection Regulation* (GDPR).[8] The GDPR also requires the data controller to be responsible for, and be able to demonstrate compliance with the above principles.

Annex II to this Guidance Note lists these principles from Article 5 of the GDPR and illustrates their relevance to ID systems. The GDPR has attracted much global attention as a recent legislative initiative in comprehensive regulation of data protection and privacy, and it is an important reference point for work in this area. Some of the newer rights and duties it

[4] World Bank Group, *Guidelines for ID4D Diagnostics*, 2018 at 2.

[5] World Bank, *Identification for Development Strategic Framework*, 2016 at 10.

[6] *Principles on Identification for Sustainable Development: Toward the Digital Age*, facilitated by World Bank Group and Center for Global Development, February 2017.

[7] See, e.g., Secure Identity Alliance Code of Conduct and the Jericho Forum Identity, Entitlement & Access Management (IdEA) Commandments.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). The GDPR supersedes the *1995 EU Data Protection Directive.*

introduced when it took force in 2018 remain the subject of debate in policy circles and a number of legal questions remain about their application in practice.

However, the GDPR's key principles mentioned above and discussed in Annex II largely have their origins in earlier European law, U.S. law[9] and international practice,[10] and are not new or particular to Europe or the GDPR. Prominent examples of internationally recognized frameworks include:

- the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* which sets out internationally recognized core principles on the collection and management of personal data;[11]
- the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), which in its current form has been ratified by 54 countries (7 of which are outside of Europe) and sets out principles for the collection and processing of personal data that is subject to automatic processing;[12] and
- the *2004 APEC Privacy Framework*, which was updated in 2015 and sets out a principles-based model for domestic privacy legislation in the APEC region.[13]

This Guidance Note has drawn on these frameworks as part of its explanations and examples of data protection and privacy principles that are reflected in the questionnaire.

The principles found in the GDPR are also reflected in one form or another in a large number of national data protection and privacy laws outside Europe, largely due to general recognition of their merit.

For instance, California enacted the Consumer Privacy Act 2018 introducing some of the rights, duties and remedies provided for in the GDPR. These principles have also spread internationally, in part, due to the obligations the European Union imposes on its Member States to ensure that personal data relating to European citizens is protected when it is exported to, and processed in, countries outside Europe. Also, the GDPR applies to the processing of data of any individual who is "in the Union" regardless of the location of the processing of the data. These factors encourage other countries seeking to interact with Europe in digital services and non-European companies who are likely to process data of Europeans to adopt similar protections.

Even in those settings where the GDPR does not directly apply, the principles it embodies, and which are reflected in the 10 principles above, reflect current "best practices" in a variety of jurisdictions and sectors representing a significant portion of the global data economy. Those principles therefore form a basis for consensus and interoperability for systems that handle personal data. It is for this reason that the IDEEA and this Guidance Note have turned to these principles to frame the due diligence process.

[9] E.g., US HEW report U.S. Department of Health Education and Welfare (HEW) (1973). Records, computers and the rights of citizens: report of the Secretary's Advisors Committee on Automated Personal Data Systems, *U.S. Government Printing Office* (available at http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm).

[10] For example, the OECD's Guidelines on the Protection of Privacy and Transborder of Personal Data and http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[11] Guidelines on the Protection of Privacy and Transborder of Personal Data .

[12] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108 . Convention 108 has recently been updated to align it more with GDPR and has been dubbed "Convention 108 +" (*see*, https://www.coe.int/en/web/data-protection/convention108/modernised). Convention 108 + has not at the time of this writing entered into force.

[13] https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015) .

IDEEA Questionnaire and Commentary

Guidance to IDEEA user

This IDEEA Questionnaire elicits information about the country's identification (ID) systems and the legal and regulatory framework in which they operate. Such information is intended to assist those considering supporting the development of existing or new digital ID systems to assess where the legal and regulatory framework may need to be strengthened. It should inform considerations of what kind of support may be needed, where it should be focused, and how much effort it may require.

Depending on what kind of ID system is envisaged, and the manner in which it is intended to operate, the output from this IDEEA Questionnaire should assist in evaluation of the chief risks under the existing legal and regulatory framework, and whether that existing framework likely needs incremental improvements or substantial reforms, or whether a new framework needs to be built from scratch.

The Questionnaire is organized along the lines of the three themes of the *Principles on Identification for Sustainable Development: Toward the Digital Age*, namely inclusion, design and governance in order to facilitate evaluation of the information obtained in accordance with those principles.

Part I. The ID system landscape

Guidance to the IDEEA user

The questions this in Part I seek to identify significant identification systems, both digital and paper-based, currently in place that may play a significant role in development of a national, digital ID system in the country, and set the parameters for the rest of the IDEEA questions.[14]

An **identification system** comprises the databases, processes, technology, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose.[15] A **digital ID system** is an identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.[16]

ID systems are sometimes described in terms of whether they are "foundational" or "functional":

- **Foundational ID systems** provide general identification and credentials to the population for public administration and a wide variety of public and private sector transactions, services, and derivative credentials. Common types of foundational ID systems include civil registries, national IDs, universal resident ID systems, and population registers.[17] A **national identification system (NID)** is a foundational identification system that provides national IDs (NIDs)—often in the form of a card—and potentially other credentials. In many countries, a primary function of national ID systems has been to establish and provide recognition and proof of citizenship and/or residency status.[18]
- **Functional ID systems** are created to manage the identity lifecycle for a particular service or transaction, such as voting, tax administration, social programs and transfers, financial services, and more. Functional identity credentials—such as voter IDs, passports, health and insurance records, tax ID numbers, ration cards, driver's licenses, etc.—may be commonly accepted as proof of identity for broader purposes outside of their original intent, particularly when there is no foundational ID system.[19] This arrangement is sometimes referred to as a

[14] This IDEEA is focused on systems that have been formally established. Self-asserted or self-sovereign IDs (created by individuals) and de facto IDs (comprising attributes that accumulate with engagement in the digital economy) are generally not likely to be covered.

[15] ID4D Glossary, World Bank, available upon request.

[16] Ibid.

[17] Ibid.

[18] Ibid.

[19] ID4D Glossary, World Bank, available upon request.

"federated identity" system. Functional ID systems may be "federated" to expand their application and serve the broader goals of a foundational system,

As mentioned above, civil registries, or civil registration systems, are included as foundational ID systems. A **civil registration system** is the continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population, as provided through decree or regulation in accordance with the legal requirements of each country.[20] Although the legal origins of civil registration systems may differ from that of many ID systems, they raise sufficiently similar legal and regulatory issues about data protection, privacy and inclusion that they are treated alongside other foundational ID systems in this IDEEA.

ID systems are often implemented by national governments through ministries, departments or agencies. In federal systems, significant ID systems implemented by state or local governments ought to be considered as well. Also, in some countries, ID systems implemented by international institutions or relief organizations function as a *de facto* form of national ID and these should be considered in answering the questions in this Part I.

1. *Existing foundational and functional ID systems:*

a. *Is there a civil registration system? ..... [Y/N]*

If so, identify the responsible government ministry or department:

_____

b. *Is there a separate **foundational** ID system? ..... [Y/N]*

*Identify each **foundational** system and the responsible government ministry or department and, if there is more than one foundational system, briefly describe the differences:*

_____

_____

c. *Is there a voter ID system? ..... [Y/N]*

d. *Are there any other **functional** ID systems which are currently used (either nationally or regionally) or have strong potential to be expanded for use, for general ID purposes? ..... [Y/N]*

e. *If so, describe the primary function of each (including any voter ID system) and which ministry or department of government is responsible. The purpose here is only to capture the key systems that could be developed into general national ID systems or offer important lessons for the assessment, and **not** every functional ID system that exists.*

Key functional ID system	Describe primary uses and any distinguishing features	Responsible ministry or department (if any)

f. *If multiple foundational and functional ID systems have been identified above, is there an agency, ministry or other entity responsible for harmonization, recognition or coordination among the systems? ..... [Y/N]*

g. *If so, identify the entity:*_____

Background

The distinction between foundational and functional ID systems is not always clear cut. In some cases, particularly when a foundational ID system is absent or underdeveloped, a functional ID system can evolve (through "federation" of the ID system) to take on a broader role, even serving as a *de facto* foundational ID system. For example, in the United States, social security numbers were originally just a functional ID system used to track income for social security eligibility. Over time the system has taken on more of a foundational role as social security numbers are in practice used for many purposes, such as for tax collection, credit evaluation and financial transactions, some of which are required by law. The use of the UK National Insurance number, Ethiopian kebele ID and Nigerian certificate of indigeneity similarly extend beyond their initial purpose.

[20] *Ibid.* UN Department of Economic and Social Affairs, Statistics Division, *Principles and Recommendations for a Vital Statistics System (Revision 3)*, 2014, para 279.

In countries with no foundational ID system or one that is still developing, an existing functional ID system that is already used more broadly for general ID purposes or a civil registration system may serve as a starting point for designing or enhancing a foundational ID system. Such existing functional ID systems might be deployed nationally or only within a certain region of a country. In order to capture the current landscape of ID systems, and the potential they hold for facilitating a digital national ID system, it is thus useful to understand all existing foundational and significant functional ID systems.

Civil registries record a variety of personal attributes, and these may sometimes be used for identification purposes. (For further information on the meaning of "attribute," see Question 60.) A voter ID system is a functional ID system which raises some of the same identity validation and data protection issues found in other ID systems. Both civil and voter registration systems thus can have an important role in development of national ID systems.

Civil registration systems and voter ID systems may be completely separate from other ID systems, may be integrated into another ID system, or may be separate with certain linkages. Those linkages can include one or more connections in operations, enforcement or rulemaking for the ID system. Many of the questions addressed in the IDEEA relating to ID systems generally are relevant to both civil registration systems and voter ID systems. For this reason, civil registration systems and voter ID systems are addressed in Part II alongside other systems.

Part II. Questions about generally applicable laws and regulations

Guidance to IDEEA user

Part II reviews the wider country conditions, particularly laws and regulations that apply generally and are relevant to the development and operation of digital ID systems.

Some ID systems may be subject to laws and regulations applicable specifically to the individual system. These should be addressed in Part III, which concerns the design, governance and legislative framework specific to individual foundational and key functional ID systems in the country. See also the introductory text in Part III.

The Legal System and Sources of Law

2. *In the table below, tick the row(s) that describe traditions present in the country's legal system.*

Descriptions of legal system	Tick
Common law tradition	
Civil law tradition	
Religious law *(specify):* _____	
Other(s) *(specify):* _____	

3. ***International conventions:*** *In the table below, indicate which international conventions and agreements the country is party to (and the date it joined) or has indicated it intends to join.*

Binding Conventions and Agreements		
Global	Current party & date	Intention to join
Convention relating to the Status of Refugees, 1951 (Articles 27-28 require states to provide every refugee with a means of identifying him or herself in the form of either a valid travel document or identity papers)		
Convention Relating to the Status of Stateless Persons, 1954 (addresses the legal status of stateless persons and provides for basic minimum standards of protection)		
Convention on the Reduction of Statelessness, 1961 (aimed at ensuring that national laws and practices do not result in statelessness, by providing minimum safeguards)		
International Covenant on Civil and Political Rights, 1966 (Article 17 on the right to privacy)		
International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), 1969		
Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1980; revised 2016 (open to all countries in the world)		
Convention on the Rights of the Child, 1989 (addresses birth registration)		
Convention on Cybercrime (Budapest Convention), 2001		

Inclusion

4. ***Constitutional provisions, laws, regulations and policies relating to discrimination, minorities, citizenship:*** *Indicate in the table below provisions of the Constitution (or equivalent foundational document) or relevant legal, regulatory or policy documents that address these topics and summarize the provisions.*

Issue	Relevant provisions of the Constitution (if any)	Laws and regulations	Government policies
National or other ID systems		Addressed in Part III	Addressed in Part III
Recognition as a person before the law			
Non-discrimination (specify if on the basis of gender, race, ethnic origin, religion, etc.)			
Protection of minorities (specify if gender, race, ethnic origin, religion, etc.)			
Defining and determining citizenship and other legal status			
Treatment of non-citizens (in the case of residents, foreigners, refugees and stateless individuals)			
Other relevant topics *(specify):*			

Background

Target 16.9 of the UN Sustainable Development Goals (SDGs)—a universal set of development objectives for 2030 that were agreed in 2015 by all UN member States —is to "provide legal identity for all, including birth registration." This target contributes to goal 16, which is to "promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels". [21]

Ethnic, racial or linguistic minorities may be at special risk of exclusion from ID systems, particularly where these minorities already face forms of exclusion or discrimination that are built into the country's legal system. An ID system may also increase the ability to identify members of these groups and more systematically implement the exclusion or discrimination.

On the other hand, some legal systems provide enhanced rights or benefits for marginalized or vulnerable groups. While an ID system may increase the ability of members of these groups to qualify for or access these rights or benefits, the ability of service providers or the community to identify them as members of the group may result in other forms of informal exclusion or discrimination.

[21] For a brief background to the Sustainable Development Goals (SDGs), see Liz Ford, "Sustainable development goals: all you need to know", 19 January 2015, *The Guardian* online. See also World Bank, "WDR16 - Spotlight on Digital Identity", 2015.

Design

Data protection and privacy

5. *Data protection and privacy laws, regulations and policies:*

a. *Are privacy and/or data protection protected in the country's constitution? ..... [Y/N]*

b. *If so, cite and quote/summarize:*

_____

Background

While legislation is a common means of establishing the various legal principles that are required to ensure trust, in some countries constitutional provisions are the original source of these rights.

Examples

The Constitution of **Kenya** provides that "every person has the right to privacy." This right includes "the right not to have information relating to their family or private affairs unnecessarily required or revealed."[22]

The Constitution of **Portugal** contains a detailed provision on information technology which gives citizens a right of access to computerized data about themselves and a right to require corrections and updates to that information. It also requires that personal data be administered by an independent entity, forbids the storage of certain data which could be the basis of discrimination without the explicit consent of the subject, and prohibits the allocation of a single national number to any citizen.[23]

The Constitution of **Turkey**, as amended in 2010, also contains a detailed provision on personal data rights, which includes the rights to be informed of personal data collection; rights of access, correction and deletion; and the right to be informed if personal data is being used consistently with the intended purpose.[24]

The Constitution of **Hungary** gives every person "the right to the protection of his or her personal data, and to access and disseminate data of public interest", and requires that the exercise of these rights must be supervised by an independent authority. [25]

The Constitution of the **Netherlands** requires that rules protecting privacy in connection with the recording and dissemination of personal data, and individual rights to be informed of and to correct recorded data concerning them, must be set forth in legislation.[26]

The Federal Constitution of **Brazil** provides a right of "*habeas data*" as one of the fundamental rights, thereby giving individuals the right to access their own personal data as held by government agencies or "agencies of a public character", and the right to correct such data.[27]

The Constitution of **Spain** provides generally for the protection of personal and family privacy and states that the law must restrict the use of data processing in order to guarantee the honor and the personal and family privacy of citizens and the full exercise of their rights.[28]

c. *Is there a general law(s) governing personal data protection and/or privacy? ..... [Y/N]*

d. *Are there sector-specific personal data protection and/or privacy laws? ..... [Y/N]*

e. *If so, cite and quote/summarize:* _____

[22] Article 31, Constitution of Kenya, 2010.

[23] Article 35, Constitution of the Portuguese Republic Seventh Revision [2005], in English translation (alternatively at this website). (For more details, see Eduardo Soares, Senior Foreign Law Specialist, "Online Privacy Law: Portugal", Library of Congress, June 2012.)

[24] Article 20.A, Protection of Private Life, paragraph added 12 September 2010; Act No. 5982, in English translation:

[25] Article VI, Hungary's Constitution of 2011, in English translation:

[26] Article 10, Constitution of the Kingdom of the Netherlands, in English translation.

[27] Article 5 (LXXII), Constitution of the Federated Republic of Brazil, 3rd edition, 2010, in English translation.

[28] Section 18(4), Spanish Constitution, 1978, as it appears in English translation.

Background

As of September 2018, 107 countries, including 66 developing or transition economies, have adopted legislation to safeguard data protection and privacy.[29]

f. *Have there been any significant court or administrative decisions that form the basis of or clarify privacy or data protection rights? ..... [Y/N]*

g. *If so, describe:* _____

Background

As constitutional provisions are often cryptic, judicial interpretation is often crucial in determining the contours of privacy rights. In addition, even where there is no specific constitutional reference to privacy (e.g., the USA and the Republic of Ireland), courts have developed these rights from the language of other constitutional provisions.

Examples

In 2015, the Supreme Court of **Mauritius** considered the constitutionality of a new identity scheme.[30] The National Identity Card Act[31] placed a legal duty on every adult citizen of Mauritius to apply for an identity card and to "allow his fingerprints, and other biometric information about himself, to be taken and recorded," with failure to comply being punishable by a criminal sanction. After holding that the Constitution of Mauritius does not contain a general right of privacy, the Court turned to the assertion that the ID scheme violated Article 9(1) of the Constitution on "Protection for privacy of home and other property." The court concluded that the *taking* of fingerprints in accordance with the applicable legal framework answers a pressing social need and, taking into consideration the safeguards provided and the relatively limited degree of interference with privacy which this entails, proportionate to the legitimate aim pursued.[32] However, the same conclusion did not apply to the *retention and storage* of the biometric data for an indefinite period, which was deemed unconstitutional.

In a 2008 case, the Supreme Court of **Japan** held that an individual's name, birth date, address, sex and resident number are not confidential, and found that the online interconnection of local government databases containing this information to the national "Jūki Net" system did not violate the right to privacy which has been read into the Constitution over the years. The Court noted that the database was secure against leaks of information, that possible misuse of the data by people handling the information was prohibited by administrative and criminal sanctions, that institutional structures to ensure proper handling of identification information had been established, and that the system did not entail the disclosure of personal information to a third party or make such information public without good reason. The Court therefore held that Jūki Net did not violate the right to privacy.[33]

In **France**, the *Conseil Constitutionnel* in 2012 invalidated a law which aimed to introduce a new eID card with an electronic chip containing information on marital status, residence, height and eye color as well as biometric information in the form of digital fingerprints and digitized face images.[34] The law established a national database for this information and provided for access to this database by various agencies. Access was provided to verify identity for the purpose of identity cards and travel documents, for the investigation of certain criminal offences (if authorized by the public prosecutor or the examining judge), and to establish the identity of a deceased person in the wake of a natural disaster or accident. The Council ruled that large portions of this law violated the constitutional right to respect for private life, being disproportionate to the goals pursued. The law ultimately enacted in the aftermath of this ruling provided that national ID cards and passports could contain name, sex, date and place of birth, home address, height, eye color, digital fingerprints and a photograph. However, this information is now accessible only to the agents responsible for verifying the identity of an individual who presents an electronic passport or ID card.

In August 2017, a nine-judge bench of the Supreme Court of **India** found that the right to privacy is a fundamental right protected by the Indian Constitution.[35] In September 2018, the Supreme Court issued a majority judgment examining whether certain aspects of the Aadhaar ID system violated this right. The majority noted the importance of balancing the fundamental right to privacy with fundamental rights "to food, shelter and employment." They held that mandatory use of

[29] UNCTAD, Global cyberlaw tracker, as of 217 September 2018. A 2017 measure puts the number at 120. See Greenleaf, Graham, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey (January 30, 2017). (2017) 145 Privacy Laws & Business International Report, 10-13; UNSW Law Research Paper No. 17-45.

[30] *Madhewoo v The State of Mauritius*, 2015 SCJ 177, Record No. 108696; see also *Jugnauth v The State of Mauritius* 2015 SCJ 178, Record No.108728, which cited *Madhewoo* and reached the same conclusions.

[31] National Identity Card Act (Mauritius), as amended by section 15 of Act 20 of 2009.

[32] Madhewoo v The State of Mauritius, at 28 of the slip opinion.

[33] Supreme Court of Japan, 2007 (O) 403 (Mar. 6, 2008), MINSHŪ Vol 62 No 3, available in English on the website of the Supreme Court of Japan at www.courts.go.jp/app/hanrei_en/detail?id=1276.

[34] *Decision n° 2012-652 DC on the Law regarding the identity protection,* 22 March 2012 (in French and in official English translation).

[35] *Justice Puttaswamy v. Union of India*, Writ Petition (Civil) No 494 of 2012, Supreme Court of India, judgement delivered on 24 August 2017.

the Aadhaar system to receive subsidies, benefits and services "whereby Government is doling out such benefits which are targeted at a particular deprived class" did not amount to a violation of the right to privacy.

h. *Do the laws and decisions specified above apply equally to public versus private entities? ..... [Y/N]*

i. *If not, explain: _____*

A. Data protection and privacy principles

Guidance to IDEEA user

Various principles are widely acknowledged to apply to the treatment of personal data. (See "Key principles for digital ID" in the Introduction to the IDEEA.) This section A explores the extent to which these general principles are enshrined in law, regulation or policy in the country in question. Even if they are not provided for specifically in relation to individual ID systems discussed in Part III, such general principles and associated obligations, rights, procedures and remedies may be applied to improve the design of existing ID systems or as the basis of new ID systems that may be introduced.

6. ***Lawfulness:*** *Does any law, regulation or policy require that the collection and use of personal data be done on a lawful basis? Examples of lawful bases include collection undertaken with consent, due to contractual necessity, in compliance with legal obligation, for the protection of vital interests, the public interest and/or other legitimate interest (or similar standards).....[Y/N]*

If so, cite and quote/summarize: _____

7. ***Fairness and transparency:*** *Does any law, regulation or policy require that the collection and use of personal data be done fairly and transparently (or similar standard), such as requiring the data subject to be informed of the purpose of data collection and intended use and sharing of the data?..... [Y/N]*

If so, cite and quote/summarize: _____

8. *Purpose limitation, proportionality and data minimization:*

a. *Does any law, regulation or policy require that the collection and use of personal data be made for a stated purpose (or similar standard)?..... [Y/N]*

If so, cite and quote/summarize:_____

b. *Does any law, regulation or policy require that the collection and use of personal data be proportionate, relevant, adequate and/or limited to the purpose for which it is collected (or similar standard)?..... [Y/N]*

If so, cite and quote/summarize:_____

Background

Purpose limitation is a data protection principle (see the Introduction to this Guidance Note) that limits the collection and use of personal data to purposes:

- which are stated in law and thus can be known (at least in theory) to the individual at the time of the data collection; or
- for which the individual has given consent.

The principle of **proportionality** requires that data collected must be proportionate to the purpose of the ID system. This is often articulated as requiring only the "minimum necessary" data should be collected to fulfil the purpose. Collection of additional data unnecessarily raises privacy risks and potentially impacts the effectiveness of the system. The more data that is collected, the more likely it is that it can be misused. By identifying the types of data that are necessary to fulfil specified purposes, a system can be designed to exclude collection of unnecessary data.

The term "function creep" is sometimes used to describe the situation where data originally collected for one purpose is used for other purposes.36 A legal and regulatory framework for an ID system will often set out the contemplated purposes for which data will be collected and used. There may also be mechanisms in place to monitor and ensure compliance with these purpose limitations.

[36] See generally, for example, Els J. Kindt, *Privacy and Data Protection: Issues of Biometric Application, A Comparative Analysis*, Heidelberg, Dordrecht, New York, London: Springer, 2013.

Examples

Purpose limitation need not be rigid and absolute, but it is typically tightly bounded in an effort to curb any unanticipated secondary uses of collected data that might harm individual interests. Even the protection against individual intrusion is not absolute, and it is balanced in situations where the data yields insight into important or urgent matters of security. For example, the **EU**'s GDPR contemplates exceptions to purpose limitation in some circumstances to safeguard various matters including national security, defense, public security, and the prevention, investigation, detection or prosecution of criminal offences, among other issues. However, these exceptions must be enacted through legislative measures which "respect the essence of the fundamental rights and freedoms" and are "necessary and proportionate."[37] Further, the principle of data minimization under the GDPR means that any data collected as part of an ID system will need to be:

- adequate (i.e. sufficient to properly fulfil its stated purpose);
- relevant (i.e. has a rational link to that purpose); and
- limited to what is necessary (i.e. no more than necessary for that purpose).

For example, if collecting data about race, ethnicity or religion is not actually necessary for the purpose of identifying an individual (i.e. if they could be identified using other data) then it would likely be contrary to the principle of data minimization to collect this data.

In the **United Kingdom**, the Data Protection Act 2018 specifically provides that "personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed." In addition, the UK Data Protection Act 2018 provides that personal data collected for a law enforcement purpose may be processed for any other law enforcement purpose provided that: a) the controller is authorized by law to process the data for the other purpose, and b) the processing is necessary and proportionate to that other purpose. Importantly, personal data collected for a law enforcement purpose may also be subject to the purpose limitation, as such data may not be processed for a purpose that is not a law enforcement purpose unless authorized by law.[38]

9. ***Data quality:*** *Does any law, regulation or policy require that the collection and use of personal data be accurate, complete and up to date (or similar standard)?* ..... *[Y/N]*

If so, cite and quote/summarize: _____

10. ***Accountability:*** *Does any law, regulation or policy require that persons or entities collecting and using personal data take responsibility for and be capable of demonstrating compliance with applicable data protection requirements?* ..... *[Y/N]*

If so, cite and quote/summarize: _____

11. ***Sensitive personal data:*** *Does any law, regulation or policy require additional protections for collection and use of sensitive personal data (e.g., information relating to race, ethnicity, religion, political beliefs, sexual orientation, health, etc.)?* ..... *[Y/N]*

If so, cite and quote/summarize: _____

12. ***Storage limitations:*** *Does any law, regulation or policy require that personal data not be kept longer than is necessary for the purposes for which it is processed (or similar standard)?* ..... *[Y/N]*

If so, cite and quote/summarize: _____

13. ***Privacy by design or default:*** *Does any law, regulation or policy require ID systems, or other systems collecting and using personal data to incorporate privacy-by-design or privacy-by-default principles or use privacy-enhancing technologies (PETs)?* ..... *[Y/N]*

If so, cite and quote/summarize: _____

Background

"Privacy by design" or "privacy by default" refers to reflecting privacy measures and privacy-enhancing technologies (PETs) in the conceptualization and architecture of data systems.[39] PETs refer to a coherent system of measures that protect privacy by eliminating or reducing the collection of personal data, preventing unnecessary or undesired processing of personal data, and facilitating compliance with data protection rules without losing the functionality of the data system in

[37] 2016 EU General Data Protection Regulation, Article 23.

[38] The Data Protection Act 2018, Article 36.

[39] See European Agency for Network and Information Security (ENISA), *Privacy and Data Protection by Design*, 12 January 2015.

question. Examples include provision for automatic anonymization or deletion of data after a certain time period and encryption tools.[40]

Examples

The EU's GDPR introduced new obligations requiring organizations to adhere to the principles of privacy by design and default so that privacy and data protection issues are considered at the outset in the design phase of any system, service, product or process and then throughout the lifecycle of that system.[41]

B. Data security

14. ***Data security:*** *Do any laws, regulations or policies require that personal data be stored and processed securely, protected against unauthorized or unlawful processing and accidental loss, destruction or damage (or similar standard)?(See also Questions 75—80)* ..... *[Y/N]*

Indicate in the table below the legal or regulatory source of any generally applicable security requirements.

Requirement	Law, regulation or policy	Applicable to which ID systems identified in Part I
Encryption of personal data		
Anonymization of personal data		
Pseudonymization of personal data		
Confidentiality of data and systems that use or generate personal data		
Integrity of data and systems that use or generate personal data		
Availability of data and systems that use or generate personal data		
Resilience of data and systems that use or generate personal data		
Ability to restore data and systems that use or generate personal data after a physical or technical incident		
Ongoing tests, assessments and evaluation of security of systems that use or generate personal data		
Others (specify):		

15. ***Data loss or breach:*** *Do any laws, regulations or policies require physical, technical or administrative safeguards to prevent loss, leakage or theft of personal data and provide for notification and remedies if they occur?* ..... *[Y/N]*

If so, cite and quote/summarize: _____

Background

Data breaches can result from multiple sources both intentional and accidental, including employees who fail to follow proper procedures, hackers who gain access to inadequately-protected databases, and thieves who steal inadequately-secured portable devices. They may be the product of a lack of adequate safeguards or oversight, but ultimately it is impossible to make a complex computerized system completely immune from a breach. The risks are magnified in the case of a large, centralized database that holds personal data.

Breach notification laws generally require data controllers to inform individuals and/or authorities that a breach has occurred. Many international standards similarly impose a duty on data controllers to notify data subjects of significant data breaches affecting their personal data. Appropriate remedies may need to be tailored to the specifics of the breach.

[40] See "Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)", 2007.

[41] 2016 EU General Data Protection Regulation, Article 25 and Recital 78.

Examples

The **EU's** GDPR requires notification to the supervisory authority of any personal data breach "without undue delay and, where feasible", within 72 hours of becoming aware of it "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons." The notification must detail certain data about the breach including the categories and approximate number of data subjects concerned and the likely consequences of the breach.[42] Similarly, subject to some exceptions, notification to the individual data subjects affected must take place "without undue delay" if the breach "is likely to result in a high risk to the rights and freedoms of natural persons" and such notification shall have at least the same data that needs to be notified to the supervisory authority.[43]

Almost every state in the **United States** has a breach notification statute, typically requiring private or governmental entities to notify individuals of security breaches involving personally identifiable data and setting out what constitutes a security breach, notice requirements (such as timing and method), and exemptions (such as for encrypted data).[44]

In **South Africa,** the Protection of Personal Information Act 4 of 2013 (most of which was not yet in force as of August 2018) requires the Information Regulator, the national supervisory authority, to notify the data subjects of breaches as soon as reasonably possible after their discovery of the compromise - taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system. The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach including. The Information Regulator may direct the responsible party to publicize information about the security breach if this would protect individuals who may be affected.[45]

In **South Africa**, a 2017 data breach resulted in the leak of the personal details of more than 30 million citizens. The Southern African Fraud Prevention Service (SAFPS) reminded consumers of the ability to apply for a free service which provides added security and can alert a credit provider or bank that a specific ID number has been compromised.[46]

C. Data sharing

16. *Limitations on data sharing:*

a. *Do any laws, regulations or policies authorize, restrict or otherwise address sharing of personal data with third parties?* ..... *[Y/N]*

b. *If so, cite and quote/summarize:* _____

c. *Indicate any laws, regulations or policies that govern the provision of notice and/or receipt of consent to data sharing or disclosure of such sharing to individuals:*

_____

Background

Because the linkage of data across databases intensifies privacy and data protection concerns, legal frameworks can mitigate risks by stipulating *all* the purposes for which personal data in an ID system is shared, both with and by government and non-government entities. In addition, public entities may be limited to obtaining specific data justified by their functions (i.e., the "need-to-know" principle).

Data sharing can take place even without the technological compatibility of interoperability. For example, police could contact ID officials or directly interface with ID systems to access data relating to an individual of interest, including biometrics, address or names of family members. Potential benefits of data sharing include:

- convenience for both government and citizen;
- better government service delivery;
- seamless service transfer when data subjects change address;
- improved risk management;

[42] 2016 EU General Data Protection Regulation, Article 33

[43] 2016 EU General Data Protection Regulation, Article 34.

[44] "Security Breach Notification Laws", National Conference of State Legislatures (NCSL), 6 February 2018.

[45] Protection of Personal Information Act 4 of 2013 (South Africa), section 22 ("Notification of security compromises").

[46] Pumza Fihlani, "Millions caught in South Africa's 'worst data breach'", *BBC News-Johannesburg*, 20 October 2017; "What to do when your data has been leaked", *African News Agency*, 20 October 2017; SAFPS website, undated.

- cost savings as duplication of effort is eliminated; and
- improved efficiency through more effective use of data.[47]

However, data-sharing between government agencies (and even between government agencies and commercial entities), if not well-regulated, can turn into a "back door" which allows circumvention of individual privacy and data protection safeguards. Comprehensive population databases, like those established as part of foundational ID systems, are a particularly tempting resource for law enforcement authorities, particularly when they contain biometric markers.

Examples

Under the EU's GDPR, certain principles must be followed in order for personal data sharing to be lawful. These include ensuring that there is a lawful basis for the sharing to take place, the individuals have been made aware data about them is being shared, ensuring the minimum amount of personal data is shared and the sharing is done as securely as appropriate for the data involved. In addition, where the recipient is acting as a processor of the personal data and the sharing facilitates the processing, a written contract is required to be in place between that party and the organization sharing the data setting out certain specific requirements in relation to the processing.

d. *Indicate any laws regulations or policies that limit sharing of persona data to the minimum extent required to perform a particular function, e.g., for criminal investigation (or a similar standard):*_____

e. *Is it legally permissible for biometric data about an individual (as opposed to the results of a sanctioned authentication) that is held by a government agency ever to be shared with any other person or entity?..... [Y/N]*

f. *If so, under what circumstances and what is the legal or regulatory source of this power?*

g. _____

Background

Policymakers and courts have struggled with striking the appropriate balance between protecting the privacy of registrants and supporting criminal investigations. One approach to such matters could be to apply the same rules that apply to other forms of searches and seizures in the country in question, such as a requirement that a warrant be obtained. This may be beneficial where a balance between personal privacy and public interest has already been struck in this regard.[48]

Examples

Article 4(2) of the EU *2016 Police and Criminal Justice Data Protection Directive 2016/680* requires that personal data collected for some other purpose – which could be for an ID system or for civil registration – can be processed by the same or another controller for crime-related purposes *only* in so far as: (a) there is legal authorization for this *and* (b) such processing is necessary and proportionate to the purpose for which the personal data was collected.[49]

In 2013, the European Court of Justice touched on the issue of information-sharing in a case which challenged the capturing of fingerprints in EU passports. The Court recognized the risk of such function creep, noting the usefulness of comparing fingerprints taken in a particular place with those in a database for purposes of criminal investigation or surveillance. However, no such use was involved in the case which was actually before the Court, so it did not make a finding on the limits of permissible use for such purposes.[50] In a 2015 case involving Dutch passports, the Fourth Chamber of the European Court of Justice found that the EU regulation on passports does not require Member States to guarantee in their national legislation "that biometric data collected and stored in accordance with that regulation will not be collected, processed

[47] See, e.g., Stephanie Perrin, Jennifer Barrigar & Robert Gellman, "*Government Information Sharing Is Data Going Out of the Silos, Into the Mines?"* (independent research report commissioned by the Office of the Information and Privacy Commissioner of Alberta, Canada), Digital Discretion Inc., January 2015 at ii.

[48] See a discussion of access to photo databases for purposes of facial recognition in the US without any requirement of reasonable suspicion or probable cause in Alex Pasternack, "The Vast, Secretive Face Database That Could Instantly ID You In A Crowd", 30 March 2017, *Fast Company* (American business magazine) website. For a similar UK debate on the issue general police access to health databases without a warrant, see, e.g., Randeep Ramesh, "Police will have 'backdoor' access to health records despite opt-out, says MP", *The Guardian*, 6 February 2014; Alan Travis, "NHS hands over patient records to Home Office for immigration crackdown", *The Guardian*, 24 January 2017; Alan Travis, "NHS chiefs urged to stop giving patient data to immigration officials", *The Guardian*, 31 January 2018.

[49] See, e.g., "The directive on protecting personal data processed for the purpose of criminal law enforcement", 27 September 2016, Council of the European Union website.

[50] *Michael Schwarz v Stadt Bochum*, Judgment of the Court, 17 October 2013, ECLI:EU:C:2013:670, at paragraphs 56-64.

and used for purposes other than the issue of the passport or travel document, since that is not a matter which falls within the scope of that regulation".[51]

In **India**, the *Aadhaar Act 2016* provides for the disclosure of information, excluding "core biometric information," pursuant to an appropriate court order, which can be made only after the government authority responsible for IDs has been given an opportunity to give input on the disclosure. It also provides for the disclosure of information, including core biometric information, "in the interest of national security" on the direction of government officers above a certain rank, where this has been authorized by an order of the central government and reviewed by an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government in the Department of Legal Affairs and the Department of Electronics and Information Technology.[52]

A broader exception to the principles of personal data protection is provided in **South Africa**, where the *Protection of Personal Information Act 4 of 2013* provides that further processing of personal information will not be considered incompatible with the purposes for which the data was collected if the further processing is necessary "to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences," "in the interests of national security" or "to prevent or mitigate a serious and imminent threat to public health or public safety; or the life or health of the data subject or another individual" (amongst other exceptions). The independent Information Regulator established by the Act also has the power to issue exemptions by notice for further processing of personal data if the public interest in such further processing "outweighs, to a substantial degree" any resulting interference with the privacy of the data subject" or "involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree" any resulting interference with the privacy of the data subject or third party; the "public interest" for this purpose includes "the interests of national security" and "the prevention, detection and prosecution of offences," among other things.[53]

In **Australia**, the federal *Privacy Act 1988* (as amended) contains as one of its "Privacy Principles" the rule that personal information about an individual collected for a particular purpose must not be used or disclosed for another purpose without the individual's consent. However, there is an exception for situations where the use or disclosure is "reasonably necessary" for the enforcement related activities conducted by or on behalf of an enforcement body – which includes use or disclosure by police for prevention, detection, investigation, prosecution or punishment of criminal offences – as well as an exception for uses and disclosures authorized by law or by court order. Use for enforcement related activities must be noted in writing as a mechanism to promote accountability.[54]

h. *Do the police and other investigative authorities have the power to collect DNA data specifically?..... [Y/N]*

i. *If so, under what circumstances and what is the legal or regulatory source of this power?*

_____

Background

Particular concerns arise in relation to collection of **DNA** data which, like other biometric data, may be used not only for the purposes of identifying an individual, but also as evidence in the process of investigating whether he or she has committed a crime.

Example

These have been the subject of several cases in the **United States**, whose courts have upheld laws requiring the collection of DNA from persons arrested but not yet convicted for felonies. In 2013, the US Supreme Court held that collecting DNA is (like fingerprinting and photographing the suspect) a legitimate police booking procedure that is reasonable and does not violate US constitutional protections against unreasonable searches and seizures. The majority opinion joined by five justices considered that the use of DNA for *identification* purpose and checking an arrestee's criminal history is no different from matching an arrestee's face to a wanted poster of a previously unidentified suspect or matching the arrestee's fingerprints to those recovered from a crime scene. It also emphasized that collection of the DNA sample was a minimally-invasive procedure (a cheek swab), that the DNA processing used for identification purposes does not reveal any genetic traits of the arrestee, that the statute at issue included sanctions for any unauthorized use of the DNA samples collected, and that the DNA samples taken were required to be destroyed if the arrest did not lead to a conviction. This led to the conclusion that the minimal invasion of privacy is outweighed by the legitimate state interest in correct identification of the arrested person. The four dissenters argued that the real purpose of the DNA samples was not identification, but rather

[51] *Joined Cases C-446/12 to C-449/12*: W.P. Willems v Burgemeester van Nuth, (C-446/12), H.J. Kooistra v Burgemeester van Skarsterlân (C-447/12), M. Roest v Burgemeester van Amsterdam(C-448/12), L.J.A. van Luijk v Burgemeester van Den Haag (C-449/12), Judgment of the Court (Fourth Chamber) of 16 April 2015 (request for a preliminary ruling from the Raad van State — Netherlands), ECLI:EU:C:2015:238, at paragraph 54.

[52] Aadhaar Act 2016, section 33. See Ankur Sharma, "Aadhaar body snubs police seeking biometrics", The New Indian Express, 2 July 2017.

[53] Protection of Personal Information Act 4 of 2013, sections 15(3), 37. As of February 2018, these provisions had not yet been brought into force.

[54] Privacy Act 1988 (including amendments up to Act 92 of 2017), section 6 (general definitions) and Schedule 1, Australian Privacy Principles, clause 6; Australian Government Solicitor, "Privacy Act reforms – implications for enforcement functions", Factsheet No 27, May 2013.

an attempt to connect a known individual to previously unsolved crimes, and thus would have found the collection of DNA samples to be an unconstitutional *investigative* measure that takes place in the absence of any basis for suspicion.[55] These pros and cons have obvious applicability to data-sharing from ID databases.

In 2018, also in the **USA**, DNA from a family genealogy database was used to identify the culprit in a long string of serial rape and murder cases dating back to the 1970s and 1980s. Law enforcement officials matched DNA from the crime scene to a distant family member and then charted that relative's family tree to locate a family member of the appropriate age, description and area of residence, whose DNA turned out to match that collected from the crime scenes. This case has prompted public discussion of the privacy issues raised by such law enforcement techniques, such as whether people who volunteer their DNA for genealogy are meaningfully consenting to all the ways in which it might be utilized. It also raises the issue that an individual who consents to the collection and use of his or her own DNA may be implicitly compromising the privacy of his or her extended family members, both past and future.[56]

Cyber threats

17. *Addressing cyber threats:*

   a. *Does the country have any laws, regulations or policies designed to identify and mitigate cyber threats? ..... [Y/N]*

   b. *If so, cite and quote/summarize:* _____

   c. *Does the country have any institutions or coordination mechanisms (e.g., a Computer Emergency Response Team (CERT)) tasked with ensuring the protection of infrastructure, systems and data from cyber threats? ..... [Y/N]*

   d. *If so, cite and quote/summarize:* _____

   e. *Briefly assess the extent to which these institutions have sufficient infrastructure and financial, technical and human resources to perform their powers and duties:*

      _____

   f. *Are these institutions established by law, regulation or policy? ..... [Y/N]*

   g. *If so, cite and quote/summarize:* _____

18. *Criminalized activities:*

   a. *Does any law criminalize unauthorized access to ID systems or other databases holding personal data? ..... [Y/N]*

   b. *If so, cite and quote/summarize:* _____

   c. *Does any law criminalize unauthorized interception of data from ID systems or other databases holding personal data? ..... [Y/N]*

   d. *If so, cite and quote/summarize:* _____

   e. *Does any law criminalize unauthorized damaging, deletion, deterioration, alteration or suppression of data collected or stored as part of ID systems or other databases holding personal data? ..... [Y/N]*

   f. *If so, cite and quote/summarize:* _____

   g. *Does any law criminalize unauthorized interference with ID systems or other databases holding personal data? ..... [Y/N]*

   h. *If so, cite and quote/summarize:* _____

[55] *Maryland v King* 569 US 435 (2013), upholding the Maryland DNA Collection Act. In the case before the Court, a man who was arrested for assault was matched by means of the DNA sample he was required to provide in terms of this law with a rape committed several years previously. The US has embarked upon a project known as the Combined DNA Index System (CODIS) that seeks to standardize collection and storage of DNA profiles at local, state, and national level. All 50 US states require the collection of DNA from persons *convicted* of felonies, but national opinion is more sharply divided on the collection of DNA from persons arrested but not yet convicted of serious crimes. A California state law requiring DNA samples to be taken from all persons arrested for any felony was approved by state voters in 2004 and narrowly upheld against a constitutional challenge in 2018 by the California State Supreme Court in 2018. *People v Buza* (California Supreme Court, 2 April 2018).

[56] See, for example, Justin Jouvenal, Mark Berman, Drew Harwell & Tom Jackman, "Data on a genealogy site led police to the 'Golden State Killer' suspect. Now others worry about a 'treasure trove of data'", *Washington Post* online, 27 April 2018; Gina Kolata & Heather Murphy, "The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder", The New York Times online, 27 April 2018.

i. *Does any law criminalize the misuse of devises or data for the purposes of committing any of the criminal behavior described in the sub-questions above? ..... [Y/N]*

j. *If so, cite and quote/summarize: _____*

k. *Does any law criminalize unauthorized input, alteration, deletion, or suppression of computer data, resulting in inauthentic data which would apply to ID systems or other databases holding personal data? ..... [Y/N]*

l. *If so, cite and quote/summarize: _____*

m. *Does any law criminalize fraudulent use or alteration of data or interference with a computer system to procure an economic benefit which would apply to ID systems or other databases holding personal data? ..... [Y/N]*

n. *If so, cite and quote/summarize: _____*

Background

Cybercrime laws are directly relevant to national, digital ID systems, which may be the object of or instrumentalities used in criminal activity. Cybercrime may have a wide range of meanings depending on the country, legal instrument and context in which the phrase is used. The purpose here is to gather a broad understanding of the degree to which the country has laws in place addressing criminal conduct (as provided in the country's criminal laws) directed against the confidentiality, integrity and availability of computer systems and networks, as well as the data stored and processed on them, and criminal acts carried out through the instrumentality of such systems, networks and data. This broad approach to the definition of cybercrime is drawn from the 2017 World Bank *Toolkit on Combatting Cybercrime*.[57]

Example

The Convention on Cybercrime (Budapest Convention), 2001[58] identifies as cybercrime:

- offenses against the confidentiality, integrity, and availability of computer data and systems, including illegal access, illegal interception, data interference, system interference and misuse of devices;59
- computer-related offenses, including computer-related forgery and computer-related fraud;60
- computer content-related offenses (defined as child pornography);61 and
- computer-related offenses involving infringements of copyright and related rights.62

The Convention also allows for ancillary liability and sanctions for inchoate offenses (attempt, and aiding or abetting and for corporate liability).63

International and extraterritorial issues

19. *Cross-border data transfers:*

a. *Do any laws, regulations or policies require personal data to be stored within the country, or otherwise limit the transfer of personal data to a foreign country?..... [Y/N]*

b. *If so, cite and quote/summarize: _____*

c. *Does the country have arrangements with foreign countries or multinational entities or schemes, including decisions of domestic and foreign bodies or agencies, to require, permit or limit transfers of personal data between countries (e.g., treaties, adequacy decisions of the EU, binding corporate rules, mutual recognition arrangements, required information sharing through the Advance Passenger Information System)?..... [Y/N]*

[57] See http://www.combattingcybercrime.org/.

[58] See https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[59] Budapest Convention, Articles 2–6.

[60] *Ibid*, Articles 7 and 8.

[61] *Ibid*, Article 9.

[62] *Ibid*, Article 10.

[63] *Ibid*, Articles 12 and 13.

d. *If so, describe:* _____

Background

The security of personal data transferred across national borders has been one of the drivers for international consensus on the fundamental principles for the protection of personal data.[64] The principle articulated in the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* is that a data controller "remains accountable for personal data under its control without regard to the location of the data".[65] However, due to uncertainty regarding data protection standards in foreign countries, many countries limit extraterritorial transfer of personal data. Such transfers may be permitted in certain circumstances or when the data protection standards in a particular third country are deemed adequate. This is particularly sensitive in the case of personal data for national ID systems, civil registration and voter registration systems.

Examples

The EU's GDPR limits transfers of personal data outside the European Economic Area except in certain circumstances. Such transfers are allowed if the European Commission issues a decision determining that the receiving country "ensures an adequate level of protection."66 Such a decision requires a comprehensive assessment of the country's data protection framework, including protections applicable to personal data and oversight and redress mechanisms.67 Adequacy decisions have been adopted with respect to 12 countries, including Canada (commercial organizations), Israel, Switzerland and the United States (limited to the Privacy Shield framework). 68 In July 2018, the EU and Japan agreed to recognize each other's data protection system as equivalent, and the European Commission has begun the process of formally issuing an adequacy decision. 69 Similarly, the United Kingdom is seeking to obtain an adequacy decision from the European Commission to apply upon the UK's exit from the European Union (Brexit).70 Transfers to non-EU countries are also permitted in other circumstances, such as if the transferor has provided "appropriate safeguards" which may be established through several means including a legally binding agreement between public authorities, certain contractual clauses (e.g. the EU Model Clauses)71 or the existence of an approved and enforceable code of conduct, among others.72

In 2015 in Ireland, Austrian PhD student and Facebook user Max Schrems challenged the legality of the transfer of his personal data by Facebook's Ireland entity to Facebook's servers in the United States before the Irish Data Protection Commissioner (DPC). The "adequacy" requirement discussed above applied under the EU Data Protection Directive, the predecessor of the GDPR. The DPC rejected Mr. Schrems' complaint on the basis that the European Commission had in 2000 determined that the US ensures an adequate level of protection of personal data transferred (known as the "safe harbor"). Mr. Schrems challenged this view, arguing that US law and practice, particularly the conduct of the United States intelligence services (including the National Security Agency), offered no real protection against US surveillance of data transferred to the US. The matter was referred to the Court of Justice of the European Union (CJEU), which found that the Irish DPC was not bound by the European Commission's safe harbor and had the right to review the adequacy of the data protections provided by the US. The CJEU also found that the safe harbor should be invalid due to lack of adequacy.

20. *International functionality and recognition of foreign ID credentials:*

a. *Excluding passports, are any ID credentials of foreign countries (whether commercial or governmental) recognized for any purpose in the country?..... [Y/N]*

If so, in the table below identify each such foreign country ID credential and the functional purpose(s) for which it is recognized.

Foreign country	ID credential(s)	Functional purpose(s)

[64] See, for example, *OECD Privacy Framework*, 2013, Chapter 3 (Explanatory Memorandum for Original 1980 Guidelines) at 42.

[65] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted in 1980 and revised in 2013, Article 17.

[66] 2016 EU General Data Protection Regulation, Art 45.

[67] European Commission, Press Release Database, Questions & Answers on the Japan adequacy decision, 17 July 2018.

[68] Ibid.

[69] European Commission, Press Release, The European Union and Japan agreed to create the world's largest area of safe data flows, 17 July 2018.

[70] Commons Select Committee, Data Adequacy Decision should be secured from EU as soon as possible, 3 July 2018. European Commission, Press Release, The European Union and Japan agreed to create the world's largest area of safe data flows, 17 July 2018.

[71] EU Commission, International data transfers using model contracts.

[72] 2016 EU General Data Protection Regulation, Art 46.

b. *In the table below, indicate any arrangements the country has or is contemplating with partner countries regarding mutual recognition of ID systems.*

Legal instrument (treaty, regional regulation, etc.)	ID systems and basic effect of mutual recognition	Partner countries	Status (e.g., finalized, in negotiations, contemplated)

Background

The mobility of citizens and the increase in digital services has increased the need for recognition of ID systems across borders. This is an increasingly important element of regional integration as citizens of one country seek to access services across the region. For countries to recognize each other's IDs, there must be a basic level of common standards of trust and assurance.

Examples

In the **EU**, the *2014 eIDAS Regulation*[73] sets out a regional system to enable mutual recognition of electronic ID systems among Member State to facilitate cross-border access to services. The Regulation was a response to the inability of citizens to use their electronic IDs to authenticate themselves in other Member States due to a lack of mutual recognition of national ID systems.[74] Under the Regulation, Member States are able to notify eligible electronic ID systems to the European Commission which adds the system in a published list. [75] Each notified ID system is designated an "assurance level" of "low," "substantial" or "high," corresponding to the degree of confidence in the claimed identity of the person utilizing the ID system.[76] Other Member States must recognize the notified ID system for access to certain public services if the assurance level of the ID system is substantial or high and is equal or higher than the assurance level required for access to the same service using a domestic ID system[77]

Kenya, **Rwanda** and **Uganda** agreed in 2013 that each country would recognize national ID cards of the other two countries as a travel document for entry.[78] The arrangement, which took effect in 2014, was part of the Northern Corridor Integration Projects which seek to "promote integration among the partner states by fast tracking projects for the benefit of citizens and the development of the region."[79]

Other ID related laws, regulations and policies

21. *Limitations on use of a universal identifier:*

a. *Are there any legal or regulatory limitations on the use of a single identifier, such as an identification number, for different purposes or in multiple government databases ..... [Y/N]*

b. *If so, indicate any law, regulation or policy that articulates such limitations:*

[73] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[74] eIDAS Regulation, Recital para 9.

[75] *Ibid*, Articles 6, 9.

[76] *Ibid*, Article 8.

[77] eIDAS Regulation, Article 6.

[78] See Cris Magoba (principal public relations officer of the Ministry of EAC Affairs), "The experience of cross border travel using national ID," 11 January 2017; Lucia Hanmer & Jean Lubega Kyazze, "Opening doors: How national IDs empower women cross border traders in East Africa," 30 November 2017, World Bank blog post.

[79] Northern Corridor Integration Projects website, About us.

Background

Some countries specifically prohibit multiple uses for or the linking of multiple government databases with the use of a single unique identifier, because this has the capacity to connect a large amount of data about an individual in a way that is inconsistent with an individual's expectations.

Some countries find the use of a single unique identification number in multiple contexts convenient for both government and citizens as this approach can reduce administrative burdens and is one means of eliminating the need to store personal data in multiple databases. Some countries even prohibit government from collecting personal data from citizens multiple times (sometimes referred to as the "ask once" principle). This approach is more viable in a country with a strong data protection framework that mitigates the risks of misuse of personal data.

Examples of prohibitions on single unique identifiers

In **Portugal**, Article 35(5) of the Constitution states: "The allocation of a single national number to any citizen is prohibited." As a result, individuals use different identification numbers for different purposes.[80]

In **Germany**, the Federal Constitutional Court ruled in 1983 that the introduction of a universal personal identifier is forbidden by German constitutional law. This decision was based on the concern that a universal personal identifier would allow an easy combination of different data sets and so could be used to create detailed personal profiles of citizens.[81]

In **Hungary**, in 1991, the Constitutional Court held that a law providing for a universal, multipurpose identifier for use in multiple government records without adequate safeguards was an unconstitutional threat to human dignity because this would endanger personal privacy by allowing for the construction of a personal profile (which would probably be distorted since it would be based on data taken out of context). The Court also found that the scheme in question would extend state power and increase the potential for state control. However, it noted that the use of such identifying numbers for data processing for a specific purpose might be possible to reconcile with the Constitution.[82]

In **Chile**, in 2012, the government introduced a "Unified Data Bank" ("*Banco Unificado de Datos*"), which compiled a range of information about citizens into a single database. The data included criminal records, information about past or present judicial proceedings, previous criminal convictions, and investigations of any kind. In 2015, the President of the Supreme Court issued a public statement criticizing the fact that this data bank was searchable by means of a citizen's national ID number, on the basis that it contained sensitive personal data in terms of Chile's data protection law. [83]

In **Austria,** there was public resistance to the use of a single unique identifier across multiple government databases. Instead, citizens use multiple, sector-specific unique identifiers which are generated from the unique identifier on their ID card—meaning, for example, that the identifier used for tax purposes is different from the one used for health services. This approach prevents information in one government agency from being linked to information in another.[84]

Examples of "ask once" limitations

Belgium has an "ask once" principle enshrined in its national legislation, aimed at preventing individuals from having to submit personal information multiple times to different government agencies.[85]

The **United Kingdom** has a "Tell Us Once" service whereby citizens inform a local authority of the birth or death of a person (online, telephone or face-to-face), whereupon that local authority, with the informant's consent, takes responsibility for sharing the information with all relevant government agencies.[86]

---

[80] See Article 35, Constitution of the Portuguese Republic Seventh Revision [2005] (English translation).

[81] Bundesverfassungsgericht [BVerfG], 15 December 1983, 65 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 1. A full English translation of this decision has not been located. The case is discussed in, e.g., Gerrit Hornung & Christoph Schnabel, "Data protection in Germany I: The population census decision and the right to informational self-determination", 25(1) *Computer Law & Security Report* 84 (2009).

[82] Constitutional Court Decision No. 15-AB of 13 April 1991 (in English).

[83] The full text of this statement is available (in Spanish) at www.pjud.cl/web/guest/noticias-del-poder-judicial/-/asset_publisher/kV6Vdm3zNEWt/content/declaracion-publica-del-presidente-de-la-corte-suprema-de-justicia,

[84] Daniel Castro, *Explaining International Leadership: Electronic Identification Systems*, The Information Technology & Innovation Foundation, 2011.

[85] See, e.g., Adrian Offerman, "OOP: the right to be asked for the same data by government only once", 8 June 2016, e-Government community website; Daniel Castro, *Explaining International Leadership: Electronic Identification Systems*, The Information Technology & Innovation Foundation, 2011. The principle is enshrined in Belgium's "Only Once Act" of 5 May 2014 (published in the Belgium Official Journal on 4 June 2014). The law is entitled "*Loi du 5 mai 2014 garantissant le principe de la collecte unique des données dans le fonctionnement des services et instances qui relèvent de ou exécutent certaines missions pour l'autorité et portant simplification et harmonisation des formulaires électroniques et papier"* and is available (in French) at www.ejustice.just.fgov.be/cgi/article_body.pl?language=fr&pub_date=2014-06-04&numac=2014203384&caller=list.

[86] "Tell Us Once (TUO)", United Kingdom, 1 Jan 2003–ongoing, Stakeholder Community Once-Only Principle for Citizens website.

In 2007, **Estonia** introduced a broad "once-only" principle which allows the state to ask citizens for the same information only once, thus forcing government agencies to communicate more efficiently, while enhancing security by storing data in several small databases which can be cross-checked rather than in one large central database.[87]

Although many **EU** Member States have begun to implement such measures at a national level, EU-wide cross-border adoption of the "once-only principle" has not been finalized. The once-only principle remains, however, one of the underlying principles stated in the European Union's "eGovernment Action Plan 2016-2020".[88]

22. ***Laws and regulations:*** *Identify any other significant laws, regulations and policies not already identified in this IDEEA having a significant bearing on identification design in the country.*

Issue	Laws and regulations	Government policies
ID requirements for passports and other travel documents		
ID requirements and protection of personal health data for health care providers		
KYC and other ID requirements and data protection for banks, other financial institutions and payment providers (including digital financial services)		
SIM card registration requirements		
ID requirements for social services and any other government services		
ID requirements for payment of taxes, receipt of tax refunds or other tax-related transactions		
ID requirements for any other common interactions with government, for example, initiating a police complaint		
Recognition of e-signatures (see Question 42)		
Digital signatures and other trust services (see Question 42)		
Collection of personal data from individuals lacking legal competency (e.g., minors)		
Public access to information		
Limitations on access to data for surveillance by public or private sector entities		
Other (specify):		

23. ***Key court rulings:*** *Describe any key court rulings with consequences for ID systems design not already mentioned:*
_____

Governance

Individual rights and protections

24. ***Consent:*** *Does any law, regulation or policy specify consent of the individual as one basis for the collection and/or use of personal data?..... [Y/N]*

If so, cite and quote/summarize, including exceptions: _____

[87] Valentina Pop, "You can't use 18th century law for a digital world", interview with former Estonian Prime Minister Andrus Ansip, *EU Observer,* 26 February 2015.

[88] TOOP, "Once-Only"; EU Commission, "eGovernment Action Plan 2016-2020", 19 April 2016.

Background

One widely (though not universally) accepted general principle is that personal data about an individual should only be collected and used with the consent of that individual unless there is another basis in law for such collection and use (see Annex II to this IDEEA Guidance Note). Where consent is the basis for collection, transparent disclosure to the individual of the nature of the personal data collected and the intended uses of such data is essential for consent to be meaningful.

Many international and regional standards and national laws make exceptions to the consent requirement for collection and use of personal data where government collects data pursuant to legal authority, such as data collected for ID systems.[89] Where no consent is required or obtained, transparency can at least provide clear and accessible explanations to assure public trust and prevent misconceptions. Individuals can be informed of which data is considered public and which will remain confidential.

Some countries require a "privacy policy" in the form of an easy-to-understand document which explains in plain language how personal data is collected and used. However, there is some debate about how frequently such documents are actually read and understood.[90] Public awareness campaigns are also crucial to disseminate information on the collection and use of personal data. These can address misconceptions and concerns and identify channels for questions and complaints.

Examples

The ***OECD*** *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (adopted in 1980 and revised in 2013) emphasize openness, stating that individuals should be able to know that data collection is taking place, the purposes of the data collection and the identity and usual residence of the data controller.[91]

In **Asia-Pacific**, the *2004 APEC Privacy Framework* contains a similar directive, stating that data controllers should provide "clear and easily accessible statements about their practices and policies with respect to personal information."

The **EU***'s* GDPR requires that there must be a valid lawful basis for processing personal data. One such lawful basis is consent of the individual, although this may not necessarily be the most appropriate legal basis, depending on the processing.[92] Where consent is relied upon, it must be "freely given, specific, informed and [an] unambiguous indication" signifying "agreement to processing of personal data."[93] Under GDPR, consent must involve a clear affirmative action. However, consent is not a valid lawful basis "where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."[94] The GDPR requires distinct "granular" consent operations for distinct processing operations so that consent for multiple different processing activities is not bundled together. Consent must specifically cover the name of the entity carrying out the processing, the purposes of the processing and the types of processing activity.

Where the personal data being processed is special category data (for example, biometric data), additional conditions to processing must be satisfied, one of which is obtaining the individual's "explicit" consent to the processing.[95] It is not clear whether there is a difference between standard consent and explicit consent (since standard consent must be specific, informed and affirmative action). However, given the GDPR has only been implemented recently it is likely that further guidance will be issued to clarify this.

The **California** *Consumer Privacy Act of 2018* applies to certain businesses that collect personal information of California residents and will go into effect in 2020. The Act, unlike the GDPR, does not strictly require consent prior to collection of personal information, in most cases. However, at the point of information collection, consumers must receive notice "as to the categories of personal information to be collected and the purposes for which the categories of personal information

---

[89] For example, the *2016 EU General Data Protection Regulation* states in its Preamble at para 40: "In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law. . ." (emphasis added).

[90] See, e.g., Whitley, E. A., and Pujadas, R. (2018). Report on a study of how consumers currently consent to share their financial data with a third party, *Financial Services Consumer Panel* at ii. "The evidence from the empirical research suggests that consent is frequently neither freely given, nor unambiguous nor fully informed. Over half of the contributors claimed not to read any terms and conditions for products and services that they sign up for, including the specific services that access their financial data. Similarly, only a small proportion of participants correctly answered a question about a detail in the policy even after having an opportunity to re–read the policy in a research setting."

[91] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, para. 12.

[92] 2016 EU General Data Protection Regulation, Articles 6(1), 23.

[93] 2016 EU General Data Protection Regulation, Article 4(11).

[94] 2016 EU General Data Protection Regulation, Recital 43.

[95] 2016 EU General Data Protection Regulation, Article 9.

shall be used."[96] Additional information must be disclosed in an online privacy policy or a website and updated every 12 months. [97]

In **Australia**, the federal *Privacy Act 1988* (as amended) contains as one of its "Privacy Principles" the rule that personal information about an individual collected for a particular purpose must not be used or disclosed for another purpose without the individual's consent. However, there is an exception for situations where the use or disclosure is "reasonably necessary" for the enforcement related activities conducted by or on behalf of an enforcement body – which includes use or disclosure by police for prevention, detection, investigation, prosecution or punishment of criminal offences – as well as an exception for uses and disclosures authorized by law or by court order. Use for enforcement related activities must be noted in writing as a mechanism to promote accountability.[98]

25. ***Right to access and review use of personal data:*** *Do individuals have the right to access and review use of personal data about them held by third parties? ..... [Y/N]*

    c. *If so, specify the source and nature of the right and any associated process:*

    _____

26. ***Rectification of personal data:*** *Do individuals have the right to rectify personal data about them held by third parties? ..... [Y/N]*

    d. *If so, specify the source and nature of the right and any associated process:*

    _____

27. ***Right to deletion of personal data:*** *Do individuals have the right to have personal data about them (including data trails) deleted? ..... [Y/N]*

    e. *If so, specify the source and nature of the right and any associated process:*

    _____

Background

Many legal and regulatory frameworks include the rights of individuals to access, review, rectify and erase personal data about them. These rights have a basis in international norms.

According to the *OECD Privacy Handbook*, "[t]he right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard".[99] General Comment 16 on Article 17 of the *International Covenant on Civil and Political Rights* states that "every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes." [100]

An important corollary to the right to access personal data is the right to rectification or erasure.[101] For example, General Comment 16 on Article 17 of the *International Covenant on Civil and Political Rights* states that if files contain incorrect personal data, then "every individual should have the right to request rectification or elimination".[102] The *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)* provides for "rectification or erasure" of any data processed contrary to the principles on data quality, which require that personal data undergoing processing must be adequate and up-to-date. [103] The *APEC Privacy Framework* states that individuals should have the right to "challenge the accuracy of information relating to them and, if possible an as appropriate, have the information rectified, completed, amended or deleted". [104]

---

[96] California Consumer Privacy Act of 2018, CAL. COV. CODE §178.100(b).

[97] California Consumer Privacy Act of 2018, CAL. COV. CODE §178.130(a).

[98] Privacy Act 1988 (including amendments up to Act 92 of 2017), section 6 (general definitions) and Schedule 1, Australian Privacy Principles, clause 6; Australian Government Solicitor, "Privacy Act reforms – implications for enforcement functions", Factsheet No 27, May 2013.

[99] *OECD Privacy Handbook*, 2013, Chapter 3 (Explanatory Memorandum for Original 1980 Guidelines).

[100] Human Rights Committee, General Comment 16 (on Article 17 on the right to privacy), 1988, Supp. No. 40, UN Doc A/43/40, para 10. A General Comment to an international convention is a non-binding guide to its interpretation.

[101] Or as it is referred to in Europe, "the right to be forgotten". See, *Case C-131/12, Google Spain v. Agencia de Protección de Datos* (AEPD), 2014 EUR-Lex (May 13, 2014). See Kelly & Satola, "The Right to Be Forgotten", University of Illinois Law Review, Vol. 1, 2017.

[102] Human Rights Committee, General Comment 16 (on Article 17 on the right to privacy), 1988, Supp. No. 40, UN Doc A/43/40, para 10. A General Comment to an international convention is a non-binding guide to its interpretation.

[103] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), Art 8(c), with reference to Art 5.

[104] 2004 APEC Privacy Framework, Art. 23(c).

Even in a mandatory ID scheme, a "right of erasure" could arise in respect of the specific aspects of personal data, biometric data, particularly genetic material, [105] a previous married surname or the names of the birth parents of an adopted child.

Examples

The **EU**'s GDPR provides for several rights of individuals with respect to personal data about them. Individuals have a right to receive confirmation that personal data about them is being processed and receive a free copy of that data (subsequent copies may incur a "reasonable fee based on administrative costs").[106] Individuals further have a right to rectification of any inaccuracies in the data, including completion of incomplete personal data completed.[107] Individuals also have a right to have personal data about them erased in certain circumstances, including where the personal data are no longer necessary in relation to the purposes for which they were collected or processed and, if the processing is based on consent, where the individual withdraws that consent and there is no other legal ground for the processing.[108]

In the **EU**, in *Google Spain v AEPD*[109], a Spanish national complained to the Spanish Data Protection Agency (AEPD) about Internet stories linking his name with attachment proceedings in a real-estate auction related to recovery of social security debts. Mr Costeja González requested that the newspaper remove or alter the pages, or that Google Spain or Google Inc remove or conceal the personal data in search results. Google objected to the Spanish National High Court, which requested a decision of the European Court of Justice (ECJ), which found that Google was a data controller against which the right to be forgotten could be exercised, and thus Mr. Costeja had the right to make the request and have it reviewed by the AEPD.[110]

The **California** *Consumer Privacy Act of 2018* applies to certain businesses that collect personal information of California residents and will go into effect in 2020. Under the Act, if requested by a consumer, a business covered by the Act must disclose, without charge and with respect to the prior 12 months, the types of personal information collected about that consumer, the specific pieces of information collected and categories of third parties with which the information has been shared, among other things.[111] These disclosures must be made within 45 days of receipt of the request.[112] Such businesses must also comply with a consumer's request to have personal information deleted unless that information is necessary for the business to perform certain enumerated functions.[113]

In **Belgium**, citizens have the ability to find out who has accessed data about them. Government workers also have to use their own e-ID cards to gain access to the ID database, leaving an access trail. There is a website maintained by a national IT organization which allows citizens to see who has used their national ID number and for what purpose. [114]

In **Estonia** it is possible for ID holders to find out which government officials have accessed data about them. [115]

28. ***Data portability:*** *Do individuals have the right to easily move, copy or transfer personal data easily from one system to another electronic environment?..... [Y/N]*

    f. *If so, specify the source and nature of the right and any associated process.*

    _____

Background

Data portability refers to the ability to easily move, copy or transfer personal data about an individual from one technological environment to another. This portability allows individuals to utilize the collected data in other contexts. Some legal and regulatory frameworks guarantee data portability as an individual right.

With respect to commercial enterprises, such portability mitigates the risks of consumers becoming locked into a single service provider that would otherwise have an advantage over competitors which did not have ready access to such data.

---

[105] See Els J Kindt, "Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis", Springer Science & Business Media, 2013; Ruth Chadwick, The Right to Know and the Right Not to Know: Genetic Privacy and Responsibility, Cambridge University Press, 2014.

[106] 2016 EU General Data Protection Regulation, Art 15.

[107] *Ibid*, Art 16.

[108] *Ibid*, Art 17.

[109] See footnote 101.

[110] See Kelly & Satola, "The Right to Be Forgotten", University of Illinois Law Review, Vol. 1, 2017.

[111] California Consumer Privacy Act of 2018, CAL. COV. CODE §§178.110(a) & (b), 178.130(a)(2).

[112] *Ibid*, §178.130(a).

[113] *Ibid*, §178.105.

[114] Alea Fairchild and Bruno de Vuyst, "The Evolution of the e-ID card in Belgium: Data Privacy and Multi-Application Usage", 2011; "National ID cards: 2016-2018 facts and trends", updated 10 February 2018

[115] Jaan Priisalu & Rain Ottis, "Personal control of privacy and data: Estonian experience", *Health Technology* (2017) 7: 441

In terms of an ID system, such a right potentially enables individuals to use personal data collected by the system for other technological applications.

Examples

The **EU**'s GDPR provides a right to individuals to receive personal data about them "in a structured, commonly used and machine-readable format" and to have that data transferred to another party "without hindrance."[116] Where technically feasible an individual has the right to have such data transferred to another party directly.[117]

The **California** *Consumer Privacy Act of 2018* applies to certain businesses that collect personal information of California residents and will go into effect in 2020. The Act includes a right to request and receive from a business covered by the Act the specific personal information that has been collected within the prior 12 months.[118] Such information must be delivered to the consumer in "a readily useable format that allows the consumer to transmit this information from one entity to another without hindrance."[119]

29. ***Automated decisions:*** *Are there rights to limit the making of decisions about individuals solely as a result of automated processing of personal data (i.e., without any human intervention)?..... [Y/N]*

    g. *If so, specify the source and nature of the right and any associated process:*

    _____

Institutions

30. ***Personal data protection authority:*** *Is there one or more administrative authority (agency, body or official) with general responsibility for protection of personal data and/or privacy?..... [Y/N]*

    h. *If so, answer with respect to each:*

    a. *What law or regulation establishes or empowers this authority?*

    _____

    b. *Indicate which of the systems identified in Part I are subject to this authority, and any limitations on its supervisory jurisdiction over such systems.*

    _____

31. ***Institutional independence:*** *For each body or agency identified in Question 30 (complete separately for each one if necessary):*

    a. *Is the agency or body effectively independent from external influence in carrying out its statutory duties, particularly from day-to-day political influence and commercial interests?..... [Y/N]*

    b. *Who appoints the authority or its members?* _____

    c. *Who has the power to remove the authority or its members?* _____

    d. *What is the term of office?* _____

    e. *Who controls its budget?* _____

32. ***Administrative powers:*** *For each body or agency identified in Question 30 (complete separately for each one if necessary):*

    a. *Does this authority have powers to receive complaints?..... [Y/N]*

    b. *Does this authority have powers to conduct investigations?..... [Y/N]*

    c. *Does this authority have powers to issue orders to cease and desist from, or to compel, certain conduct? ..... [Y/N]*

    d. *Does this authority have powers to impose substantial penalties or other remedies?..... [Y/N]*

    e. *If so, describe:* _____

---

[116] 2016 EU General Data Protection Regulation, Art 20.

[117] *Ibid*.

[118] California Consumer Privacy Act of 2018, CAL. COV. CODE §§178.110(a) & (b), 178.130(a)(2).

[119] *Ibid*, §178.130(a)(2).

f. *Briefly describe any other significant powers or duties (or limits on them) of this authority relevant to protection of personal data and privacy.*

_____

g. *Has the authority brought any significant initiatives and cases to encourage and enforce compliance with data protection and privacy laws? ..... [Y/N]*

h. *If so, describe:* _____

i. *Is there a right of judicial review or appeal for a person aggrieved by a decision of this body? ..... [Y/N]*

Background

Personal data protection and privacy generally, including with respect to ID systems, is often subject to the oversight of an independent supervisory or regulatory authority to ensure compliance with privacy and personal data protection law, including protecting individuals' rights. The supervisory authority might be a single government official, ombudsman or a body with several members.

Genuine independence of such an authority is a key factor, with independence being measured by structural factors such as the composition of the authority, the method of appointment of members, the power and timeframe for exercising oversight functions, the allocation of sufficient resources and the ability to make meaningful decisions without external interference.[120]

The powers and duties of such an authority may include:

- duties to monitor, investigate and enforce compliance with individual privacy and personal data protection rights;
- duties to monitor developments and their impact on individual privacy and personal data protection rights;
- powers to receive complaints and conduct investigations of potential violations of individual privacy and personal data protection rights;
- powers to issue decisions on violations of such rights and order remedial action or meaningful sanctions;
- duties to promote public awareness of the rights of individuals and the responsibilities of those entities holding and processing personal data; and
- a duty to give specific attention to the personal data protection rights of children and other vulnerable individuals.[121]

The supervisory authority may handle public complaints, even though every individual about whom data is collected may have recourse to an external binding legal process and ultimately the courts at least on matters of law. In terms of remedies, the authority may have the power to oblige the ID system to rectify, delete or destroy inaccurate or illegally collected data.

The supervisory authority might also have other powers and duties, such as issuing opinions prior to the implementation of data processing operations, advising on legislative or administrative measures, and recommending codes of conduct or referring cases to national parliaments or other state institutions. The supervisory authority may also play a role in keeping the public informed about their rights and obligations and about personal data protection issues in general—issuing regular reports, publishing opinions and other public communications.[122]

Examples

In **South Africa**, the *Protection of Personal Information Act 4 of 2013* established the Information Regulator, an independent body subject only to the Constitution and to the law. This body is appointed by the President on the recommendation of the National Assembly, after nomination by a committee composed of members of all the political parties represented in the National Assembly. It is ultimately accountable to the National Assembly. It has a broad range of supervisory functions, including a duty to: conduct public education, monitor and enforce compliance with the law, consult stakeholders and mediate between opposing parties, handle individual complaints, conduct relevant research, issue codes of conduct and guidelines, and facilitate cross-border cooperation. Among its monitoring functions are the periodic assessment and

[120] Recital 117 of the GDPR provides, "The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organizational and administrative structure."

[121] Derived from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), as it is expected to be amended by the forthcoming modernizing Protocol (new Art 15) and 2016 EU General Data Protection Regulation, Articles 57 and 58.

[122] Council of Europe, "Explanatory Report to the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows", 1981, paras 13-16. See also Council of Europe, "Draft Explanatory Report prepared for proposed modernized Convention 108", 2016, paras 114-140.

monitoring of public and private bodies engaged in processing of personal data and monitoring the use of unique identifiers of data subjects.[123]

In the **Philippines**, the *Data Privacy Act of 2012* established the independent National Privacy Commission. The Commission, which is attached to the Department of Information and Communications Technology, is headed by a Privacy Commissioner who is assisted by two Deputy Privacy Commissioners (one responsible for Data Processing Systems and one responsible for Policies and Planning). All three Privacy Commissioners must be expert in the field of information technology and data privacy, and all are appointed by the President for three-year terms and are eligible for reappointment for a second term of office. The Commission has its own secretariat. The Commission's many duties include monitoring compliance with the data privacy law; receiving and investigating complaints; regularly publishing a guide to all laws relating to data protection; reviewing and approving privacy codes voluntarily adopted by personal information controllers; providing opinions on the data privacy implications of proposed national or local statutes, regulations or procedures; and coordinating with data privacy regulators in other countries.[124]

Under the **EU**'s GDPR, Member States are required to provide for a supervisory authority to monitor the application of the regulation.[125] However, many Member States had previously established their own supervisory authorities under the *EU Data Protection Directive (Directive 95/46/EU)*, the incumbent EU data protection regime.

In the **United Kingdom**, the *Data Protection Act 1984* introduced the role of Information Commissioner (previously, the Data Protection Registrar) although the powers granted to the Information Commissioner increased in scope under the Data Protection Act 1998 and most recently, the *Data Protection Act 2018*. The Information Commissioner is an independent official appointed by the Crown and operates the UK Information Commissioner's Office (ICO). The ICO is sponsored by the Department for Digital, Culture, Media and Sport (DCMS) and ultimately reports to Parliament. It is an independent regulatory body which seeks to monitor, investigate and enforce all applicable data protection and privacy legislation in the UK (including Scotland, to a limited extent).

33. ***Financial sustainability:*** *For each body or agency identified in Question 30 (complete separately for each one if necessary):*

    a. *Has the body or agency historically been adequately funded to enable it to achieve its statutory and other responsibilities? ..... [Y/N]*

    b. *Has the budget of the body or agency increased or decreased since its formation? ..... [Y/N]*

    c. *Is the body or agency expected to be adequately funded to cover its costs? ..... [Y/N]*

    d. *If not, why not?* _____

    e. *Have there been persistent budget shortfalls? ..... [Y/N]*

    f. *If so, what reasons have been given?*_____

    g. *What sources of revenues does the authority rely on to cover its costs?*

Substantial source of funding	h.
Fees	Y/N
Public funds	Y/N
Penalties	Y/N
International aid	Y/N
Private investment	Y/N
Other (specify): _____	Y/N

34. ***Objections, complaints and remedies:*** *Do individuals have a right to object to the use personal data about them, file complaints and seek redress? ..... [Y/N]*

    i. *If so,*

    a. *Specify the source and nature of the right and any associated process:*

    _____

[123] As of August 2018, the Protection of Personal Information Act 4 of 2013 had not yet been brought fully into force.

[124] See Data Privacy Act of 2012 (Philippines), Chapter II.

[125] 2016 EU General Data Protection Regulation, Article 51(1).

b. *Identify the entity or entities responsible for receiving such objections and complaints, conducting investigations and applying remedies:*

_____

c. *Describe the processes for making an objection, bringing a complaint and seeking redress, and how the entity using the data is required to respond:*

_____

d. *Are such processes used to a significant extent in practice? ..... [Y/N]*

e. *If not, describe any significant barriers individuals face.*

_____

f. *Describe the remedies available to individuals for violation of any of the rights or protections relating to personal data about them.*

_____

Background

ID systems often have a channel through which individuals can file complaints to enforce their rights to access, review, rectify and erase personal data. Complaints may be handled by an independent supervisory authority, often with the ultimate recourse of judicial review, and the appropriate legal and regulatory framework can set out clear procedures and remedies. Some remedies include compensation if an individual has suffered material damage from violation of privacy rights and protections.

Examples

The **EU**'s GDPR provides that every individual about whom personal data is being processed has the right to lodge a complaint with a data protection authority if the individual considers that the processing of the personal data is in breach of the GDPR.[126] Individuals also have the right to an effective judicial remedy against a legally binding decision of a data protection authority concerning them, or against an organization processing personal data about them where that individual considers the processing of such data is in breach of the GDPR.[127] Individuals also have the right to compensation from such organizations where they have suffered material (and non-material) damage as a result of such breach.[128]

[126] 2016 EU General Data Protection Regulation, Article 77.

[127] *Ibid*, Articles 78 and 79.

[128] *Ibid*, Article 82.

Part III. Questions about *each* ID system and its legal framework

Guidance to IDEEA user

Part III seeks to build a picture of the legal and regulatory regime for the country's significant existing ID and civil registration systems in the context of their broad design, requirements and administration. Complete this Part III separately with respect to **each** of the following:

- Foundational ID systems (including any civil registration systems) identified in Part I (including any national ID, civil registration system or other foundational system).
- Functional ID systems identified in Part I (including voter registration).

Where there is more than one ID system to be addressed, copy and paste a blank version of this Part III to address each one. (Do not attempt to address multiple systems in a single copy of Part III.) Where any questions are not relevant to the type of system being addressed, such as questions with respect to digital data in the case of a paper-based ID system, write "n/a".

In some cases, an ID system's features and requirements may be provided for in a law, regulation or policy specific to the system, in which case these should be addressed in the questions in this Part III. However, some requirements may exist in generally applicable laws, regulations, policies or case law, such as a generally applicable law on data protection and privacy. These should have been addressed in Part II along with other broader country factors. There is no need to duplicate in this Part III answers that have been provided in Part II – it may be simpler to indicate "See Part II" as an answer to the relevant question in Part III.

Generally, aim for simplicity of presentation, avoid unnecessary duplication, cross-refer to other answers where helpful, and use discretion as to how and in which Part best to address a topic.

The ID System, its Purposes and Capabilities

35. *Identify the ID system addressed here.*

_____

36. *Is the system foundational or functional (or effectively both)?*

_____

37. *Describe briefly what the ID system is for and what it does.*

_____

Guidance to IDEEA user

The purpose of an ID system should inform its design and functionality, the data it must collect, and the ends to which it is employed, and should be reflected in the legal framework that governs it. This section explores the various aspects of the basic purpose and capabilities of the ID system:

- The first sub-section below concerns the "**legal, regulatory and policy definitions**" of the system's purpose. These may limit the permitted design, functionality and usage of the system, including the collection and use of personal data.
- The second sub-section below concerns the "**capabilities**" of the system, which may include: identification, authentication, authorization and attribution. The type and scope of personal data required to be collected and used by the ID system will depend on which of these capabilities the system has. For example, a system that only authenticates individuals' identities likely requires less personal data than a system intended to support the authorization of individuals to complete transactions or receive public services.
- The third sub-section below explores the "**functional purposes**" for which the system is used. This includes practical activities such as accessing public services, receiving health care, opening bank accounts, international travel or voting. These functional purposes will also inform the types of data the ID system will need to collect and use.

Legal, regulatory and policy purposes

38. *Purpose definition and limitations:*

a. *Indicate any law, regulation or policy that defines (or limits) the purposes, uses or authority of the ID system and summarize the key points.*

_____

b. *Indicate and summarize exceptions to those definitions or limitations.*

_____

Example

Article 15 of **Nigeria**'s *National Identity Management Commission Act, 2007* sets out six "objectives" of the National Identity database, which include providing "a medium for the identification, verification and authentication of citizens," facilitating "the provision of a secured and a reliable method for ascertaining, obtaining, maintaining and preserving information and facts about citizens" and facilitating "the provision of a convenient method for individuals" to "provide proof of facts about themselves" to "other persons who reasonably require such proof."

Capabilities

39. *Identification:*

a. *Describe the identifier(s) used (e.g., unique number, user name, etc.):*

_____

b. *Is the identifier(s) kept confidential, i.e., only known to the ID system and the individual or available to third-parties in certain circumstances? ..... [Y/N]*

c. *Are these identifiers sufficiently unique to enable identification? ..... [Y/N]*

d. *If not, explain:* _____

e. *Describe any significant legal, technical or administrative factors that limit the nature or scope of identification transactions that can be performed using the ID system:*

_____

Background

Identification is the process of recognizing a person's identity, i.e., who they claim to be.[129] It involves asserting or presenting some evidence of an identity to a system, i.e., claiming to be a particular individual. It may involve giving a username, a unique number, a smart card, a process ID, a biometric attribute (e.g., placing your finger on a scanner), or anything else that the system has designated as a means of uniquely identifying the individual. Many ID systems use unique ID numbers or alphanumeric codes as identifiers (see Question 66). Identification is often combined with authentication (see Question 40).

40. *Authentication:*

a. *Can the ID system be used for authentication, i.e., to confirm the identity of an individual? ..... [Y/N]*

b. *If not, skip the rest of this Question 40.*

c. *Describe any significant legal, technical or administrative factors that limit the nature or scope of authentication transactions that can be performed using the ID system:*

_____

d. *Describe the authentication methods used (e.g., presentation of a password or biometric data):*

_____

e. *Are these methods sufficiently robust to enable the authentication?..... [Y/N]*

f. *If not, explain:* _____

g. *Does the ID system provide an explicit guarantee of the accuracy of authentication?..... [Y/N]*

[129] ID4D Glossary, World Bank, available upon request.

h. *Does a law or regulation assign legal responsibility for inaccurate authentication? ..... [Y/N]*

i. *If so, cite and quote/summarize:*_____

j. *Does the ID system include a system for resolving disputes over authentication inaccuracies? ..... [Y/N]*

k. *Is the dispute resolution system established by law or regulation? ..... [Y/N]*

If so, cite and quote/summarize: _____

Background

Authentication is the process of proving that a person is who they claim to be, i.e., the person enrolled in the system.[130] Digital authentication generally involves a person electronically presenting one or more "factors" or "authenticators" to "assert" their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person is (e.g., their fingerprints), knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or does (e.g., their handwriting, keystrokes, or gestures).

This evidence can be evaluated to produce a "yes" or "no" answer by comparing captured biometrics, a process known as biometric verification:

- ***offline*** for example with the biometrics stored on the ID credential, or with smartcards using a challenge/response that depends upon the user's PIN code to authenticate; or
- ***online*** with the biometrics stored on a central server in connection with the ID number provided on the credential.

When employing authentication functionality, an ID system may be constrained by the available technology and infrastructure. Offline digital authentication typically requires a smartcard or similar digital credential in combination with another factor (such as a PIN or biometric data). In addition, online digital authentication requires substantial ICT infrastructure to permit authentication against a database or even local authentication via point-of-service devices.[131]

Policymakers may specify or limit the range of transactions over which the authentication is valid. This may be achieved through laws, regulations or policies, or by technical or administrative constraints. For example, some transactions may require additional verification of an authentication, such as from a notary or other verifying party.

Like any other technical process, authentication is subject to errors. ID systems often anticipate some level of false positives and negatives in authentication and include allocations of risk (liability) and mechanisms for resolving any disputes.

Whether authentication functionality and techniques are employed will inform the types and amounts of personal data that are necessary to be collected by the ID system, and how these may be used. The means of authentication available are limited by the type of credential and the data stored on it or remotely.[132] The particular authentication uses envisioned will drive design choices for the credential and data storage.

41. *Authorization:*

a. *Can the ID system be used for authorization (i.e., to confirm particular attributes, privileges or permissions of an individual's identity)? ..... [Y/N]*

b. *If not, skip the rest of this Question 41.*

c. *Describe any significant legal, technical or administrative factors that limit the nature or scope of authorization transactions that can be performed using the ID system:*

_____

d. *In the table below, indicate any attributes that can be confirmed by the ID system in an authorization transaction. Indicate which government or private sector entities are capable of confirming such attributes through an authorization transaction with the ID system.*

Attribute confirmed in authorization	By government (specify agency or department)	By private sector (specify types of entities)

[130] ID4D Glossary, World Bank, available upon request. Authentication is similar to verification, and the terms are often used interchangeably. Verification is the process of determining the veracity or authenticity of identity attributes or credentials in order to facilitate access to a particular service. They terms can be distinguished by whether the process involves determining the veracity of particular attributes or credentials (verification) or ensuring that a person is the "true" owner of an identity or credential (authentication).

[131] World Bank Group, *Guidelines for ID4D Diagnostics*, 2018 at 19 (brackets omitted and acronym spelt out). A recent discussion of authentication capacity in Africa can be found in World Bank Group, *The State of Identification Systems in Africa: A Synthesis of Country Assessments*, 2017 at 43-44. See also Alan Gelb and Julia Clark, "Identification for Development: The Biometrics Revolution," CGD Working Paper 315. Washington, DC: Center for Global Development, 2013 at 9-10.

[132] World Bank Group, *Guidelines for ID4D Diagnostics*, 2018 at 19.

Name		
Date of birth		
Age		
Sex		
Nationality		
Address		
Eligibility for *[specify]*		
(Add additional rows as needed)		

e. *Describe the authorization methods used to confirm attributes:*

_____

f. *Indicate any authorizations for individuals that are published or otherwise publicly available or able to be queried:*

_____

Background

Authorization is a means of using an ID system to communicate permissions to use or access public or private benefits and services.

In some cases, authorization can be conferred by confirming particular attributes of an individual's identity, such as age, address or enrollment in a social benefit program. For example, an individual may become authorized to consume alcohol at a certain age and the individual's date of birth can be confirmed through an ID system. Alternatively, an authorization can be recorded on or linked directly to the identity of the resident. For example, a driving license communicates the authorization to drive a car.

Authorization functionalities which utilize confirmation of certain attributes go beyond mere confirmation of an individual's identity to involve the sharing of personal data. For example, a service provider might enter an ID number into a web portal, perhaps along with a second factor such as a password or PIN code, and then be able to access personal data about the ID holder. This approach is used in in Thailand, Indonesia and Tanzania. Alternatively, the service provider may only receive a response of "authorized" or "not authorized."

Whether authorization functionality is employed, the techniques used and any attributes that can be confirmed will inform the types and amounts of personal data that are necessary to be collected and how they may be used.

42. *Attribution:*

a. *Can the ID system be used to create binding e-signatures? ..... [Y/N]*

b. *Can the ID system be used to create digital signatures? ..... [Y/N]*

c. *If neither, skip the rest of this Question 42.*

d. *Describe any legal, technical or administrative factors that limit the nature or scope of attribution transactions that can be performed using the ID system.*

_____

Background

Attribution refers to use of the ID electronically to bind a person via an e-signature of some kind,[133] in the same way as a hand-written signature on a legal document.[134] This generally requires a legal framework that recognizes e-signatures as legally binding instruments.[135]

[133] The 2001 UNCITRAL Model law on electronic signatures defines an electronic signature as "means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message."

[134] See, e.g., Eliza Mik, "Chapter 4 - Identification and Attribution," University of Sydney, 2007.

[135] Joseph J. Atick, *Digital Identity: The Essential Guide*, ID4D, [2014] at 20

A digital signature is a type of e-signature that utilizes public key infrastructure (PKI) as a means of coding and encrypting a document. By utilizing a pair of "keys" (one which is public and one which is private and only available to the signer), the identity of the signer can be authenticated and the receiver can be assured that the document has not been altered by a third party.

Whether e-signatures and digital signature functionality is employed may inform the types and amounts of personal data that are necessary to be collected and how they may be used.

43. ***Other capabilities:*** *Describe any other capabilities of the ID system (i.e., beyond identification, authentication, authorization and attribution described above) and any limitations on their use and the source of that limitation:*

_____

44. ***Integration of capabilities:*** *Describe the level of technical and administrative integration of the available capabilities described in responses to Questions 39-43:*

_____

Background

A system that combines elements of identification, authentication, authorization and attribution together into a single, unified system under the control of a single or small number of administrators aggregates the risks of these separate purposes. While such aggregation and integration may increase efficiency, the system becomes vulnerable to single points of failure, whether hardware, software, or the people administering the system. In particular, the principles of "least privilege" and "separation of duties" apply in these environments to reduce the risk of human error or deliberate misuse (see Question 81).

Functional purposes

45. ***Specific services and tasks:*** *For each service/task below, indicate whether the ID is legally recognized for the purpose of accessing the service or carrying out the task, and whether it is legally required for such purpose. Indicate also whether other IDs may be used instead.*

Service/task	Legally recognized	Mandatory	Other substitutable IDs (*specify*)
Access to traditional banking (e.g., savings or current account opening)	Y/N	Y/N	
Access to credit (e.g., bank loans)	Y/N	Y/N	
Access to digital financial services (e.g., mobile money account opening)	Y/N	Y/N	
SIM card registration	Y/N	Y/N	
Voting or voter registration (*specify*): _____	Y/N	Y/N	
Eligibility for employment	Y/N	Y/N	
As a travel document for domestic travel (*specify*): _____	Y/N	Y/N	
As a travel document for foreign travel, whether as or in place of a passport (*specify countries where accepted*): _____	Y/N	Y/N	
Eligibility for passport	Y/N	Y/N	
Purchase of real estate	Y/N	Y/N	
Purchase of insurance	Y/N	Y/N	
Access to public pension benefits	Y/N	Y/N	
Access to public health services	Y/N	Y/N	
Registration of a business	Y/N	Y/N	
Agricultural services (*specify*): _____	Y/N	Y/N	
Education enrolment or exams (*specify*): _____	Y/N	Y/N	
Social assistance programs (*specify*): _____	Y/N	Y/N	

Other (*specify*):_____	Y/N	Y/N	

Background

Question 45 requests information on the role of the ID system in accessing services and performing tasks. These roles inform the types and amounts of personal data that are necessary to be collected by the ID system and how they may be used.

The third column in the table above relates to substitutability of the ID system. If no other ID is substitutable (or if the substitutable ID is not readily available), the ID system can be considered required for that particular service or task. Whether the ID system is required for an individual to access services and perform tasks is an indication of the level of incentive to register with that ID system. If essential services or tasks require registration, this may indicate a *de facto* obligation to register even in the absence of an explicit mandate (see Question 56).

The third column should also provide some insight into whether there are fragmented, overlapping forms of identification in use which could be rationalized and streamlined. Some countries have a fragmented approach to identification, with disparate forms of ID documents such as health insurance cards, bank identity cards and voter identity cards. This can increase costs and undermine the utility and popularity of the foundational ID.

In addition, Question 45 may provide insight into the disadvantage facing a person unable to register with the ID system, and so help in assessing the consequences of exclusion. While ID systems can be a tool to improve social and economic outcomes, the interests of marginalized and vulnerable groups must be closely assessed to avoid any further disadvantage. A strict conditioning of essential government services on registration in an ID system may be detrimental if coverage is not yet widespread and/or access to the system is not broadly inclusive. This problem can be particularly acute when eligibility for registration is limited only to individuals with citizenship or other legal status.

46. *Is the ID system recognized in any foreign countries?* ..... *[Y/N]*

If so, in the table below list the functional purposes for which the ID is recognized abroad, and identify with a tick the countries in which the ID system may be used for that purpose. See Question 45 for a list of examples of functional purposes. If there are too many countries, copy and paste to create a new table below or format a different means of efficient presentation.

Functional purpose(s)	[Country]	[Country]	[Country]	[Country]	[Country]	[Country]
[List]						

Inclusion

Coverage and eligibility

47. ***Coverage:*** *The information below should be based on readily available sources or interviews.*

a. *What percentage of the population **as a whole** is registered in the ID system? Provide the actual percentage or estimate the range. ……[0-20 21-40 41-60 61-80 81-100%]*

b. *Provide the basis for this percentage:* _____

c. *What percentage of the population **above the minimum age** is registered in the ID system? Provide the actual percentage or estimate the range. ……*
[0-20 21-40 41-60 61-80 81-100%]

d. *Provide the basis for this percentage:* _____

e. *What percentage of the population **that is estimated to be eligible** (e.g., it may be that only citizens are eligible) is registered in the ID system? Provide the actual percentage or estimate the range..... [0-20 21-40 41-60 61-80 81-100%]*

f. *Provide the basis for this percentage: _____*

Background

There are many advantages of good coverage. With a robust ID system, individuals are better able to access services and governments are able to operate and direct public resources more efficiently. Robust ID systems may also improve national statistics to better inform future policies.

Question 47 seeks to provide a general sense of the percentage of the population which is included in the foundational or key functional ID system being reviewed. Exclusion may be due to eligibility requirements, such as citizenship or legal status, which form an institutional barrier to those populations who cannot meet those requirements (see Question 48). To avoid distorting coverage comparisons, Question 47(c) asks about coverage of the general population who meet the age requirement. Question 47(e) asks about coverage of only the eligible population to provide a sense of whether there are obstacles to coverage that are unrelated to eligibility, i.e., what percentage of those individuals who *can* register *have* registered.

When assessing coverage under Question 47 it is important to remember that marginalized persons (such as refugees, illegal immigrants or persons not recognized as citizens) may be overlooked in censuses or other population estimates. In the absence of universal death and emigration registration, the most effective way to measure coverage is to use survey-based approaches, rather than administrative data from the ID system itself.

Estimates of the percentage of the population which is registered with the ID system can give some indication of the level of inclusion in the system. Low levels of coverage may prompt further analysis to see if any discriminatory factors are responsible for the shortfall, and how the shortfall can best be addressed.

Examples

In **Thailand**, the government is using the national ID system to help achieve universal health coverage and improve overall delivery of health services, as well as many other government services.

In **Peru**, universal registration of the population facilitates immediate government assistance in the event of a natural disaster. These examples show how a national ID system with good population coverage can help a country achieve a wide range of development goals.

48. *Differentiation among citizens, non-citizens, refugees, migrants, etc.:*

a. *Does the ID system differentiate based on legal status (e.g., citizens, legal residents, refugees/asylum seekers, stateless persons)? (For example, differential treatment could involve providing different forms of ID, providing different identifiers, including specific attributes on a credential, or treating certain legal status groups as ineligible for the ID.)..... [Y/N]*

b. *If so, describe how: _____*

c. *Is there a distinct non-citizen version of the ID? ..... [Y/N]*

d. *If so, describe any differences from the citizen version in credentials, uses, functionality or rights bestowed:*
_____

e. *Is there a system of independent oversight of the ID system's decisions on IDs issued in relation to the legal status of the person? ..... [Y/N]*

f. *If so, indicate the responsible authority and describe the process:*
_____

g. *In the table below, for each category of person indicate with a tick mark whether they are entitled to, required to, or not permitted to register with the ID system (assuming all other eligibility factors, such as minimum age, are met). If distinct non-citizen IDs are available for certain categories, indicate in the box whether they may or must be obtained. Alongside the tick, provide any explanatory context (e.g., if temporary residents must live in the country for a certain period of time to obtain eligibility, indicate that time). Revise the table if it does not fit categories used in the country, and add any additional categories of persons at the bottom of the table.*

Category	ENTITLED to register	REQUIRED to register	NOT PERMITTED to register	ENTITLED / REQUIRED to obtain a non-citizen ID
All persons born in the country				

All persons present in the country				
All adults present in the country				
Citizens residing inside country				
Citizens residing outside country				
Citizens who have dual citizenship with another country				
Permanent residents				
Temporary residents (e.g., persons on temporary work or study permits)				
Migrants with proof of legal immigration status				
Migrants with ID documents from another country but without proof of legal immigration status				
Migrants lacking ID documents and proof of legal immigration status				
Persons born in the country with no documentation of citizenship or legal immigration status				
Refugees/asylum seekers				
Stateless persons				
Minors who would otherwise be eligible				
[Add any other categories]				

Background

Some ID systems limit registration or make other distinctions on the basis of citizenship or other legal status, potentially excluding significant segments of the population from the benefits of the ID system. Other ID systems are open to non-citizen residents, including persons who have been granted permanent residence status, adults who are domiciled in the country in question by virtue of marriage to a citizen, children who are domiciled in the country by virtue of a parent's status, or persons temporarily present in a country on work or study visas.

Where registration is open to some **non-citizens**, the credential issued may vary based on legal status. For example, citizen and non-citizen ID numbers may vary in construction, or physical credentials may be labelled with "citizen" or "non-citizen" designations or issued in different colors or formats. Data on citizenship can be embedded in a "smart card" in a way that is visible only to those who need data on citizenship status.

Where there is a discernible distinction in physical credentials, it is important to assess whether this violates individual privacy by making legal status evident to persons without any legitimate interest in this data. It is also important to consider whether this creates additional opportunities for discrimination and exclusion. On the other hand, in some countries, the use of some distinctions between the credentials issued to citizens versus non-citizens may overcome political reluctance to register non-citizens, reducing exclusion. These issues need to be considered in the context of each country and carefully balanced.

Migrants, refugees and stateless persons present special problems of identification. Individuals in these groups who have no identity documents may be harassed, exploited, detained, expelled or stranded in transit countries. The absence of legally-valid identification documents issued by the host country leads to additional vulnerabilities including barriers to:

- accessing basic services such as health care, education for children, and social benefits including legal employment;
- registering vital events in the host country such as births, deaths and marriages; and
- future naturalization in the host country or by undermining protection for human rights.[136]

[136] Bronwen Manby, *Identification in the Context of Forced Displacement*, World Bank, June 2016 at 8-9, 11.

Governments are required under the *1951 UN Convention relating to the Status of Refugees* to provide every refugee with a means of identifying him or herself in the form of either a valid travel document or identity papers. Similar obligations apply to stateless persons and the internally displaced under the *1954 Convention relating to the Status of Stateless Persons*.[137] Furthermore, governments may find that issuing identity documents of some sort to persons in these categories aids security, crime prevention and detection and the provision of public services. Inclusion in an ID system is one way to meet these obligations and reap these benefits.

There are also challenges inherent to issuing identification to members of these groups including:

- resistance from governments which seek to restrict access to documentation;
- resistance from refugees and other migrants who do not want to be identified;
- human trafficking and false documentation; and
- difficulties of identity validation in the absence of documentation.[138]

The collection of biometric data on refugees also poses particular risks if the data is shared and finds its way back to a government from which the refugees fled, as this could place them at heightened risk if they are deported or repatriated.[139]

An ID system may also allow for registration and issuance of credentials to **citizens who reside outside of the country**. The *1963 Vienna Convention on Consular Relations* provides authority for issuing identity cards to persons who are resident outside their country of nationality.[140] While such identity credentials would have no bearing on the individual's status in the state of residence, they could help the home-country government locate citizens in case of emergencies such as accidents or national disasters and it can help with tracing citizens who go missing. Keeping track of citizens who reside outside their country of nationality can also assist with keeping national civil registration records up-to-date, such as by connecting records of citizen marriage or death outside the country with the records on file inside the country.

The issuance of ID credentials to citizens living outside their home countries also has benefits for those citizens. In some cases, a lack of identification in the country of residence may limit access to services that are available to them or intensify their fear of contact with police and other official institutions. Lack of identification can also prevent immigrants from opening bank accounts, which may mean that they may have to cash pay-checks using expensive check-cashing services, or transport and store cash, which makes them vulnerable to robbery and theft, or use unreliable informal networks or expensive wire-transfer services to remit money to families at home.[141] Possessing ID credentials from their home country can be particularly important for refugees or illegal immigrants in their current country of residence, who might otherwise be completely undocumented.

Examples

In **Botswana**, the National Identity Card (popularly known as "*omang*") is issued only to citizens and designed to serve as a proof of citizenship.[142]

In **India**, the Aadhaar system issues an identification number backed up by biometrics to every "resident" of India, defined by the enabling law as "an individual who has resided in India for at least 182 days in the last 12 months."

Mexico provides a distinct type of ID ("matrícula consular") to any Mexican citizen living abroad, through consular officials in the citizen's country of residence. Where applicants cannot provide sufficient documentation for the ID, the consulate confirms the applicant's identity by investigating his or her background through authorities in Mexico. The applicant must also provide proof of their address in the country of residence. The identification card includes an ID number issued by the Government of Mexico, a photograph and the address in the country of residence, with corresponding data being recorded in central registry in Mexico. This identification document has no bearing on immigration status in the country of residence and merely demonstrates that the holder is a Mexican national living outside of Mexico. In the United States of America, immigrants can use the matrícula consular for purposes such as opening bank accounts, obtaining a taxpayer identification

---

137 Convention relating to the Status of Stateless Persons, 1954, Article 27; UN Guiding Principles on Internally Displaced Persons, Principle 20; Kampala Convention, Article 13.

138 See Bronwen Manby, *Identification in the Context of Forced Displacement*, World Bank, June 2016 at 19.

139 Jennifer Lynch, *From Fingerprints to DNA: Biometric Data Collection U.S. Immigrant Communities and Beyond*, Immigration Policy Center, 2012 at 3.

140 Consular functions include "protecting in the receiving State the interests of the sending State and of its nationals, both individuals and bodies corporate, within the limits permitted by international law" and "helping and assisting nationals, both individuals and bodies corporate, of the sending State" (Art 5.a and e).

141 "Consular ID Cards: Mexico and Beyond", 1 April 2003, Migration Policy Institute.

142 See Botswana's National Registration Act, Chapter 01:02; "What is a National Identity Card?", Government of Botswana website.

number for the payment of federal income tax, obtaining drivers' licenses or proving their identity to law enforcement officers.[143]

In **New York City**, municipal identification cards are offered to all residents, regardless of their immigration status, to give them a form of ID that is valid for interactions with schools, hospitals, city government, law enforcement agencies and some banks. This move has been praised by civil rights and immigration reform advocates as a step toward integrating undocumented immigrants into their local communities, and criticized by those who believe it encourages illegal immigration by offering benefits without requiring legal status.[144]

49. *Minimum age:*

a. *What is the minimum age at which otherwise eligible individuals are **permitted and/or required to register** in the ID system?*

Permitted?.....[Y/N] Required? .....[Y/N]

b. *What is the minimum age at which otherwise eligible individuals are **permitted and/or required to be issued a unique identification number** (if applicable) by the ID system?*

Permitted?.....[Y/N] Required? .....[Y/N]

c. *What is the minimum age at which otherwise eligible individuals are **permitted and/or required to be issued a physical or electronic credential** (if applicable) by the ID system?*

Permitted?.....[Y/N] Required? .....[Y/N]

d. *Specify if any **separate category of credential is issued only to children** and describe the differences from the credential issued to adults:*

_____

e. *Specify if any separate categories of credential are issued to different categories of population groups and describe the differences from other credentials:*

_____

f. *What is the minimum age at which otherwise eligible individuals are **permitted and/or required to have biometric data captured** (if applicable) by the ID system?*

Permitted _____years Required _____years

g. *If biometric data of children is captured, specify any requirement that it be updated and indicate when such updates are required:*

_____

Background

Globally, registration for national IDs generally tends to take place between the ages of 14 and 18, sometimes using a unique identification number that has been assigned at the time of birth registration.145 However, some countries register children in their national ID systems and issue ID credentials to children from very young ages or even from birth.

Registering children in ID systems can facilitate access to public benefits and services, help to prevent identity theft, child trafficking and child labor and obviate the need to present other documents such as birth certificates in order to access services. It may be useful in particular for access to health services and education. A low age of enrolment can increase certainty of identity since birth certificates in many countries are easily forged. Registering children in ID systems could also help children from marginalized groups prove their identity or status, lowering the risks of harassment, exclusion or discrimination. Recent innovations for children include using ID systems to connect a child with emergency contact numbers and immunization history.

---

[143] See National Immigration Law Center, "Basic Facts about the Matrícula Consular", last updated December 2015; "Matrícula Consular" (in Spanish), 22 January 2018, General Consulate of Mexico in New York website.

[144] See, e.g., Aaron Morrison, "Immigrant Identification Card: New York's ID Program Watched by Immigration Reform Advocates Across Nation", *International Business Times*, 15 January 2015; "IDNYC Municipal ID Card", undated, Official Website of the City of New York: "The IDNYC program offers a photo identification card for residents of New York City who are at least 14 years old. This municipal ID card connects New Yorkers to services, programs, and benefits, regardless of immigration status, homeless status, or gender identity."

[145] For example, in South Africa, citizens and permanent residents must apply for an identity card at age 16 – but the ID number will be the same one which was assigned at the time of birth registration in the civil registration system.

However, children typically do not engage in transactions without the assistance of adults, reducing the utility of their inclusion in some ID systems. Registration of children also raises some risks. Children are more vulnerable to identity theft than adults and if credentials are issued to children, certain protective measures may be needed as such thefts may go undetected for years.[146] The issuance of ID credentials to children may lead to further disadvantages for children from marginalized groups, who may be unable to obtain IDs and whose parents or guardians may lack the necessary incentives for enrolment. Privacy may be more easily compromised or abused when data subjects are young children, who are less equipped to verify and monitor the accuracy and use of data about them.

Collecting biometric data from children raises special practical and ethical considerations.[147] Countries which issue ID credentials to children typically require that these be renewed or replaced at a later stage to allow for the collection of mature biometrics or to replace the photograph as the child matures.[148] The collection of sensitive personal data also raises more complicated issues of consent for children compared to adults.[149] Finally, some have argued that child identity documents divert resources from more fundamental efforts to improve a country's birth registration system, or increase the ID coverage of adults.[150] Accordingly, the rationale for any such policy should be clearly articulated and understood in the specific country context.

Examples

Belgium: An-eID card is compulsory for citizens from the age of 12. Children under age 12 may obtain a Kids-ID card (issued to the person with parental authority over the child), and this is compulsory for children under 12 who travel abroad.[151] Children's IDs contain a safety feature which provides contact numbers in case of emergencies. The reverse side of the Kids-ID contains a hotline number which use the child's identification number to link automatically to the telephone number of one of the child's parents or another relative. Parents may also provide up to five additional contact numbers, classified by order of importance. If there is no response to any number on the list, the call automatically goes to an agency for missing children. The Kids-ID contains an electronic chip designed to protect children on the Internet by enabling them to identify themselves in chat rooms which are reserved for children.[152]

Uruguay: A *Cédula de Identidad* (identity card) is compulsory from birth. Enrolment takes place at birth, and parents must obtain an identity card for the infant within 45 days. A thumbprint is taken at enrolment. However, because of the difficulty of using the fingerprints of newborns for matching, this biometric information is initially stored but not used for identity validation or de-duplication. When a child reaches age five, a complete set of ten fingerprints is taken and stored as the basis for identity validation.[153]

India: Children may be registered in the Aadhaar program from birth, but no biometrics are captured for children under age five. Their Unique Identification Number (UIN) is processed on the basis of demographic information and a facial photograph, and linked to their parents' UINs. Children may be re-enrolled when they reach age five with ten fingerprints and iris and facial photographs. The biometric data is updated once they reach age 15.[154] It is not legally compulsory for children to enroll in Aadhaar, but many schools ask parents to provide their children's Aadhaar card as a condition of admission.[155] The Government of India has also made access to the free school midday meal for children contingent on the

---

[146] See, e.g., Ron Lieber, "Identity Theft Poses Extra Troubles for Children", *The New York Times*, 17 April 2015.

[147] See, e.g., European Union Agency for Fundamental Rights, *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, 2018 at Chapter 7.

[148] See Alan Gelb & Anna Diofasi, "Preliminary Discussion Paper on the Future of Identification and Development", Center for Global Development, draft version dated 31 October 2015.

[149] See, e.g., "Child ID Cards and Unanswered Questions", Outstanding Health Situations, Thai Health 2012, Institute for Population and Social Research, Mahidol University: 2012.

[150] See, e.g., Cyril Bennoua, "Will child ID cards really protect children's rights?", The Jakarta Post, 6 April 2016.

[151] "The electronic ID card", undated, Direction générale des Télécommunications et de la Société de l'Information website; "Kids-ID to be available for all under-12s", 25 March 2009, Zetes Group website.

[152] Alea Fairchild and Bruno de Vuyst, "The Evolution of the e-ID card in Belgium: Data Privacy and Multi-Application Usage", 2011; "The electronic ID card", undated, Direction générale des Télécommunications et de la Société de l'Information website; "Kids-ID: Belgian child protection services, both within Belgium and abroad", [2016], Gemalto (digital security company) website.

[153] Vanina Camacho, Guillermo Garella, Francesco Franzoni, Luis Di Martino, Guillermo Carbajal, Javier Preciozzi & Alicia Fernandez, "Recognizing infants and toddlers over an on-production fingerprint database", paper delivered at 2017 International Conference of the Biometrics Special Interest Group (BIOSIG), 20-22 September 2017. See also "The story behind Uruguay's new eID card platform", undated, Gemalto (digital security company) website.

[154] FAQs-Children, "How will children be captured in the database?", undated, Unique Identification Authority of India website.

[155] See, e.g., Sanskriti Talwar, "'Poor kids not getting school admissions for want of Aadhaar'", The Sunday Standard, 15 April 2018; "Aadhaar for kids: How to enroll your child for Aadhaar number", The Times of India online, updated 13 March 2018; "Nursery admissions 2018: Five things to know before applying", The Indian Express online, updates 20 December 2017; Kamini Mehtal, "Without Aadhaar card, your kid might not get school admission", The Times of India online, 25 November 2017; "Nursery admission for your 3-yr-old? Get an Aadhaar card", Daily News and Analysis India, 3 January 2017.

provision of "proof of possession" of an Aadhaar number or Aadhaar authentication.[156] There are accounts of Aadhaar registration for children resulting in the identification of missing children who were reunited with the families.[157] The government is focusing on expanding the enrolment of children, with schools and day care centers being targeted for enrolment.[158]

Indonesia: Beginning in 2016, optional identity cards have been issued to newborns along with their birth certificates in a number of provinces. There are two categories of identity cards for children: one for children under 5 years old and another for children between the ages of 5 and 17 years old. The Child Identity Cards (*Kartu Identitas Anak* (KIA)) are automatically changed into Citizen Identity Cards (*Kartu Tanda Penduduk* (KTP)) at age 17 (or younger for a married female), but the identity number does not change.[159] Some areas reportedly experimented with incentives such as partnering with local businesses to provide discounts for school supplies and staple foods for parents of children with IDs.[160]

Malaysia: "MyKad" ID cards are issued at age 12, and updated at 18. Children below age 12 may apply for non-compulsory "MyKid" ID cards. The MyKid card, unlike the adult MyKad, does not record a photograph or a thumbprint but contains a chip with information about birth, health and education.[161] The Health Ministry in 2017 announced a plan to utilize MyKid as a medium to record immunization history, replacing the current immunization handbook.[162]

Accessibility and barriers to inclusion

50. *Fees and other costs:*

a. *Does the ID system charge fees for registration?* ..... *[Y/N]*

b. *Does the ID system charge fees for renewal upon expiration?* ..... *[Y/N]*

c. *Does the ID system charge fees for replacement of lost credentials?* ..... *[Y/N]*

d. *What other significant fees apply?* _____

e. *Can an individual who cannot afford fees get an exemption?* ..... *[Y/N]*

If so, how? _____

f. *Identify any groups automatically exempted from ID costs (e.g. rural residents, the elderly):*

_____

g. *Are the costs set by law, regulation or policy?*..... *[Y/N]*

h. *If not,*

i. *i. What person or agency sets costs?* _____

j. *ii. Is it required to do so in accordance with a law, regulation or policy?*..... *[Y/N]*

Background

While ID systems may impose fees on individuals as a means of achieving financial sustainability (see Question 102), such fees are consistently identified as a barrier to registration. Even a low user fee could present a barrier to access for many.[163] Furthermore, even uniform costs may impact differentially on some groups, such as persons without their own transport, persons who live in remote areas, or women who lack independent access to financial resources.

---

[156] Ministry of Human Resource Development (Department of School Education and Literacy), Notification, New Delhi, 28 February 2017: (1) Individuals desirous of availing the benefits under the [Mid Day Meal] Scheme offered at the Schools are required to furnish proof of possession of Aadhaar number or undergo Aadhaar authentication."

[157] See, e.g., Maya Sharma, Nehal Kidwai, "How Aadhaar Card Helped Reunite Missing Children With Their Families", updated 12 July 2017, NDTV website.

[158] See "UIDAI plans to formalize child enrolments for Aadhaar", *LiveMint* e-paper, 26 December 2015.

[159] See Erika Anindita Dewi, "Govt to issue identity cards to RI children", *The Jakarta Post*, 29 February 2016.

[160] Cyril Bennoua, "Will child ID cards really protect children's rights?", *The Jakarta Post*, 6 April 2016.

[161] "MyKid", Ministry of Home Affairs, National Registration Department, 2016. The terms for both MyKid and MyKad are wordplays. "My" refers to the digital address for "Malaysia" as well as the being English word "my", and "Kid" is an abbreviation for "Kad Identiti Diri" ("personal identity card") as well as being slang for a child, while "Kad" is an abbreviation for "Kad Akuan Diri" ("personal identification card") or "Kad Aplikasi Digital" ("Digital Application Card") as well as meaning "card".

[162] Zahratulhayat Mat Arif, "MyKid may be used to store immunisation history of children", *New Straits Times*, 28 August 2017.

[163] Alan Gelb and Anna Diofasi, "Using Identification for Development: Some Guiding Principles", Center for Global Development, 2016.

Fees may be applied at the time of initial registration or subsequently, for example a fee imposed to obtain a copy of a lost or destroyed credential or, in the case of civil registration, birth certificates. There may also be indirect costs, such as travel and lost wages, which have a disproportionate impact on the poor.

With respect to civil registration systems, UNICEF advocates that birth registration (including late registration) should be free, as a mechanism to ensure that birth registration is universal.[164] The principle that all birth registrations, including late registrations, should be free of charge has also been recognized in several UN resolutions.[165] Free death registration will also likely encourage accurate reporting.[166]

Examples

Some countries register individuals and provide an initial ID credential for free but impose a fee for replacing lost credentials. For example, in **Malaysia**, prompt application by citizens for e-ID cards (within 30 days of reaching the requisite age of 12) is free, while non-citizens and citizens who register late must pay a fee. Replacements for lost or damaged cards are on a sliding scale based on the number of replacements, with exemptions being available to persons with disabilities, the poor, senior citizens, children below age 18, victims of natural disasters and persons who lost their cards as a result of being a victim of crime. [167]

Even if free birth registration is the official policy, this may not always be respected in practice. In **Indonesia**, a 2013 amendment to the relevant law eliminated fees for all civil registration documents, but many parents continued to report paying "fees" and parents of unregistered children continue to identify cost as the main reason for failure to register the births.[168]

51. ***General barriers to inclusion:*** *Are there barriers to inclusion which have been identified as significantly responsible for inhibiting registration of eligible individuals in the ID system..... [Y/N]*

If so, specify. _____

Background

There may be numerous practical barriers to participation in an identity system, ranging from direct costs to access to registration locations to language barriers. A complex or geographically centralized registration process can serve as a barrier to registration. Even modest fees can create barrier when considered with other costs imposed on individuals to complete registration. By identifying the inhibiting factors that contribute to coverage gaps in the eligible population, interventions can be designed to remedy those specific factors. For example, if the cost of registration fees inhibits registration, subsidies or waivers may be considered for certain populations. If lack of information about or mistrust of the ID system is inhibiting registration, then outreach and education campaigns may be useful.

Examples

A 2015 country assessment of **Côte D'Ivoire** found that the cost of a national ID card was FCFA 5,000. However, the estimated additional out-of-pocket expenses to obtain the card including the cost of supporting documentation totaled around FCFA 10,000-13,000. This aggregate amount reflected approximately one month of wages for a poor person, creating a huge barrier to registration.[169]

In **Kenya** the enrolment process for the nation ID involves in-person verification at the National Registration Bureau and printing and physical mailing of applications. While the process is supposed to take approximately 30 days, residents outside of Nairobi reported that it could take as long as 2 years.[170]

---

[164] Committee on the Rights of the Child, "General Comment No. 7: Implementing child rights in early childhood", para 25. UNICEF's Implementation Handbook for the CRC states that birth registration should be "free, or at least free to poor parents". Rachel Hodgkin & Peter Newell, *Implementation Handbook for the Convention on the Rights of the Child (Third Edition),* UNICEF, 2007 at 100. See also, e.g., UNICEF, *A Passport to Protection: A Guide to Birth Registration Programming*, 2013 at 23, 25.

[165] Such resolutions include: A/HRC/RES/28/13, 7 April 2015, para 6; A/HRC/34/L.24, 20 March 2017, para 9; A/RES/69/157, 3 February 2015, para 48(i)-(j); A/HRC/22/L.14/Rev.1, 19 March 2013, para 5; A/HRC/19/L.31, 20 March 2012, paragraphs 29-30; A/HRC/19/L.24, 16 March 2012, para 4.

[166] UN Department of Economic and Social Affairs, Statistics Division, *Principles and Recommendations for a Vital Statistics System (Revision 3)*, 2014, para 364.

[167] "RM1,000 for third replacement IC from Thursday", *Free Malaysia Today,* 15 October 2015; "MyKad Application For Children Aged 12", Malaysia Ministry of Home Affairs, National Registration Department website.

[168] James C. Knowles, "Assessment of the quality and relevance of existing data to monitor the gender dimensions of CRVS in Asia and the Pacific", Report to the UN Foundation under the Data2X Initiative, May 2016 at 7-8.

[169] World bank Group, Identification for Development (ID4D) Identification Systems Analysis, Country Assessment, Côte D'Ivoire, June 2015 at 16.

[170] ITU-T Focus Group Digital Financial Services, Review of National Identity Programs, May 2016 at 31.

52. *Discriminatory barriers to inclusion:*

k. *In the table below, tick where there are legal barriers to registration in the ID system for specific population groups, and describe the barriers.*

Population groups	Legal barriers? (tick)	Describe the barriers
Individuals who do not speak an official language		
Racial groups *(specify)*		
Ethnic groups *(specify)*		
Religious groups *(specify)*		
Women		
Individuals with disabilities		
Elderly		
Individuals in remote or inaccessible areas (*specify, and list each separately*)		
Undocumented children, or children of undocumented adults		
Neglected, abandoned or orphaned children (*specify*)		
Mentally ill		
Other(s) (specify):		

Background

While Question 51 sought to identify factors that may inhibit registration of eligible individuals, Question 52 identifies barriers to registration that affect specific populations who may be vulnerable to exclusion. Although explicit exclusionary measures aimed at specific groups are uncommon, administrative procedures such as the location of offices and the languages spoken by relevant staff may pose *de facto* barriers. In addition, ID systems may exclude or marginalize persons such as transgender persons, nomads, religious minorities or dissidents – who challenge the national authority's standard notions of identity.

When responding to Question 52, it may important to consider the role of barriers in other, related ID systems that may also impact the ID system at issue. For example, in some cases registration in a separate civil registration system or a functional ID system may be necessary for or otherwise affect registration in a national ID system. For example, birth registration documents may be required to register in an ID system or may make such registration faster and less expensive.

The principles of social justice relating to social inclusion are enshrined in international conventions such as the *International Covenant on Economic, Social and Cultural Rights*. Several international conventions address the exclusion of specific groups, including the *Convention on the Elimination of all Forms of Racial Discrimination*, the *Convention on the Elimination of All Forms of Discrimination Against Women*, the *International Convention on the Protection of the Rights of all Migrant Workers and Members of their Families*, and the *United Nations Declaration on the Rights of Indigenous Peoples*.

Examples

Some barriers are specific to certain populations. For example, a woman in **Afghanistan** must submit her husband's ID card or the ID card of a male relative to complete the application for a Tazkera ID.[171]

In **Iraq**, a woman can only be granted Civil ID Status if vouched for by a male relative.[172]

[171] ITU-T Focus Group Digital Financial Services, Review of National Identity Programs, May 2016 at 34.

[172] *Ibid*.

53. ***Reducing barriers to registration:*** *If barriers were identified in Question 52, have any laws, regulations or policies been introduced to overcome such barriers? ..... [Y/N]*

If so, cite and quote/summarize, and if information is available, evaluate their effectiveness.

_____

Background

Once barriers to registration are identified, policies can be developed, and actions can be taken, to increase inclusion. For example, if lack of fluency in an official language is a barrier for some groups, registration centers could increase staff fluent in local languages. If geographical isolation is a barrier to registration, outreach efforts could be made to reach those populations.

Examples

In some countries, such inclusion efforts are built into the legal framework. For example, in **India**, the Aadhaar Act calls for special measures to ensure the inclusion of women, children, senior citizens, persons with disability, unskilled and unorganized workers, nomadic tribes and other categories of individuals as may be specified by regulations. [173]

In **Pakistan**, to increase female enrolment, the National Database and Registration Authority established 15 women-only registration centers staffed fully by women. The agency also penetrated remote areas with mobile vans, motorcycle registration units, and even hikers, and worked with community leaders to enroll minorities such as transgender communities. [174]

54. ***Monitoring:*** *Does the body(ies) or agency(ies) managing the ID system issue regular substantive reports on progress in the adoption and use of the ID system? ..... [Y/N]*

   I. *If so, what indicators does it use? (Indicate with a tick in the table below)*

Penetration and use	Internal management	Published or otherwise reported
Penetration of IDs in the population		
Penetration of IDs in particular population groups (specify – e.g., by gender, age, racial, ethnic or religious group)		
Number and types of services in relation to which the ID is used for authentication		
Volumes of usage for authentication transactions		
Other: (specify)		

Births, deaths and other events

Guidance to IDEEA user

As explained in the introduction to this Part III, Part III is to be completed for each foundational ID system, including any national ID, civil registration system or other foundational system, as well as key functional ID systems. However, this sub-section is likely only relevant to civil registration systems: leave it blank when completing Part III for other systems.

55. *Births, deaths and other events*

   a. *In the case of a civil registration system, is registration in the system compulsory for births of eligible individuals? ..... [Y/N]*

   b. *If not, explain:* _____

   c. *In the case of a civil registration system, is registration in the system compulsory for deaths of eligible individuals? ..... [Y/N]*

   d. *If not, explain:* _____

[173] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 18 of 2016, §5.

[174] World Bank, *Identification for Development Strategic Framework*, 2016 at 31-32.

Background

In the case of birth registration, the principle that it should be compulsory is widely accepted and has a basis in international law.175 There is a duty flowing from the UN Convention on the Rights of the Child and the International Covenant on Civil and Political Rights to register the birth of all children immediately after their birth.176 This duty requires that birth registration apply to all children born within the country's territory "without discrimination of any kind, irrespective of the child's or his or her parent's or legal guardian's race, color, gender, language, religion, political or other opinion, national, ethnic or social origin, property, disability, birth or other status".[177]

Even when registration of all births is required, there may be other barriers to inclusion. Practical barriers may prevent registration of children born outside medical facilities or in remote areas or who are abandoned. Social factors may discourage reporting of children to unmarried parents or parents without IDs or citizenship. Some countries may also impose administrative requirements which can have an unintended exclusionary effect. For example, requirements that both parents participate in the registration process can exclude children born outside state-recognized marriage. Rules which allow only fathers or only mothers to register births in some circumstances or time periods for registration may not allow for the traditional naming practices of some ethnic groups.[178]

Registration of deaths is also critical to a civil registration system, as it is necessary to provide accurate population data and can be valuable in de-duplication processes for both a civil registration and a separate ID system and in reducing fraud. The UN High Commissioner for Human Rights reported in mid-2016 that the average rate of birth registration globally had reached approximately 65 per cent in 2010, while it was estimated that only about only 36 per cent of all global deaths were registered between 2005 and 2009.[179] Loopholes in death registration can hamper effective de-duplication in ID systems and facilitate ID theft. Although death registration is not explicitly addressed by any major international treaties, it is relevant for the exercise of other human rights, including rights relating to health, property, inheritance, social security and the right to remarry after the death of a spouse.[180] In many jurisdictions, a death certificate is needed for the settlement of the deceased's estate and access to inherited property. One mechanism which can be used to enforce death registration is to make production of a death certificate a pre-requisite for burial or other disposal of the body.[181]

The imposition of **sanctions** on individuals who fail to report births (or deaths) is more complex as fines or other penal sanctions may discourage registration or lead to false data about the date when the birth (or death) occurred to give the appearance of compliance with a prescribed time period.[182] Public education campaigns and the removal of practical barriers to registration, such as opening more registration offices to reduce distances or utilizing mobile registration points, can increase registration rates without the need to impose sanctions. Conditioning government services, such as school enrolment or social grants, on the production of a birth certificate may also encourage registration although this raises issues of exclusion and discrimination.

Examples

Some countries have successfully incorporated incentives to promote birth registrations. For example, **Ukraine** provides an incentive to timely birth registration in the form of a lump-sum childbirth grant.[183] Similarly, in **Cambodia**, some communes offer small cash payments as an incentive to register deaths.[184] In **Nepal**, widowhood pensions are provided to women who can provide death and citizenship certificates for their deceased husbands.[185]

Other countries have incorporated technological advances to increase registration. For example, in **Tanzania**, despite a law requiring registration of births, in 2010 only about 16% of children were registered with civil authorities and less than 9%

---

[175] See, e.g., UN Department of Economic and Social Affairs, Statistics Division, *Principles and Recommendations for a Vital Statistics System (Revision 3)*, 2014, para 283; Rachel Hodgkin & Peter Newell, Implementation Handbook for the Convention on the Rights of the Child (Third Edition), UNICEF, 2007 at 100.

[176] Article 7 of the UN Convention on the Rights of the Child; Article 24(2) of the International Covenant on Civil and Political Rights.

[177] Article 2 of the UN Convention on the Rights of the Child; Article 7 of the UN Convention on the Rights of the Child.

[178] "Strengthening policies and programmes for universal birth registration and vital statistics development", Report of the High Commissioner for Human Rights, UN General Assembly, Human Rights Council, A/HRC/33/22, 1 July 2016, para 18.

[179] *Ibid*, paras 11-13 (footnotes omitted).

[180] *Ibid*, para 10.

[181] World Bank, *Identification for Development (ID4D) Integration Approach*, 2015 at 83.

[182] UN Department of Economic and Social Affairs, Statistics Division, *Principles and Recommendations for a Vital Statistics System (Revision 3)*, 2014, para 373.

[183] UNICEF, Every Child's Birth Right: Inequities and trends in birth registration, 2013 at 13.

[184] James C. Knowles, "Assessment of the quality and relevance of existing data to monitor the gender dimensions of CRVS in Asia and the Pacific", Report to the UN Foundation under the Data2X Initiative, May 2016 at 9.

[185] James C. Knowles, "Assessment of the quality and relevance of existing data to monitor the gender dimensions of CRVS in Asia and the Pacific", Report to the UN Foundation under the Data2X Initiative, May 2016 at 9.

had birth certificates.[186] UNICEF partnered with mobile network operator Tigo to enable mobile phones to be used by health workers to send birth registration information to Tanzania's Registration Insolvency and Trustee Agency (RITA).[187] Registration information is sent to RITA via an Android or STK application, which issues a birth certificate that is stored in a central database and sends an SMS to a registrar confirming the certificate can be issued to the child.[188]

e. *Does the system register marriages?* ..... *[Y/N]*

f. *Does the system register divorces?* ..... *[Y/N]*

g. *Does the system register adoptions?* ..... *[Y/N]*

h. *Does the system register surrogate pregnancy births?* ..... *[Y/N]*

Mandatory nature

56. *Explicit and implicit mandates:*

a. *Where persons must register with the ID system (see Questions 48, 49 and 55), describe the source and nature of the mandate (e.g., sanctions under a law):*

_____

b. *If there is no explicit mandate, describe any conditions that make it mandatory as a practical matter, such as a requirement to be registered to access state or other essential services:*

_____

Background

An ID system may be *explicitly* mandatory, in the sense that the law imposes a sanction for failure to participate.

An ID system may be *implicitly* mandatory if access to state services depends on registration in the system, so that it is impractical for anyone to opt out. The degree to which an ID is required for practical transactions may mean that an ID system which is ostensibly "voluntary" is in fact mandatory in reality (see Question 45 and subsequent discussion).[189] A strict conditioning of essential government services on the presentation of a specific ID can be problematic if access to that ID system is not sufficiently inclusive or is applied in discriminatory ways. This problem can be particularly acute when IDs are provided only to citizens, unless alternative means are made for residents and other groups ordinarily living in a country to establish their identity and access public and private sector services (see discussion under Question 48).

Examples

In **Pakistan**, registration for the National Identity Card is technically voluntary. However, the credential is required to open a bank account, obtain a passport or gas or electricity connection, pay a utility bill or enter into any transaction with the State.[190]

57. ***Requirement to carry:*** *Are persons required to carry the ID credential? (Ignore this question if it is not a physical credential.)*..... *[Y/N]*

c. *If so,*

a. *What is the legal basis of this requirement?*

_____

b. *Does this apply only to some sub-groups of the population and, if so, which ones?*..... *[Y/N]*

_____

c. *Is this requirement routinely enforced in practice?* ..... *[Y/N]*

[186] UNICEF, New simplified birth registration initiative for children under-five launched in Tanzania, 11 May 2015.

[187] UNICEF, In Tanzania, you can now get your birth certificate by mobile phone, 16 October 2015.

[188] GSMA, Regulatory and policy trends impacting Digital Identity and the role of mobile, October 2016.

[189] This has been a question that has arisen in respect of Aadhaar, for example. See, e.g., Tinesh Bhasin, "The Aadhaar confusion: Voluntary, yet mandatory", *Business Standard*, 16 October 2017; Chirag Madia, "Aadhaar linking is voluntary, it's not mandatory to avail services: Experts", *Business Standard*, 10 January 2018. Further court rulings on this issue are expected.

[190] Malik, T., Center for Global Development, Technology in the Service of Development: The NADRA Story, 2014.

d. *What sanctions apply for failure to carry the ID credential?*

_____

Background

Some countries make it compulsory for persons to carry ID credentials with them at all times and impose fines or other sanctions for failure to do so. Such systems have been criticized on the grounds that they create too many openings for abuse. Demanding that ID credentials be shown can be an avenue for police harassment of minority groups or persons who appear "foreign" and so are suspected of being illegal immigrants, as well as serving as a prelude to more intrusive searches or investigations. It may also make people unnecessarily fearful of a situation where their ID credential is lost, stolen or destroyed. The mere fact of having to prove identity in a public space for no particular purpose may impinge on an individual's privacy—such as pass laws applied in apartheid South Africa. However, public attitudes about requirements such as these may vary depending on the local legal and cultural attitudes.

Examples

In the Netherlands, police officers, ticket inspectors on public transport and certain special enforcement officers (e.g., labor inspectors and forest wardens) are entitled to ask to see proof of identity without giving a reason. This may arise in various situations, such as traffic management, the maintenance of public order or the investigation of criminal offences. Failure to present an ID in such situation is punishable by a fine.[191]

In Spain, failure to present an ID gives police the right to detain the person temporarily while they ascertain his or her identity, and to issue a fine – although these steps do not commonly take place.[192]

Design

Vendors, technology and procurement

58. *Technology and vendor neutrality:*

a. *Is the ID system broadly technology neutral? ..... [Y/N]*

b. *Is the ID system broadly vendor neutral? ..... [Y/N]*

c. *Does any law, regulation or policy require the ID system to use open standards? ..... [Y/N]*

d. *Do any laws, regulations or policies constrain choices of technologies or vendors used in the ID system. (See also Question 59.) ..... [Y/N]*

e. *If so, cite and quote/summarize: _____*

f. *Do any contracts constrain choices of technologies used in the ID system or tie in any vendor? ..... [Y/N]*

g. *If so, cite and quote/summarize: _____*

h. *Describe any other factors that constrain choices of technologies used in the ID system:*

_____

i. *Describe any other factors that constrain competition among vendors to work on the ID system. (See also Question 59.)*

_____

Background

Dependency on a particular technology or a particular vendor can result in vendor or technology "lock-in," increasing costs and reducing flexibility of the system to meet a country's needs as they develop. A *technology neutral* design is one that approaches the ID system in a functional and output-oriented way instead of requiring specific technologies. A *vendor neutral* design ensures that a sufficient number of vendors are available to implement, maintain and improve the system

[191] Government of the Netherlands, "Compulsory identification"

[192] See "Spain: Personal Id Required in Spain", undated, Tripadvisor website; "Carrying ID in Spain", undated, Spanish Solutions website (citing Article 4 of Organic Law 4/2000); "Carrying ID", 15 October 2017, Citizens Advice Bureau Spain website.

to ensure competition. Technology and vendor neutral designs limit dependence on specific technologies and vendors, allowing for competition, lower prices, better return on investment, and improved system sustainability and flexibility including for future upgrades or introduction of new features.[193]

Any time a system procures a technology from a vendor, the terms of the purchase involve a commitment to that technology and vendor for the period of the contract. The objective when considering lock-in is to minimize unnecessary constraints in choice of technology or supplier over unnecessarily long periods of time.

The degree to which a system may be subject to vendor or technology lock-in can depend on a number of factors, and these may not be evident at the time decisions are made. Adoption of a standard for which a limited range of technologies or suppliers are available may lock the system into these and other technologies that are compatible with them for years. Contractual provisions in supply contracts or intellectual property licensing agreements (e.g., for software) may limit changes of technology or vendor for system maintenance and upgrades in years to come.

The ability of a country to maximize its flexibility in future changes of technology and vendor depends on its leverage and scale. Smaller, low-income countries may even benefit from longer term commitments to vendors. Public-private partnerships, for example, involve a long-term commitment to work with a particular private sector provider, but on the basis of certain performance targets and remedies.

Example

India's Aadhaar ID system relies on a competitive, standards-based ("plug and play") procurement model. Its standard-setting programs rely on standards that promote transparency, accountability, scalability, and technical compliance. These, and real-time, quality monitoring allow flexibility in procurement and competition among vendors, thereby limiting costs.[194]

59. *Procurement*

a. *Does the ID system utilize transparent procurement processes? ..... [Y/N]*

b. *Are the procurement processes set by law, regulation or policy? ..... [Y/N]*

c. *Do the procurement processes appear to work well in practice (e.g., integrating consideration of long-term development of the ID system, an understanding of the required technology and standards and overall financial management)? ..... [Y/N]*

d. *If not, explain. (There is no need to repeat information provided in Question 58.)*

_____

Registration

A. Collection of personal data

60. *Demographic and biographical data captured:*

a. *Indicate with a tick in the table below the demographic and biographical data captured as part of registration, whether it is mandatory, and indicating which items are "human readable" (visible to anyone on a physical ID credential) and/or "machine readable" (readable from an ID credential by a card-reader or other machine).*

Personal attribute	Captured by system	Mandatory	Human-readable on credential	Machine-readable on credential
Surname (or equivalent)				
Given/ first name				
Other names (specify):				

[193] World Bank, *Identification for Development Strategic Framework*, 2016 at 27-28; *Principles on Identification for Sustainable Development: Toward the Digital Age*, facilitated by World Bank Group and Center for Global Development, February 2017 at 13.

[194] Performance Lessons from India's Universal Identification Program, Alan Gelb and Julia Clark, Center for Global Development, CGD Policy Paper 020 of May 2013.

Biological sex				
Gender				
Date of birth				
Address / place of residence				
Data about mother *(specify):*				
Data about father *(specify):*				
Citizenship				
Residence status				
Refugee status				
Stateless person status				
Race (specify):				
Ethnicity (specify):				
Religion (specify):				
Sexual orientation *(specify):*				
Occupation or employment				
Marital status				
Languages				
Other data (specify):				

b. *What law, regulation or policy (if any) makes it mandatory to capture the indicated*

c. *attributes?*_____

Background

Any ID system involves a set of attributes that uniquely represents an individual. Some of these may be mandatory, in that registration cannot occur or the ID cannot be used without them. Some may be voluntarily included.

An **attribute** is a named quality or characteristic inherent in or ascribed to someone or something. In identification systems, common personal identity attributes include name, age, sex, place of birth, address, fingerprints, a photo, a signature, an identity number, date and place of registration, etc. [195]

The inclusion of indicators of **race or ethnicity** in an ID system increases the risk of discrimination and may require mitigating measures as to how the data may be used. While it is generally agreed that indicators of race or ethnicity should be eliminated from ID schemes, in some cases there have been countervailing concerns. When race or ethnicity is captured, the Committee which monitors the *Convention on the Elimination of Racial Discrimination* recommended that if no justification appears to the contrary, such identification shall be based upon self-identification of the individual concerned. Thus, if a public agency indicated the ethnic background of children in their birth certificates, basing this on the earlier ethnic classification of one or both of the parents, it would violate this principle of self-identification.[196]

Example

The **EU**'s *eIDAS Implementing Regulation (2015/1501)* established a minimum set of unique identity attributes for an individual for the purposes of basic requirements for mutual recognition of digital identity schemes. Mandatory attributes include: current family name(s), current first name(s), date of birth, and a unique identifier which is as persistent as possible in time. Additional attributes include: family name at birth, first name at birth, place of birth, current address and gender.

Under the **EU**'s GDPR, data regarding an individual's racial or ethnic origin would be considered "special category data." Given the sensitive nature of special category data, the GDPR provides for additional protections to ensure that the

[195] ID4D Glossary, World Bank, available upon request.

[196] General Recommendation No. 8 (1990) of the Committee on the Elimination of Racial Discrimination, Office of the High Commissioner on Human Rights (OHCHR), *Human Rights Indicators: A Guide to Measurement and Implementation,* United Nations, 2012 at 48.

processing of such data is lawful. For example, to process special category data, an entity must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

In the **United Kingdom**, the *Data Protection Act 2018* introduces additional safeguards in relation to special category data. For example, where processing for law enforcement purposes is "sensitive processing," there must be an "appropriate policy document" in place which explains the procedures for securing compliance with the data protection principles and the periods for which personal data is likely to be retained.

d. *If gender designations are captured:*

i. Is there an option to choose a "third" or an indeterminate gender?.....[Y/N]
ii. Is there an option to change the gender designation?.....[Y/N]
iii. If so, what must a registrant provide to effect a change in the gender designation (e.g., personal preference suffices, medical evidence of gender reassignment, psychological evidence of gender identification, evidence of error in existing designation, etc.)?

_____

iv. Is the change valid for legal purposes (e.g., marriage)?.....[Y/N]
v. Is the change kept confidential?.....[Y/N]

Background

The indication of **gender or biological sex** in ID system registration raises unique issues. The first is whether the ID system differentiates between these two distinct concepts. The World Health Organization defines "sex" as "[t]he different biological and physiological characteristics of males and females . . ." and gender as "the socially constructed characteristics of women and men . . ."[197] Some ID systems may use one term or the other (or the two interchangeably), without any consideration for this distinction.[198] While gender is traditionally thought of as a binary attribute (male vs female), some countries have introduced a third gender. If an individual transitions to a new gender, the ID system may need to be updated.

Examples

In a 2007 decision that recognized fundamental human rights for sexual and gender minorities, the Supreme Court of Nepal established a "third gender" category. Third gender is used to describe biological males with "feminine" gender identity or expression or biological females with "masculine" gender identity or expression. In 2008, the first Nepali citizen gained official recognition as third gender on a national citizenship ID card.[199]

India's Aadhaar identification system, which recognizes a gender category of "transgender,"[200] permits updates of gender information.[201]

e. *If religious designations are captured:*

i. Is there an option to choose an indeterminate religion?·····[Y/N]
ii. Is there an option to change the religious designation?·····[Y/N]
iii. Is the change kept confidential to the system and the individual?·····[Y/N]

Background

The inclusion of **religious designation** in an ID system raises similar risks of discrimination. The Human Rights Committee which monitors of the *International Covenant on Civil and Political Rights*, has issued a General Comment stating that the rights protected by the Convention must be understood to mean that no one can be compelled to reveal adherence to a religion or belief.

Examples

Under the **EU**'s GDPR, data about an individual's religion is considered to be "special category data."[202] Processing of such data would be subject to additional conditions and safeguards for the processing to be lawful. (See Question 60(0)) Special category data is afforded a higher level of legal protection. The unlawful processing or failure to adequately protect such

[197] World Health Organization, Gender equity and human rights, Glossary.

[198] The IDEEA and this Guidance Note generally refers exclusively to "gender" for both simplicity and uniformity.

[199] Michael Bochenek & Kyle Knight, "Establishing a Third Gender Category in Nepal: Process and Prognosis," *Emory International Law Review,* 2012, Vol 26.

[200] Neelam Pandey, "In a first, Aadhar recognizes 1,600 transgender persons," *Hindustan Times*, 27 August 2013.

[201] See Aadhaar data update form.

[202] 2016 EU General Data Protection Regulation, Article 9.

data could create more significant risks to a person's fundamental rights and freedoms, for example, by putting them at risk of unlawful discrimination.

In **Egypt**, controversy around the inclusion of religion on national IDs has been continuing for many years. In 2009, Egypt's Supreme Administrative Court upheld a lower court's ruling that all Egyptians have a right to obtain official documents such as ID cards and birth certificates without stating their religion and held that a person can put a dash in the religion field instead of choosing one of the three officially-recognized religions. In 2016, a bill was introduced into Parliament with the aim of amending the law to remove the religion field from identification cards and all official documents, and to protect citizens from being compelled to disclose their religion except where necessary to determine family matters such as inheritances and marriages.[203]

In 2016, **Jordan** recently removed all mention of religion from the face of its smart ID cards, although information about the religion of the card holder remains encoded on the card's chip and can be accessed by card readers. Supporters of the move asserted that it would advance equality before the law, while it was opposed by some who felt that it could be contrary to the Constitution's recognition of Islam as the state religion. One factor may have been concern that Islamic State terrorists might use the statement of religion on the cards to single out victims.[204]

In **Indonesia**, a law that required Indonesian citizens to choose one of the country's six main religions (Protestantism, Catholicism, Hinduism, Buddhism, Islam and Confucianism) on their ID cards was invalidated by a 2017 decision of the Constitutional Court, which ruled that the government must provide a seventh category for "follower of a native faith" ("penghayat kepercayaan"). Previously, individuals who left the religion field bank reportedly faced practical problems and discrimination, or even prosecution as atheists – while making an incorrect indication could expose individuals to charges of falsification of documents.[205]

In **India**, to minimize the burden of registration and promote inclusion, the Aadhaar ID system limits the demographic information it collects to an individual's name, gender, date of birth and address.[206]

61. *Biometric data captured:*

a. *Indicate with a tick in the table the biometric features captured as part of registration, whether it is mandatory, and indicating whether they are "human readable" (visible to anyone on a physical ID credential) and/or "machine readable" (readable from an ID credential by a card-reader or other machine).*

Biometric		Captured by system	Mandatory	Human-readable on credential	Machine-readable on credential
Photograph * Suitable for use with facial recognition? *[Y/N]* * Specify format:					
Fingerprints:					
How many on each hand?					
Tick which fingers:					
Right thumb					
Right index finger					
Right middle finger					
Right ring finger					
Right little finger					
Left thumb					
Left index finger					

[203] Liam Stack, "Egyptians win the right to drop religion from ID cards", *Christian Science Monitor*, April 20, 2009; Human Rights Watch, *Prohibited Identities: State Interference with Religious Freedom*, 2007; Rami Galal, "Will Egypt stop listing religion on official IDs?", Al Monitor, *Egypt Pulse*, 14 June 2016.

[204] Gregory Tomlin, "Jordan: No more religion on ID cards", *Christian Examiner*, 5 July 2016; "Jordan loses religion from identity cards", *Albawaba*, 5 July 2016; Suzanna Goussous, "Authorities to begin releasing smart IDs by mid-May", *The Jordan Times*, April 12, 2016.

[205] Gary Nguyen, "Indonesian law requiring citizens to identify with 1 of 6 religions is overturned", *World Religion News*, 9 November 2017; Devina Heriyanto, "Q&A: Indonesia's native faiths and religions", *The Jakarta Post,* 14 November 2017.

[206] GSMA, Aadhaar: Inclusive by Design, March 2017 at 21.

Left middle finger					
Left ring finger					
Left little finger					
Signature * Alternative provision for those unable to sign? [Y/N]					
Iris					
Palmprint					
Eye color					
Hair color					
Height					
Voice print					
DNA					
Other (specify):					

b. *What law, regulation or policy (if any) makes it mandatory to capture the indicated attributes?*_____

Background

Biometric data comprises physical or behavioral attributes of an individual, including fingerprints, irises, facial images, gait, signatures, keystrokes, etc. [207] It results from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person.[208]

Photographs are considered to be biometric data only when they are processed in a way which allows for unique identification or authentication, such as by means of facial recognition software. [209] Genetic material is also a form of biometric data. It invokes privacy concerns different from those involved in other biometrics, as DNA can contain information about a person's entire genetic make-up, including information about other family members, family relationships, health, race and other personal matters (See Question 16).[210]

Collection of biometric data may be restricted or prohibited by the existing legal and regulatory framework. Many legal systems contain constitutional or other protections of privacy rights which may extend to capturing biometrics for an ID system (see questions in Part III).

Some ID systems take measures to avoid physical exclusion from the ID system for individuals with disabilities or those who lack particular physical characteristics. For example, the parameters of some systems may exclude persons such as amputees who lack fingerprints, or persons who perform manual labor which causes erosion of their fingerprints. Those ID systems may include non-discriminatory alternatives.

Advances in technology have allowed for reliable authentication with a high degree of accuracy if sufficient high-quality biometric data is captured and compared. However, the degree of accuracy which is achieved can be affected by factors such as the technology used and the skill of the operators who capture the data.

Accuracy can be improved by increasing the number of biometrics captured (such as recording ten fingerprints instead of two), performing data quality checks at the time of data capture and recapturing substandard data, ensuring that biometric images are mapped to the right body part and by using multiple types of biometrics (such as fingerprints together with iris scans).[211] The accuracy of biometric verification as a means of authentication must also be considered in light of the country's population size and technology capacities.

[207] ID4D Glossary, World Bank, available upon request.

[208] *See*, 2016 EU General Data Protection Regulation, Article 4(14).

[209] Council of Europe, "Draft Explanatory Report prepared for proposed modernised Convention 108", 2018 at para 58; *2016 EU General Data Protection Regulation*, Recital 51.

[210] Jennifer Lynch, "From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond", Immigration Policy Center, 2012, Executive Summary at 2.

[211] See Alan Gelb and Julia Clark, "Identification for Development: The Biometrics Revolution." CGD Working Paper 315. Washington, DC: Center for Global Development, 2013.

Example

India's Aadhaar system captures a large amount of biometric data (10 fingerprints plus two irises) in light of its population of some 1.2 billion people. It is estimated that the probability that a duplicate enrolment would not be caught (a false negative) is 0.035% and the probability that an individual would be erroneously classified as a duplicate enrolment (a false positive) is 0.057%.[212]

62. *Performance monitoring:*

a. *Do the operators who capture the data receive training on how to capture high-quality data? ..... [Y/N]*

If so, describe if this differs for biometric as opposed to non-biometric data capture:

b. _____

c. *Are initial quality checks performed locally during data collection? ..... [Y/N]*

If so:

Describe if these differ for biometric as opposed to non-biometric data capture:

d. _____

Describe the quality metrics used for biometric and non-biometric data capture:

e. _____

f. *Is data recaptured if quality standards are not met?..... [Y/N]*

g. *What key performance indicators (KPIs) does the body or agency use for monitoring performance, and does it publish or otherwise disclose these?*

KPIs and other data	Internal management	Published or otherwise reported
[Set out each KPI or other data used to monitor development and performance of the ID system]	[Y/N]	[Y/N]

h. *Is the monitoring process dynamic, i.e., is there a quality improvement capability (plan/do/check/act) or equivalent to improve quality over time? ..... [Y/N]*

i. *Are the KPIs themselves reviewed and updated regularly? ..... [Y/N]*

j. *Is performance monitoring required by law, regulation or policy? ..... [Y/N]*

k. *If so, cite and quote/summarize:*_____

Background

Effective management of an ID system depends on monitoring its performance. The success of an ID system depends on the degree to which it is technically robust, operating with integrity, including enrolling and authenticating correctly.

Measuring performance may enable policy makers to compare a system's use of different methods of identification, to compare with other countries' performance, to monitor a system's improvements over time, and to evaluate and manage trade-offs within the system itself. Dynamic monitoring of KPIs and allowing KPIs to evolve would tend to improve the system if the right oversight and incentives are present.

B. Validation and de-duplication

63. *Validation:*

a. *Is the data captured from individuals validated at the time of initial registration? ..... [Y/N]*

b. *Is the data validated or updated after initial registration? ..... [Y/N]*

c. *What procedures are used to validate data?*

Validation Procedures	Initial registration	Subsequently (specify when)

[212] *Ibid*, at 10.

Comparison with feeder documents (e.g., birth certificate, electoral card)	[Y/N]	[Y/N]
Door-to-door house survey	[Y/N]	[Y/N]
Attestation by public official or administrator	[Y/N]	[Y/N]
Attestation by private introducer or community member	[Y/N]	[Y/N]
Attestation by parent	[Y/N]	[Y/N]
Other (describe): _____		

d. *Is validation required by law, regulation or policy? ..... [Y/N]*

e. *If so, cite and quote/summarize:*_____

Background

Once identity data is captured, it may be validated by means of a variety of technological and administrative procedures. These may confirm the accuracy of the personal data collected, establish that the person exists and is alive, and link the data relating to the person in question with other existing records or databases.

Validation ensures that the assignment of the collection of attributes to an individual is accurate. While biometrics on their own can be used for de-duplication, i.e., to ensure that each individual is registered only once (see Question 64), additional procedures are needed to confirm that the personal data (name, birthdate, etc.) assigned to the individual registered in the ID system are correct.[213]

Common techniques for validation include confirming the authenticity of a birth notification form presented by the parents and/or examining the ID credentials and other documentation provided by the parents. Initial validation normally takes place after registration or data collection but before an ID credential is issued. It can be followed by additional validation procedures at different stages, such as periodic de-duplication exercises.

Example

Validation processes may take place at both central and local levels. In Tanzania, a list of individuals is posted together with photos in the relevant community, to allow members of the public to assist with correcting inaccurate information. ID applications are also vetted by "village and district security committees," which include representatives of various agencies, including the immigration department, police and local government. This validation process sometimes entails interviewing the applicant or requesting additional supporting information.[214]

64. ***De-duplication:*** *Is there a process of de-duplication? ..... [Y/N]*

a. *If so, is it recurrent? ..... [Y/N]*

b. *If recurrent, how often?* _____

c. *Is de-duplication required by law, regulation or policy? ..... [Y/N]*

d. *If so, cite and quote/summarize:* _____

Background

In the context of identification systems, deduplication is a technique to detect and eliminate duplicate identity records. Biometric data—including facial photographs, fingerprints and iris scans—are commonly used to de-duplicate identities in order to identify false or inconsistent identity claims and to establish uniqueness.[215]

The process involves reviewing ID registrations to ensure that no individual is registered more than once. It ensures that each ID is tied to a unique individual by identifying duplicated individuals and removing such duplicates from the system.

[213] World Bank Group, *Guidelines for ID4D Diagnostics*, 2018 at 16.

[214] World Bank Group, *The State of Identification Systems in Africa: A Synthesis of Country Assessments*, 2017 at 41.

[215] ID4D Glossary, World Bank, available upon request.

De-duplication should not be confused with identify validation (see Question 63). De-duplication ensures the uniqueness of each identity in the system but does not ensure a correct match between an ID record and a particular individual. Validation, in contrast, links records in a database to the appropriate living person.[216]

Young or rudimentary ID systems may have a de-duplication process which is based on cross-checking demographic or biographical data. However, biometric de-duplication is becoming increasingly common, using techniques such as fingerprints, iris scans, or facial recognition. The most robust and advanced ID systems utilize a combination of techniques, including multiple types of biometric data ("multimodal biometrics").[217] If a single mass de-duplication exercise would strain the processing capacity of electronic matching systems, de-duplication can also take place on a rolling basis as new registrations are processed.

65. *Levels of assurance:*

a. *Does the system provide one or more defined levels of assurance (LoA)?..... [Y/N]*

If so, describe the features of the level(s) of assurance and any difference depending on use.

Level of assurance	Features of the LoA	Uses

b. *Are levels of assurance specified in any law, regulation or policy? ..... [Y/N]*

If so, cite and quote/summarize: _____

Background

Level of (identity) assurance (LOA) is the ability to determine, with some level of certainty or assurance, that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity.

Different levels of assurance that the digital identity claimed by an individual is correct may be provided depending on the type of services and transactions for which an ID system is used.[218] The degree of confidence in the invoked identity indicates the level according to technical specifications, standards and procedures used to decrease or prevent alteration or misuse of the identity. The risk of failure or breach and the sensitivity of the service being accessed will influence the level of assurance required. For example, changing an address may rely on a lower level of assurance than changing a password. Financial and health services often require a higher level of assurance than others due to the sensitivity of the data that is collected and maintained in those systems.

Levels of assurance may be indicated by reference to international standards, such as ISO/IEC 29115, for example. The EU has established a common set of levels of assurance to apply to enrolment, ID scheme management and authentication.[219] In the US, the National Institute of Standards and Technology (NIST) published Digital Identity Guidelines[220] in 2017 that, among other things, set out:

- Identity assurance level (IAL): The robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing errors.
- Authenticator assurance level (AAL): The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication errors (i.e., a false claimant using a credential that is not rightfully theirs).
- Federated assurance level (FAL): The robustness of the assertion protocol the federation uses to communicate authentication and attribute information (if applicable) to a [replying party].

---

[216] Alan Gelb and Julia Clark, "Identification for Development: The Biometrics Revolution," CGD Working Paper 315. Washington, DC: Center for Global Development, 2013; "Identity in a Digital Age: Infrastructure For Inclusive Development", USAID [2017] at 9.

[217] See, e.g., *Identity for Development in Asia and the Pacific*, Asian Development Bank, 2016, at 20, 39. See also Identification for Development (ID4D) initiative, *Technical Standards for Digital Identity (Draft for Discussion)*, International Bank for Reconstruction and Development/The World Bank, 2017, Part 4.

[218] The required level of assurance is assessed by each organization in light of factors such as inconvenience, risk of financial loss or liability, harm to the entity's programmes or public interest, unauthorized release of sensitive information, personal safety, and civil or criminal violations.

[219] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

[220] NIST https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

Levels of assurance can be important for purposes of mutual recognition of systems, including across borders, where a system must meet a particular level of assurance in order to qualify for recognition for a given purpose. High levels of assurance can be achieved by using multi-factor verification, including through digital technologies. For example, mobile phones can be used to authenticate identity by generating and receiving one-time log-in passwords, storing credentials on the device's secure element for purposes of logging in. They can be used also for signing and encrypting documents, or using near field communications (NFC) to store and use credentials.[221]

C. Identifiers and credentials

66. ***Unique ID numbers and alphanumeric codes:*** *Does the ID system issue a unique number (or other alphanumeric code) for each registered individual?..... [Y/N]*

c. *If so,*

a. *Is that number assigned at birth? ..... [Y/N]*

b. *If not assigned at birth, when is it assigned?* _____

c. *Is that number visible on a physical credential? ..... [Y/N]*

d. *Is the number random (i.e., not based on a pattern which could be linked to personal data)?..... [Y/N]*

e. *If the number could be linked to personal data,*

f. *i. What personal data does the number encode (e.g. gender, date of birth, citizenship status, place of residence, etc.) and which of these can be revealed from the number?*

_____

g. *ii. Could the personal data be readily devised from the pattern? ..... [Y/N]*

h. *Is the nature of the number specified by law, regulation or policy? ..... [Y/N]*

i. *If so, cite and quote/summarize:*_____

Background

A unique ID number (UIN), in the context of identification systems, is a number that uniquely identifies a person—i.e., each person only has one UIN and no two people share the same UIN—for their lifetime. UINs are typically assigned after validating a person's identity and statistical uniqueness through a process such as biometric deduplication.[222] As of 2016, approximately 70 countries assigned a UIN, with lengths varying from 5 digits (San Marino) to 18 digits (People's Republic of China and Mexico).[223] There are no specific international standards that regulate or include recommendations for assignment of UINs.[224] When UINs are assigned, they can be generated randomly or code information about the individual or the location where the UIN was issued.

An ID number which reveals personal traits may lead to discrimination, profiling, and social exclusion. It could even enable service providers to set different prices for their services, or to restrict their availability, on the basis of certain digits in a person's identification number. Coded numbers based on personal data also make fraud easier in some cases as they are more vulnerable to being guessed or profiled. Even apparently innocuous data can lead to indirect disclosure of personal data that could be used for discrimination. For example, a number indicating the region where the individual lives or was born may be used to infer ethnicity or religion if such ethnicity or religion is predominant in that region.

In addition, coded numbers can also be counterproductive to the goal of maintaining a single ID number throughout a person's lifetime. For example, a number that encodes citizenship will need to be changed if citizenship status changes, a number that encodes place of residence will need updating if a person moves, and a number that encodes gender would need updating in the case of a gender reassignment (see Question 60). In some cases, a unique number for each individual (such as a social security number) serves either as its own credential or is associated with a physical or digital credential. If constructed in a way which encodes certain personal data, this can raise privacy issues.

The processing of ID numbers may also raise data security and privacy concerns, as a number may be used to identity an individual and may be used to access and aggregate multiple sources of data about that person.

[221] See Smart Card Alliance, Mobile Devices and Identity Applications (2012).

[222] ID4D Glossary, World Bank, available upon request.

[223] World Bank Group, *ID4D, Integrating Unique Identification Numbers in Civil Registration*, 2016 at 9.

[224] *Ibid*, at 13.

Examples

In **South Africa**, the first six digits of a person's 13-digit identification number are based on the year, month and date of birth. The next four digits differentiate men from women (females are assigned numbers between 0000-4999 and males between 5000-9999), and the next digit shows whether the person in question is a South African citizen (with 0 indicating a citizen and 1 indicating a permanent resident). Until the late 1980s, the twelfth digit was used to indicate a person's race, but all references to race have now been eliminated. The last digit is a "checksum digit", meaning that it is calculated by means of a formula to confirm that the other digits in the number sequence are valid.[225]

Patterned numbers may also be more vulnerable to being un-encrypted, which can compromise a host of data which is linked to such numbers. For example, **South Korea** uses a 13-digit Resident Registration Number (RRN) based on birth date, gender, and place of birth. Encrypted RRNs are associated with patient prescription and medical data, but a group of researchers showed that this encryption can be penetrated. Such concerns prompted calls for a redesign of the national identifier. [226]

In the **EU**, the GDPR allows Member States to provide exemptions or specific rules in relation to processing national identification numbers[227] and also in relation to processing for statistical purposes.[228] However, to the extent that individuals can be identified, this processing must still be subject to appropriate safeguards under the GDPR to ensure the rights and freedoms of the individuals involved.

67. ***Form of the credential:*** *Is a credential issued?..... [Y/N]*

j. *If a credential is issued:*

a. *Does it include a physical ID?..... [Y/N]*

b. *If so, describe the credential (paper, plastic or polycarbonate card with no chip, plastic or polycarbonate smart card with a chip, hybrid card, registered SIM card, smartphone app, other):*

_____

Background

A credential is a document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include—but are not limited to—ID cards, certificates, numbers, passwords, or SIM cards. A biometric identifier can also be used as a credential once it has been registered with the identity provider. [229]

Credentials traditionally take the form of physical credentials, such as paper, but new technologies have led to innovation and diversification. Today, physical ID credentials may take the form of an ID card made of material such as paper, plastic or polycarbonate (with or without a magnetic strip, a one-dimensional or two-dimensional barcode or a microchip making it a "smart card") or SIM card used in a mobile communication device such as a smartphone. Some ID credentials are purely digital, such as an app for a smartphone or other mobile communication device. The nature of a physical or digital credential will be relevant when considering what data is stored on or accessible from the credential and how to safeguard the security of that data.

Some ID credentials may contain a one-dimensional barcode, which is an optical machine-readable representation of data:

Some ID credentials may contain a two-dimensional barcode, which can store a larger amount of data:

[225] See, e.g., "What your South African ID number reveals about you", 28 August 2016, *My Broadband* online news; "Decoding your South African ID number", 7 October 2016, Western Cape Government website; "Identity by numbers", undated, Sunday Times Heritage Project website. "

[226] Latanya Sweeney and Ji Su Yoo, "De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data", *Technology Science,* 29 September 2015; "Identifying problems with national identifiers: Supposedly encrypted numbers can be easily decrypted", 29 September 2015; Mark Buell, "Post Equifax, We Need to Reconsider How to Identify People", 26 September 2017, Internet Society website; "South Korean ID system to be rebuilt from scratch", 14 October 2014, *BBC News* website.

[227] 2016 EU General Data Protection Regulation, Article 87.

[228] *Ibid*, Article 89.

[229] ID4D Glossary, World Bank, available upon request.

Examples

Some ID systems work **without a physical credential**, such as systems where authentication occurs by means of online matching of biometrics or a unique ID number to a central database. The Aadhaar system in **India** is an example of this type of system. The Unique Identification Authority of India issues a 12-digit unique identity number to any resident of India for the purpose of verifying identity on the basis of basic demographic and biometric data. This system allows a person's identity to be authenticated online, without the need for a physical credential. To do so, the individual's Aadhaar number and biometric data are submitted to the Central Identities Data Repository (CIDR), where these are authenticated against the data stored in the central registry. The CIDR then responds with a simple "Yes" or "No" answer. Registered passwords (Personal Identification Numbers, or PINs) or single-use passwords are used in some contexts to strengthen authentication of identity. [230]

ID credentials may take **multiple forms** within a single country. For example, in **Austria**, the national ID can take the form of a physical "citizen card" (*Bürgerkarte*) or a card-less mobile phone ID (*Handy-Signatur*). The government notes that both perform the same function of proof of identity and signature.[231] In **Estonia**, persons with a physical ID card can apply for a supplementary "Digi-ID", which is a "smart card" that can be used for authenticating the holder and providing digital signatures in electronic environments.[232] They can also apply for a supplementary "Mobiil-ID", a digital identity added to the holder's mobile phone to facilitate the use of various e-services.[233] Yet another optional extra is the "Smart-ID", an electronic application which can facilitate verified access to e-services from any of the user's electronic devices.[234]

c. *Does any law, regulation or policy specify the data to be displayed on or accessible from the credential? ..... [Y/N]*

d. *If so, cite and quote/summarize:*_____

e. *Is the data displayed on or accessible from a credential required to be proportional to or limited to the minimum necessary (or a similar standard) to fulfil a specified purpose? ..... [Y/N]*

Background

Some types of data may be accessible from a physical ID credential. While the accessibility of such data may have legitimate purposes and increase efficiency, it can also increase the risk that data is shared unintentionally or with persons who have a legitimate interest in only some of the data visible on the credential. Credentials which reveal personal data may increase the risks of discrimination, profiling and social exclusion.

Examples

Namibia provides physical ID cards of one color to citizens and another color to permanent residents—meaning that persons without any legitimate interest in this attribute can be informed of it automatically and even from a distance.[235]

In Cameroon, ID cards introduced by a 2016 decree list "profession/occupation" on the face of the card.[236] This is an attribute which is likely to change over time for many individuals, and arguably unnecessary information for identification purposes – either on the ID credential or in the associated database.

India is in the process of rolling out a scheme to provide special color-coded identity cards to persons with disabilities, for the purpose of easy linkage to government schemes and services. The Ministry of Social Justice and Empowerment will launch a centralized database of disabled persons and issue Unique Disability Identity (UDID) cards. These cards will have a colored bar on one end to indicate the degree of disability, with a red bar indicating a disability of 80% or more, a blue bar indicating a disability of between 40% and 80%, and a yellow bar for a disability below 40%.[237] There will two categories of UDID cards: lifetime cards for persons with permanent disabilities, and cards with specific validity periods for persons

---

[230] "Aadhaar Technology & Architecture: Principles, Design, Best Practices, & Key Lessons," UIDAI, March 2014.

[231] "What's the Main Difference Between Mobile Phone Signature and Citizen Card?", Digitales Österreich website; Daniel Castro, *Explaining International Leadership: Electronic Identification Systems*, The Information Technology & Innovation Foundation, 2011.

[232] "What is Digi-ID?", Estonia ID website.

[233] *Ibid*.

[234] Link from "Smart-ID", Estonia ID website to Smart-ID website; "The electronic vote: a reality which no longer surprises anyone in the country (2016 update)", Gemalto (digital security company) website; Kalev Leetaru, "Estonia's ID Card and the March of Cryptography", 11 September 2017, *Forbes* online; Republic of Estonia Information System Authority, "Possible Security Vulnerability Detected in the Estonian ID-card Chip", 5 September 2017, Riigi Infosüssteemi Amnet website.

[235] Identification Regulations, Government Notice 96 of 2001 (GG 2533), issued in terms of the Identification Act 21 of 1996. Regulation 3 specifies that an identity card issued to a Namibian citizen will be blue while that issued to a permanent resident will be pink.

[236] Medjom Colby, "Cameroon introduces new ID cards", 29 August 2016, Youth Blog supported by the Commonwealth Youth Programme; Mark Bareta, "Cameroon: Microchip In All ID Cards Soon", *Bareta News*, 5 August 2016. Each new ID also has a SIM card allocated to it. CRTV, "Biya signs decree changing format of most identification documents in Cameroon", *Cameroon Concord News*, 9 August 2016.

[237] "Disabled People in India to get Unique ID Cards", 16 June 2015; "Color-coded Unique Disabled Identity cards for disabled soon", *The Times of India*, 22 May 2016.

with temporary disabilities.[238] This system is intended to encourage transparency, efficiency and ease of delivering government benefits, as well as to provide a mechanism for eliminating fake disability certificates or malpractices in the delivery of benefits to persons with disabilities.[239]

68. *Period of validity:*

a. *Indicate in the table below how often the ID credential must be renewed or replaced, if applicable specifying different periods for any specific groups of ID holders (e.g. children, the elderly, non-citizens)?*

Group	Period of validity (years)

b. *Is the period of validity set by law, regulation or policy? ..... [Y/N]*

c. *If so, cite and quote/summarize:*_____

Use, storage and protection of personal data

A. Use and retention of personal data

69. *Purpose limitation on collection and use of personal data:*

a. *Does any law, regulation or policy specific to the ID system limit the system's collection and use of data to a stated purpose? ..... [Y/N]*

b. *If so, specify, including whether it is required to be proportionate to or minimum necessary for that purpose:*

_____

c. *Does the ID system employ physical, technical or administrative safeguards to monitor or ensure the ID system's compliance with any purpose limitations? ..... [Y/N]*

d. *If so, describe these:* _____

70. ***Records of usage of personal data:*** *Does the ID system maintain records of how individual personal data has been used, shared or otherwise processed? ..... [Y/N]*

e. *If so:*

a. *Indicate which data is recorded and the uses.*

Data use/sharing/processing	Recorded?	Describe uses
Individual(s) whose data was used/shared/processed	Y/N	
Purpose of the use/sharing/processing	Y/N	
Description of the type of data used/shared/processed	Y/N	
Identification of type of recipients of any data	Y/N	
Identification of specific recipients of any data	Y/N	
Identification of who asked for authentication, when, where, etc.	Y/N	
Identification of size of transaction (e.g., value in currency)	Y/N	

[238] Ananya Sengupta, "Center lines up smart IDs for disabled", *The Telegraph* (Calcutta).

[239] "Database for the disabled", *The Telegraph* (Calcutta), 29 April 2015; Taru Bhatia, "A number that can make life easier for differently abled", 22 January 2016, Governance Now; Nidhi Sharma, "Color-coded cards to be launched for 2.7 crore disabled", *The Economic Times*, updated 11 December 2016. The government report "Detailed Project Report: National Disability Database & Unique Disability ID creation", authored by the Department of Disability Affairs, can be viewed in draft form online, but not downloaded. (It can also be viewed at this alternate site.)

Requested assurance level (which may indicate the data subject was doing something of high value)	Y/N	
Identification of country in which data may reside as a result of a cross-border transfer	Y/N	
Other (list):		

b. *Are data trails anonymized? ..... [Y/N]*

c. *If so, is the anonymization effective (i.e., can they be de-anonymized)? ..... [Y/N]*

d. *Is the ID system required by any law, regulation or policy to maintain records of how individual personal data has been used, shared or otherwise processed?..... [Y/N]*

e. *If so, indicate the law, regulation or policy:* _____

Background

One of the benefits of an ID system is the ability to use it to establish identity for multiple purposes such as financial transactions, health care, and the use of public transportation, although this may also create a "single point of failure" risk. In the case of some digital ID systems, every time an ID credential is used by an individual it can generate usage and transaction data that can be collected and stored.

Purpose-limitations on use of personal data are addressed in connection with both collection and use in Question 69. Here, Question 70 concerns records of the use made of the personal data. Such "data trails" (or "breadcrumbs", "footprints" or "exhaust") can be stored in databases and be combined with other data trails like web-browsing records. Government institutions or commercial enterprises can use them to construct a detailed personal profile of an individual and their behavior (e.g., movements, activities and preferences).[240] Data relating to such a "digital persona" could be used for commercial opportunities, surveillance or social control.[241]

While there may be debates about the appropriateness of the aforementioned uses, data trails may also be useful in detecting fraudulent activity, as they can alert the ID system when there is atypical activity. They may also provide important data needed to monitor usage and study trends. This can help in identifying new features that are needed and in streamlining design. To mitigate the risks to individual privacy, data trails can be anonymized when stored in a database to permit analysis of the data without linking it to a specific identity. The result of successful anonymization is that certain data protection legislation may be unlikely to apply (for example, the EU's GDPR does not apply to anonymized data, as an individual cannot be identified from such data).

71. ***Period of data retention:*** *Is personal data held by the ID system destroyed or erased after the purpose for which it was collected is completed?..... [Y/N]*

f. *If so,*

a. *What time period elapses before this takes place?* _____

b. *If data is stored on an ID credential, how is that data destroyed or erased?*

_____

c. *Is the period of retention set by law, regulation or policy? ..... [Y/N]*

If so, cite and quote/summarize:_____

B. Interoperability, federated systems and other data sharing

72. ***Interoperability:*** *Is the ID system interoperable or otherwise linked with:*

a. *Other government databases within the country? ..... [Y/N]*

b. *If so, explain:* _____

c. *Private sector or other non-governmental databases within the country?..... [Y/N]*

d. *If so, explain:* _____

[240] For a broad look at data trails generated in other contexts, and their connections with "big data", see Joseph Jerome, "Big Data: Catalyst For A Privacy Conversation", 48 *Indiana Law Review* 213 (2014).

[241] Alea Fairchild & Bruno de Vuyst, "The Evolution of the e-ID card in Belgium: Data Privacy and Multi-Application Usage", ICDS 2012: The Sixth International Conference on Digital Society, 2012 at Part 15.

e. *Government databases outside the country? ..... [Y/N]*

f. *If so, explain: _____*

g. *Private sector or other non-governmental databases outside the country? ..... [Y/N]*

h. *If so, explain: _____*

i. *Are the ID system's application programming interfaces (APIs) generally available to third party organizations enabling them to create new, connected services? ..... [Y/N]*

j. *If so, explain: _____*

k. *If databases are integrated, are there any significant technological or administrative controls on what data can be read by others? ..... [Y/N]*

If so, explain: _____

l. *Are the interoperability or integration of databases and applicable controls addressed by any law, regulation or policy? ..... [Y/N]*

If so, cite and quote/summarize:_____

Background

Interoperability is the ability of databases, devices, or systems to talk with each other, exchanging data or queries. In some cases, interoperable databases or systems may be directly connected, allowing for the real-time exchange or updating of data; in others, databases or systems may be interoperable via a trusted third-party exchange layer that facilitates communication across disparate systems.[242]

In practice, interoperability can mean many things. It could mean that an ID system "pulls" data from another ID system or civil registration system. It could also mean that a functional database "connects" to a foundational database to authenticate an individual (but with no transmission of data) or that the databases share data about the same individual (see Question 74). A common objective is to ensure that interoperability (e.g., between national ID and civil registration systems, or between entities seeking authentication and the ID system) occurs "in a timely and low-cost manner, subject to appropriate privacy and security safeguards".[243]

Interoperability across public programs can increase efficiency by eliminating unnecessary duplication of effort – for example, by eliminating "ghost workers" or rationalizing social benefit program and other public transfers. The ability to match individuals across databases can increase efficiencies in such processes, but may also increase the challenges of data protection. However, interoperability also increases risks to privacy and data security when data is stored or accessible in multiple systems. To mitigate these risks, some systems limit data sharing to the absolute minimum necessary.[244]

In the case of a **civil registration system**, the system may be the backbone of a foundational ID system and if they are separate, the civil registration and ID systems can be aligned by linking the two. Civil registration and ID systems may even be combined under a single legal framework.

Examples of possible types of linkages between the two systems include:

- A person's record in the ID system is created at the time of their birth registration.
- A unique identification number issued at the time of birth registration is the same number used to identify the individual in the ID system.
- The systems are linked in respect of updates, so that an identity in the ID system is de-activated when a death is recorded.
- Results of de-duplication are shared between systems.[245]

Personal data collected for civil registration and ID systems may overlap, even where there are separate systems. Thus, the same privacy and security issues are relevant to both.

---

[242] ID4D Glossary, World Bank, available upon request.

[243] *Principles on Identification for Sustainable Development: Toward the Digital Age*, facilitated by World Bank Group and Center for Global Development, February 2017 at 12.

[244] See, e.g., Alan Gelb & Julia Clark, "Identification for Development: The Biometrics Revolution", CGD Working Paper 315. Washington, DC: Center for Global Development, 2013, *Identification Systems for Social Protection*, 2016, Guidance Note at 6-7. .

[245] See *Integration of Civil Registration and Vital Statistics and Identity Management Systems: Botswana Success Story*, World Bank Group, September 2015.

In some countries, national ID systems are born out of a **voter ID system**. A voter ID card or some other voter ID credential used to verify eligibility to vote at polls on election day may be utilized more generally for purposes of identification in other situations. This voter ID system may even evolve into a *de facto* national ID system. However, as voting is generally limited to citizens, such a system likely excludes non-citizen residents.

In addition, there may be linkages between separate voter ID and other ID systems. For example, individuals may be required to provide proof of identity using another ID credential when registering to receive a voter ID card. If the other ID system is not sufficiently inclusive, this may result in unintentional disenfranchisement. Worse yet, the other ID system may be manipulated politically to impose barriers that exclude certain groups from the electoral process.

73. *Federated identity management:*

a. *Does the ID system rely upon a common set of policies, practices and protocols to manage a common identity system across several organizations? ..... [Y/N]*

b. *.....If so, describe these, including how they establish the responsibilities of participants in the ID system:*

_____

c. *To what degree and how does the ID system integrate public and private ID systems or provide for mutual recognition?*

_____

Background

Governments may tend to prefer to manage enrolment, credentials and authentication themselves for IDs used to access government services. However, governments might also rely on other firms in order to reduce costs and risks, and better manage procedures. For instance, carefully selected third parties like banks, post offices, telecommunications operators and others might be relied upon to provide identification, as in the UK's UK.VERIFY system.

Thus, service providers may rely on "federated identity," where identification is carried out by a third party, permitting secure exchange of credentials between organizations using policies, practices and protocols that comprise a common identity system. The "portability" of the ID data across different systems and service providers that results may allow the individual to use the same credential and authenticator with several service providers. This may rely upon an open standard solution that offers interoperability among service providers.[246]

Countries with centralized government or an existing non-digital national identity system may be more likely to adopt centralized digital identity registration. More decentralized political structures (e.g., where a country's regional governments have substantial powers) may be more amenable to decentralized identity systems. These might rely on federation agreements to permit a single sign-on.[247]

Federated identity systems require establishing in laws and contracts the various legal responsibilities of identity providers to service providers that rely on the correctness of the identity established, data about the person, and the credentials used.

Examples

In the UK, GOV.UK Verify allows certified companies to act as "identity providers." These follow prescribed procedures and standards set with specified levels of assurance in order to verify an individual's identity for purposes of accessing government services.248 They do not involve issuance of an ID card or establishment of a central identity register.

In Canada, the SecureKey Concierge system enables individuals to use existing banking credentials with enrolled financial institutions to access online government services online.249

[246] For example, the GSMA Mobile Connect is based on an open standard solution that uses the OpenID Connect protocol. It offers broad interoperability between mobile operators and service providers, including government services). See http://www.gsma.com/personaldata/mobile-connect.

[247] See OECD (2011), "National Strategies and Policies for Digital Identity Management in OECD Countries", OECD Digital Economy Papers, No. 177, OECD Publishing. Available at http://dx.doi.org/10.1787/5kgdzvn5rfs2-en

[248] Companies such as Verizon, Experion, Barclays, the Post Office, the Royal Mail and others have become certified identity providers. See https://identityassurance.blog.gov.uk/tag/certified-companies/.

[249] See http://www.skconcierge.us/the-canadian-experience/.

74. *Data sharing:*

a. *In the tables below, indicate any agencies or institutions with which personal data collected for purposes of the ID system is shared, how it is shared (e.g., integrated access to electronic database through APIs, response to request, etc.), and safeguards that apply.*

Data sharing with *government* agencies and institutions			
Type of data shared	Agency with which data is shared	Method by which data is shared	Safeguards

Data sharing with *non-government* and institutions			
Type of data shared	Agency with which data is shared	Method by which data is shared	Safeguards

b. *Are requirements for data sharing and safeguards provided for in any law, regulation or policy? (See also Question* ***Error! Reference source not found.****.)..... [Y/N]*

c. *If so, cite and quote/summarize:*_____

C. Data system security

75. ***Storage of data:*** *Is personal data digitally stored by the ID system?..... [Y/N]*

a. *If not, describe how it is stored (e.g., paper records):* _____

b. *If stored digitally, indicate with a tick in the table below how each type of data is stored and whether encrypted.*

Personal data	Central database	Multiple databases	On physical credential	Other (*specify*)	Encrypted
When initially collected during registration					
Used for authentication					
Used for authorization					
Data trails					
Other (specify):					

c. *Describe any encryption used if indicated in the table above:*

_____

d. *Is the storage of the data addressed by law, regulation or policy? ..... [Y/N]*

e. *If so, cite and quote/summarize:* _____

Background

The format of the database will affect the functionality and financial sustainability of the ID system. For example, paper-based storage of identity data is expensive, inefficient and precludes the offering of electronic identification services.

The format of the database will also inform the identification of security risks, appropriate safeguards to mitigate the risks, and the ability to recover data. Centralized storage of any digital data, including biometric data, in a central database makes it more vulnerable to hacking. While the use of encryption mitigates some risks, it does not provide an absolute guarantee of safety. With unauthorized access to an improperly secured database, a bad actor could alter biometrics so that the fingerprints, iris scan or other biometrics of the actual person no longer matched that person's file—making it difficult for them to confirm their identity. Unlike other data which can easily be replaced (such as passwords), once biometric data is compromised, it is nearly impossible to rectify.

Another risk of using a central database to store personal data is that it may tempt officials to seek improper access to the database to identify an unknown person whose personal data, such as biometrics, have been collected. This intensifies the danger of "function creep," or the gradual widening of the purposes for which the data will be used (see Questions 72 and 74).

In some systems, personal data is stored only on a physical credential. For example, a reader is required to confirm that the biometrics of the person presenting the token match the biometrics stored on that token. This approach may limit the impact of compromise or unauthorized disclosure to only one individual (but also faces challenges in keeping data updated and costs of issuing replacement tokens).

76. *Security and breach of databases:*

f. *If personal data is digitally stored in a database(s) (see Question 75),*

a. *Is the database(s) in the country? ..... [Y/N]*

b. *Does it use the databases of a third-party cloud-based provider? ..... [Y/N]*

c. *If so, provide details: _____*

d. *Are there effective physical, technical and administrative controls in place to protect the confidentiality, integrity, and availability of stored data? ..... [Y/N]*

e. *Provide details: _____*

f. *If different types of personal data are stored in different ways, describe the differences:*

_____

g. *Is data transfer encrypted?..... [Y/N]*

h. *Is the security of the data governed by law, regulation or policy? ..... [Y/N]*

i. *If so, cite and quote/summarize:_____*

77. ***Security features in use of ID credentials:*** *If the ID system uses physical ID credentials, does the system employ effective mechanisms to prevent unauthorized use of credentials? ..... [Y/N]*

a. *Describe the key security features of the physical credential:*

_____

b. *Is there a secondary means of identification (such as a photograph on the ID or a password supplied by the holder of the ID)? ..... [Y/N]*

If so, specify: _____

c. *If data is stored on a credential, is access to the data controlled by the ID holder? (such as a requirement that the holder consent by entering a PIN)..... [Y/N]*

If so, specify: _____

d. *Are there any other security features which apply to any third party who is attempting to access data from the credential (e.g., limits on what data can be extracted, required authentication of the service provider, etc.)? .....[Y/N]*

If so, specify: _____

e. *Are the security features required by any law, regulation or policy specific to the ID system? ..... [Y/N]*

f. *If so, cite and quote/summarize:*_____

Background

Some systems apply different access-control restrictions for various types of data stored on a credential. For example, it is possible to engineer an ID system to allow basic data to be read from the credential without additional steps, while other data can only be accessed after entry of a PIN by the ID holder.

ID credentials can make use of various extra security features. One possibility is to pair the credential with the biometrics of the individual presenting it. It is also possible to encrypt the data so that communication with a card reader or a terminal can take place only if the ID holder enters a personal code which essentially unlocks the credential, like the PIN codes used in combination with some credit or debit cards.

It is possible to employ security measures on the other side of the transaction as well and such security measured can be built into the technology used to read ID cards. For example, it is possible to restrict access to specific categories of personal data, such as biometric data, to service providers that have specific government authorization for this purpose. It is also possible to restrict card readers so that they can access only the relevant attributes to be identified in a particular context.

For example, if the only relevant attribute is knowing whether the card-holder has attained a certain age (such voting age, drinking age or age of majority), the card reader can be programmed to receive only a yes or no answer to this question.[250] Similarly, if traffic police need to know if a driver possesses a valid driving license, they could use a card reader which reveals only this data—and not the status of the driver's residence in the country, for instance. Where the only data needed is authentication of the card-holder's identity, the card reader can reveal only a "yes" or "no" answer to the question of whether the person presenting an ID card is the person represented by that card, without revealing any other data. Such efforts to minimize the amount of personal data processed will also assist in ensuring that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (known as the "data minimization" principle under the EU's GDPR).

Moreover, authentication capacity can be limited to licensed service providers. Card readers or terminals can be configured to grant access to data only after the transmission of a verification code which proves authenticity.

Example

In **Germany**, before an individual transmits information from his or her e-ID card, the service provider must first transmit a valid authorization certificate with information about the service provider. This "double-sided, mutual authentication" both provides proof of identity for the service provider and is evidence that the service provider has met data privacy and security requirements set out by the government which, for example, prohibit using the data for illegitimate business purposes.[251]

78. ***Degrees of security protection:*** *Indicate in the table below any heightened degrees of data confidentiality and security for different types of data.*

Type of data	Heightened degree of confidentiality (as compared to other personal data)?	Heightened security measures (as compared to other personal data)?
Biometrics in general		
Specific biometrics *(list)*:		
Other sensitive personal data *(list)*:		

79. ***Security of biometric data:*** *Are there technical or administrative safeguards to prevent actual biometric data about an individual (as opposed to the results of a sanctioned authentication) from being shared with any other person or entity?*..... *[Y/N]*

If so, describe. _____

80. *Privacy-enhancing technologies (PETs):*

a. *Does the ID system use PETs?* ..... *[Y/N]*

If so, describe any PETs currently in use by the ID system:

_____

[250] Daniel Castro, *Explaining International Leadership: Electronic Identification Systems*, The Information Technology & Innovation Foundation, 2011.

[251] Daniel Castro, *Explaining International Leadership: Electronic Identification Systems*, The Information Technology & Innovation Foundation, 2011.

b. *Is the ID system's use of PETs required by any law, regulation or policy? ..... [Y/N]*

If so, cite and quote/summarize: (See also Question 13.) _____

D. Administrative measures to protect personal data

81. *Allocation of powers and duties:*

a. *Are the powers of administrators separated among functional or other aspects of the ID system? ..... [Y/N]*

b. *If so, describe how: _____*

c. *Are the powers of administrators limited to only those necessary to the performance of their function? ..... [Y/N]*

d. *If so, describe how: _____*

e. *Are these separations and limitations imposed by law, regulation or policy? ..... [Y/N]*

If so, cite and quote/summarize:_____

Background

The concepts of "least privilege" and "separation of duties" can mitigate the risks of human error in the handling of personal data or deliberate misuse. **Separation of duties** limits the power of any single administrator. For example, there may be separate organizations in identification, authentication, authorization, and authorization, limiting the administrative capability of one person. Under this arrangement, one person or organization would create identities, another would administer authentication, and yet others would administer the authorizations granted by the system. By separating and limiting administrative power, policy makers reduce the risk associated with a single "rogue" administrator or agency. **Least privilege** is closely related to separation of duties and is the principle that any administrator has only the powers necessary to perform his or her delegated function – and no more.

82. *Staff confidentiality:*

a. *Are there clear and sufficient confidentiality obligations and procedures for staff of the ID agency?..... [Y/N]*

b. *If so, do the obligations and procedures also extend to any subcontractors (whether private or public) and any employees and staff of subcontractors? ..... [Y/N]*

c. *Describe the available remedies for breach of confidentiality (e.g., dismissal, criminal sanction):_____*

d. *Are the confidentiality obligations, procedures and remedies set by law, regulation or policy? ..... [Y/N]*

e. *If so, cite and quote/summarize:_____*

E. Data loss, breach and misuse

83. ***Notifications:*** *Does the ID system provide for notifications to be made in the case of personal data breach, loss, theft or other misuse or any fraudulent activity? ..... [Y/N]*

If so,

a. *Specify the form of notification, and to whom and when it must be made:*

_____

b. *Are requirements for notifications for personal data breach, loss, theft or other misuse or any fraudulent activity provided for in any law, regulation or policy? ..... [Y/N]*

If so, cite and quote/summarize:_____

c. *Are the data breach notification requirements limited to digital records, or do they also cover personal data in paper records or held in other forms? ..... [Y/N]*

84. *Significant past instances:*

a. *Describe any past instances of significant data breach, loss, theft or other misuse or any fraudulent activity and the remedies applied:*

_____

b. *Describe any technical or administrative measures introduced in light of the instances described in (a) to prevent future instances:*

_____

F. Cyber threats and cybercrime

85. ***Critical infrastructure.*** *Is the ID system identified as critical infrastructure for cyber security purposes? ..... [Y/N]*

86. ***Cooperation.*** *Do the ID system administrators participate in any cyber security emergency response planning? (See also Question 17.)..... [Y/N]*

Governance

Individual rights and protections

A. Information and consent to collection and use of personal data

87. ***Legal basis for collection and use:*** *Is the collection and use of personal data by the ID system authorized by law, regulation or policy? (See also Question 6.)..... [Y/N]*

If so, cite and quote/summarize:_____

88. *Information provided to individuals about the use of personal data about them:*

a. *Are individuals who register informed of how personal data about them will be used? ..... [Y/N]*

b. *If information is only provided with respect to some of the data about them, explain which data is and is not addressed: _____*

c. *Describe the information process at the time of registration. Provide separately any written materials presented or distributed to individuals.*

_____

d. *Describe any subsequent information processes:*

_____

e. *Describe any general information campaigns to inform the public:*

_____

f. *Are individuals informed of how long personal data collected from them will be retained? ..... [Y/N]*

g. *Are individuals informed of which personal data collected will be public and which will be confidential? ..... [Y/N]*

h. *Are individuals informed of their rights with respect to personal data about them (e.g., the right to access, review, rectify or erase data about them or the right to withdraw consent)? ..... [Y/N]*

i. *If so, identify which rights: _____*

j. *What assurances, if any, are users given that personal data about them will only be used for the disclosed purposes?_____*

k. *Is the provision of information to individuals about the collection and use of personal about them data required by any law, regulation or policy? ..... [Y/N]*

l. *If so, cite and quote/summarize:_____*

89. ***Consent to collection and use of personal data:*** *(See also Question 24):*

a. *Does the registration process include obtaining consent to the collection and use of personal data? ..... [Y/N]*

b. *If so, describe the consent process: _____*

c. *If consent is obtained for only some of the data collected, explain which data is and is not the subject of consent:*

_____

d. *If consent is withheld, can registration proceed?..... [Y/N]*

e. *If so, what personal data can an individual withhold without preventing registration?*

_____

f. *Is an individual able to withdraw consent after giving it?.....[Y/N]*

g. *If so, describe the process and the actions the ID system must take upon such withdrawal:*

_____

h. *If personal data of minors is collected, how is consent treated?*

_____

i. *Is consent required to be obtained by any law, regulation or policy? ..... [Y/N]*

j. *If so, cite and quote/summarize:*_____

90. ***Information and consent regarding data sharing:*** *Is data from the ID system shared with other public or private bodies or agencies?..... [Y/N]*

If so,

a. *Is the potential for such sharing disclosed as part of the information and consent processes described in the responses to Questions 88 and 89? ..... [Y/N]*

b. *Is consent (excluding any consent process described in the responses to Question 89) required prior to any particular instance of such sharing taking place? ..... [Y/N]*

i. If so, explain the consent procedure:

_____

ii. If consent is required, can it be revoked at a later stage? [Y/N]

c. *If no consent is required, are individuals informed about data-sharing after the fact?..... ..... [Y/N]*

d. *If so, describe how such information is provided:*

_____

e. *Is the sharing of data required and/or restricted by law, regulation or policy? ..... [Y/N]*

f. *If so, cite and quote/summarize:*_____

B. Access, rectification, deletion and portability rights

91. ***Access to and review use of personal data:*** *(See also Question 25.)*

a. *Do individuals have the ability to confirm personal data about them is being processed and/or access personal data about themselves (including data trails) that has been collected? ..... [Y/N]*

b. *Describe the process for any such confirmation or access and any barriers individuals face:*

_____

c. *Describe any limitations on the types of data available or the circumstances relating to such confirmation or access:*

_____

d. *Describe the fees and any limitations on the fees or other costs that can be assessed on an individual for such confirmation or access:*

_____

e. *Are the rights, limitations and processes set by any law, regulation or policy? ..... [Y/N]*

f. *If so, cite and quote/summarize:*_____

92. ***Rectification of personal data:*** *(See also Question 26.)*

a. *Do individuals have the ability to rectify personal data about them (including data trails) that has been collected? ..... [Y/N]*

b. *Describe the process for any such rectification and any barriers individuals face:*

_____

c. *Describe any limitations on the types of data subject to or the circumstances relating to such rectification:*

_____

d. *Describe the fees and any limitations on the fees or other costs that can be assessed on an individual for such rectification:* _____

e. *Are the rights, limitations, processes and fees set by any law, regulation or policy? ..... [Y/N]*

f. *If so, cite and quote/summarize:*_____

93. ***Right to deletion of personal data:*** *(See also Question 27.)*

a. *Do individuals have the ability to have personal data about them (including data trails) deleted from the ID system? ..... [Y/N]*

b. *Describe the process for any such deletion and any barriers individuals face:*

_____

c. *Describe any limitations on the types of data subject to or the circumstances relating to such deletion:*

_____

d. *Describe the fees and any limitations on the fees or other costs that can be assessed on an individual for such deletion:* _____

e. *Are the rights, limitations, processes and fees set by any law, regulation or policy? ..... [Y/N]*

f. *If so, cite and quote/summarize:*_____

94. ***Data portability:*** *(See also Question 28.)*

a. *Do individuals have the ability to easily move, copy or transfer personal data about them easily from the ID system to another electronic environment? ..... [Y/N]*

b. *Is such data portability established in any law, regulation or policy? ..... [Y/N]*

c. *If so, cite and quote/summarize:*_____

Institutions

A. Relevant institutions and third parties

95. ***Administrative and supervisory bodies:*** *Identify the body(ies) or agency(ies) which are primarily responsible for administrative supervision of the ID system.*

_____

a. *Is the body(ies) or agency(ies) established by a law? ..... [Y/N]*

b. *If so, identify the law:*_____

c. *Describe the institutional relationship of the body(ies) or agency(ies) to the government (e.g., autonomous body reporting to Minister, Cabinet, Parliament or other government agency):*

_____

Role	Entity (note if private sector)	Supervising authority (if any)
Data capture from individuals		
Validation of identity		
De-duplication		
Registration of individuals in the ID system		
Issuance of ID credentials		

Changing or updating data (such as name changes, change of address, etc.)		
Storage of physical or electronic records and database		
Authentication services		
Cross-border transfer of data		
Protection of individual privacy rights		
Others (specify):_____		

96. ***Institutional independence:*** *For each body or agency identified in Question 95 (complete separately for each one if necessary):*

   a. *Is the body or agency effectively independent from external influence in carrying out its statutory duties, particularly from day-to-day political influence and commercial interests?..... [Y/N]*

   b. *Who appoints the authority or its members? _____*

   c. *Who has the power to remove the authority or its members? _____*

   d. *What is the term of office? _____*

   e. *Who controls its budget? _____*

97. *Roles of institutions and third parties:*

   a. *Indicate in the table any third-party entity (including any private sector entities) which implements the indicated roles and any authority responsible for supervising that entity:*

   b. *If multiple parties are involved, explain or illustrate which is doing what, if necessary using a matrix or flow chart:_____*

   c. *If any third-party entities (government or private-sector) collect, store or process personal data, how does the ID system ensure compliance with data protection and privacy obligations?_____*

98. *Administrative powers:*

   a. *Does the agency(ies) or body(ies) have powers enumerated by law to carry out its(their) functions? ..... [Y/N]*

   b. *Which agencies or bodies have legal powers relating to the ID system included in the table below:*

Powers	Empowered agencies or bodies (if any)
Require submission of data	
Cancel ID credentials	
Limit the scope of application of the ID system or a credential	
Set fees	
Levy fines	
Conduct investigations	
Resolve disputes	
[Add any other relevant powers] _____	

99. ***Inter-agency conflict:*** *If multiple government bodies or agencies are involved in either administration or implementation, has inter-agency conflict been a problem?..... [Y/N]*

   c. *If so, how? _____*

100. ***Private sector outsourcing and PPPs (public-private partnerships):*** *If any of the roles identified in Question 97 are carried out by private sector service providers:*

   a. *Is the role of private sector providers structured as a PPP? ..... [Y/N]*

b. *(PPP here refers to a legal arrangement between one or more private entities and one or more public entities regarding governance, financing and operation of a service, often organized under, for example, a concession or management agreement.)*

c. *If so, describe the structure and the participants:*

_____

d. *Are all such private sector service providers and their data systems used for the ID system located inside the country?..... [Y/N]*

If not, which are not? _____

e. *Is there an approval process for permitting private sector providers to participate in the ID system?..... [Y/N]*

*If so, describe the approval process:*_____

f. *Does the government retain ownership and control of data collected or stored by private sector providers?... [Y/N]*

Background

The private sector is often a valuable partner to government in implementing an ID system. For example, because the private sector is likely to have technical expertise and operational efficiency that government entities lack, governments may outsource some aspects of the ID system to private sector entities to reduce ongoing costs. However, any involvement of the private sector in the operations of an ID system creates the need for additional safeguards to ensure that personal data is secure and not misused. These might include: (a) a mandatory authorization process, (b) a requirement that private sector providers be located within the country, and (c) government-retained ownership and control over any data collected and stored by the private sector provider on behalf of the ID system.

Public-private partnerships (PPPs) allow government to utilize private sector investment and/or expertise to fund and operationalize an ID system. Private sector entities such as banks and health care providers are often potential partners as they are key beneficiaries of the ID systems and have an interest in their successful implementation. Such entities can be harnessed to design, construct and/or operationalize an ID system in exchange for a return on its investments, for example, through fees collected upon issuing of credentials or imposed on identity services transactions.

A wide variety of PPP models may be employed to further an ID system. Private-sector partners may be utilized for one or more discrete functions, including designing and building system infrastructure, financing initial and/or ongoing capital investment, or operating the ID system which may involve registration, validation, credential issuance or authentication services. PPPs may also be structured in a variety of forms, including as concessions or long-term service agreements. [252]

Examples

Albania: As part of an initiative to modernize its paper-based ID system, the Government of Albania granted a concession to Aleat, a joint venture of IDEMIA (formerly Morpho) and the Albanian – American Enterprise Fund in 2008 to issue 1.5 million eID cards.[253] Aleat was responsible for every aspect of the project, including technology development, operation and maintenance. The concession was extended in 2013 for an additional 10 years.[254] Aleat continues to incur all the design, building and operational costs and retains a portion of user fees relating to the IDs collected from individuals.[255]

India: India's Aadhaar ID system relies on private-sector partners to register its 1.2 billion citizens. The Unique Identification Authority of India (UIDAI) enters into MOUs with public- and private-sector entities, including state governments, banks, telecom companies and insurance agencies to serve as "Registrars." These Registrars then sub-contract local "Enrolment Agencies" to carry out the actual data capture for registration. The data is sent to the UIAI for verification and de-duplication and issues a unique Aadhaar number. Registration is free to individuals and the Government pays Enrolling Agents a fee for each individual enrolled.[256]

[252] GSMA, World Bank Group, and Secure Identity Alliance, Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, 2016 at 30.

[253] GSMA, World Bank Group, and Secure Identity Alliance, Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, 2016 at 35.

[254] Aleat website, Who we are.

[255] GSMA, World Bank Group, and Secure Identity Alliance, Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, 2016 at 35. Aleat website, Who we are. Morpho website, Press releases and News, OT-Morpho becomes IDEMIA, the global leader in trusted identities, 28 September 2017.

[256] GSMA, World Bank Group, and Secure Identity Alliance, Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, 2016 at 30 and 39.

B. Objections, complaints and remedies

101. ***Objections, complaints and remedies:*** *(See also Question 34.)*

a. *Is there a mechanism for individuals to object to the ID system's use of personal data about them? ..... [Y/N]*

b. *Is there a mechanism for individuals to file complaints or seek redress for violation of rights or protections relating to privacy and data protection? ..... [Y/N]*

c. *Describe the circumstances on which objections, complaints and redress may be based:*

_____

d. *Identify the entity or entities responsible for receiving such objections and complaints, conducting investigations and applying remedies:*

_____

e. *Describe the processes for making an objection, bringing a complaint and seeking redress, and how the entity using the data is required to respond:*

_____

f. *Are such processes used to a significant extent in practice? ..... [Y/N]*

g. *If not, describe any significant barriers individuals face:*

_____

h. *Describe the remedies available to individuals for violation of any rights or protections:*

_____

i. *Are the rights and processes for objections, complaints and redress set in any law, regulation or policy? ..... [Y/N]*

j. *If so, cite and quote/summarize:*_____

C. Financial sustainability

102. *Funding of the ID system:*

a. *Is the ID system expected to be adequately funded to cover its costs? ..... [Y/N]*

b. *If not, why not?* _____

c. *Have there been persistent budget shortfalls? ..... [Y/N]*

d. *If so, what reasons have been given?*_____

e. *What sources of revenues does the ID system rely on to cover its costs?*

Substantial source of funding	
Fees	Y/N
Public funds	Y/N
Penalties	Y/N
International aid	Y/N
Private investment	Y/N
Other (specify): _____	Y/N

f. *What are the estimated costs per person for registration of an individual in the ID system and issue of an ID credential (if ID credential are used)?*

_____

g. *How are costs distributed? E.g., are there low cost and high cost regions? Are subsidies necessary to keep part of the system going, with part operating at the expense of another?*

h. _____

Background

Sustainability is a key principle of ID systems. They must be designed to achieve long-term financial and operational stability, without compromising the goal of universal coverage and accessibility.

Financial sustainability does not necessarily require charging fees to persons who apply for IDs. It can be achieved by alternative means, such as by charging fees to service providers for identity authentication or for enhanced or expedited services.

Outsourcing to private-sector providers and the development of PPP models to harness private-sector investment and expertise (see Question 100) can also provide opportunities to enhance financial sustainability by realizing cost savings. Another potential source of overall savings to government services is achieved from the elimination of "ghost workers" on the government payroll and/or elimination of fraud or duplication in the provision of state benefits.[257] However, such elimination will likely only yield one-time rather than recurring savings.

If there is a dependency upon subsidies or cross-process financing, and a decline in income from part of the system subsidizes other parts that have lower income or higher costs, the financial model may become unstable.

Examples

Pakistan: The National Database and Registration Authority (NADRA) achieves financial sustainability by charging fees associated with the National ID Card. NADRA internalizes the costs of initial enrolment and production of the cards and charges fees to third parties, such as banks and government bodies, when they use an individual's biometric data for authentication. NADRA also organized an independent public company that provides services to other countries to implement ID programs. The ability to self-fund potentially gives NADRA more flexibility over its budget than other ID programs that are restricted by the resources and timelines of their funding sources. [258]

Nigeria: Beginning in 2007, Nigeria instituted the Integrated Payroll and Personnel Information System (IPPIS), an electronic ID system to manage the payment of salaries and wages of government employees.[259] In 2018, the Nigeria Police Force was integrated into IPPIS and it was discovered that 80,115 "ghost officers" were on the payroll. The Government estimated that over N288 billion has been saved by IPPIS in personnel since 2007 including by removal of ghost workers throughout various ministries, departments and agencies.[260]

[257] See World Bank, *Principles on Identification for Sustainable Development: Toward the Digital Age*, facilitated by World Bank Group and Center for Global Development, February 2017 at 14.

[258] ITU-T Focus Group Digital Financial Services, Review of National Identity Programs, May 2016 at 31.

[259] IPPIS website, About, What is IPPIS.

[260] Udo, Bassey, *Premium Times*, "Over 80,000 'ghost officers' uncovered in Nigerian Police," 26 March 2018.

Annex I. Governance, Social and Cultural Factors

Guidance to the IDEEA user

Complete this section only if no ID4D Diagnostic has been carried out.

Policy and governance environment

103. *Digital policy:*

a. *Is the country implementing a broad policy of digitalization of government services? ..... [Y/N]*

b. *i. Summarize the policy and how far the country has advanced in these initiatives:*

c. _____

d. *ii. Which body(ies) or agency(ies) are leading these efforts?*

e. _____

f. *Is the country pursuing the establishment of conditions to develop the digital economy (e.g., legal and regulatory frameworks for e-commerce, recognition of intellectual property, digital financial services, competitive telecommunications markets, etc.)? ..... [Y/N]*

g. *i. Summarize progress the country has made in these initiatives:*

h. _____

i. *ii. Which body(ies) or agency(ies) are leading these efforts?*

j. _____

Background

The country's current state of development and future plans for providing digital means of access to Government services and for developing a vibrant digital economy will be important demand considerations for the development of a national digital ID system. This may influence the type of system required, the capabilities and functional purposes, any need for system harmonization and/or establishment of a new system, as well as the timescale.

104. ***Governance and compliance culture:*** *Using the World Bank Governance Indicators, provide the most recent data for each indicator in the table below.*

Indicator	Year	Data provided
Voice and Accountability (VA)		
Political Stability and Absence of Violence/Terrorism (PV)		
Government Effectiveness (GE)		
Regulatory Quality (RQ)		
Rule of Law (RL)		
Control of Corruption (CC)		

Background

While a legal and regulatory framework governing an ID system should promote inclusion, safeguard data and protect privacy, the framework is undermined if it cannot be enforced or is routinely ignored or undercut. It is therefore important

to consider whether laws in the country are generally monitored and adhered to, as a way of assessing the likelihood that an ID system will effectively protect the rights of individuals which are embodied in the country's legal framework.

Question 104 seeks to provide insight into a country's "culture of compliance." It refers to indicators outside the ID framework that can serve as proxies for likely compliance with the legal framework of an ID system. If there are indications that compliance is unlikely, then stronger protections may need to be built directly into the technology and other design elements of the system

The *World Bank World Governance Indicators*, which is an interactive data set of over 1,000 indicators from different data sources, summarizes views on the quality of governance in specific countries from a large number of enterprise, citizen and expert surveys conducted by various survey institutes, think tanks, non-governmental organizations, international organizations and private sector firms.[261] The indicators compiled measure six broad dimensions of governance:

- **Voice and Accountability (VA)** – capturing perceptions of the extent to which a country's citizens are able to participate in selecting their government, as well as freedom of expression, freedom of association, and a free media.
- **Political Stability and Absence of Violence/Terrorism (PV)** – capturing perceptions of the likelihood of political instability and/or politically-motivated violence, including terrorism.
- **Government Effectiveness (GE)** – capturing perceptions of the quality of public services, the quality of the civil service and the degree of its independence from political pressures, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies.
- **Regulatory Quality (RQ)** – capturing perceptions of the ability of the government to formulate and implement sound policies and regulations that permit and promote private sector development.
- **Rule of Law (RL)** – capturing perceptions of the extent to which agents have confidence in and abide by the rules of society, and in particular the quality of contract enforcement, property rights, the police, and the courts, as well as the likelihood of crime and violence.
- **Control of Corruption (CC)** – capturing perceptions of the extent to which public power is exercised for private gain, including both petty and grand forms of corruption, as well as "capture" of the state by elites and private interests.[262]

Viewed as a whole, values provided for these indicators can give a sense of the "culture of compliance" for the country and can inform the approach taken to ensure robust protection of rights.

105. *Corruption:*

a. *Provide the country's score and country ranking in its Transparency International Corruption Perception Index. (See https://www.transparency.org/research/cpi)*

Score (0-100): ____ (100 = low corruption, 0 = high corruption). Ranking ___/___

b. *Provide the country's Trace Bribery Risk score and country ranking.*

Score (0-100): ____ (0 = low risk, 100 = high risk). Ranking ___/___

c. *Are there corruption laws that would apply to the operation of ID systems and use of personal data? ..... [Y/N]*

d. *If so, specify:* _____

e. *Are there established procedures for addressing instances of corruption?..... [Y/N]*

f. *Are anticorruption provisions contained in ID operational manuals?..... [Y/N]*

g. *Has any of the ID systems addressed in Part III been the subject of inquiry as to corruption? ..... [Y/N]*

h. *If so, explain.* _____

[261] World Bank World Governance Indicators.

[262] World Bank World Governance Indicators, FAQs.

Background

Corruption has the capacity to undermine most safeguards which could be put in place to safeguard personal data. The questions are intended to highlight the degree to which corruption is a problem, and the country's willingness to reduce, address and control it. Where corruption is a particularly intransigent problem, this might point the need for particularly strong guarantees of independence for the agency which will monitor implementation of the legal framework on privacy, non-discrimination, procurement and other aspects affecting ID systems.

106. *Recent election experiences*

a. *Have there been any recent credible allegations or findings of voter fraud? ..... [Y/N]*

a. *Is there a functioning system whereby voter registration decisions can be challenged or reviewed? ..... [Y/N]*

b. *Was there any recent experience of election-related violence? ..... [Y/N]*

c. *Does the public generally have confidence in the validity of recent election results? ..... [Y/N]*

d. *Provide any insights relevant to the development and operation of ID systems.*

e. _____

Background

Information about recent election experience provides useful insights into various aspects of the country's needs and readiness for developing existing or new ID systems. For example:

- Voter registration is a functional registration system which raises some of the same data validation issues found in ID systems. Some ID systems are born out of, or linked to, voter registration. In such cases, the integrity of the voter registration system may be closely linked to the integrity of the ID system. Voter registration involves identity authentication which may link to a foundational ID system, but it may be risky to connect a foundational ID system to elections (or other politically-contentious functional uses) if the elections (or other functional uses) have a troubled immediate past.
- Most countries being assessed will have a voter registration and voting system in place governed by a legal framework. Because elections are highly politicized events, they can provide a good illustration of whether or not the legal framework is respected in the context of political stress.
- Elections are often closely observed by local and international monitoring bodies and the press, which may generate a range of available commentary on voting from different political viewpoints.

Social and cultural factors

107. *Literacy and digital literacy:*

a. *What is the adult literacy rate? Use UNESCO eAtlas or equivalent source.*

b. _____*% as of* _____ *(year)*

c. *Rate the use of the digital services among the population in the table below, ticking the appropriate box.*

Function	Hardly any	Some	Widespread	Near universal
Use of mobile phones				
Use of smart phones				
Use of internet (mobile or fixed)				
Use of mobile money or other digital financial services				
Use of e-health services				
Use of e-government services				
Use of e-signatures and other trust services				

d. *Are there any groups within the population who are significantly less digitally literate than the general population? ..... [Y/N]*

e. *If so, specify:* _____

Background

An assessment of digital literacy is useful in several respects.

A population's familiarity and comfort with digital technologies, such as mobile phone, internet and mobile money usage may provide some insight into opportunities and challenges presented by the introduction of an electronic ID system. A population with little experience with these technologies can be expected to require greater outreach and education efforts to become familiar with a new digital technology. Similarly, any specific population group that is less digitally literate than the population as a whole may require additional outreach efforts. Such population groups may also be more vulnerable to exploitation.

Digital literacy is also relevant to a population's ability to understand the contemplated uses of personal data collected for ID purposes. This can cut both ways. If a population is unfamiliar with a new technology, individuals may be hesitant to trust or adopt it. However, in many developing countries, technological leapfrogging has meant that members of the public are more comfortable with using mobile devices and similar technology, having little experience with more basic technologies.

Finally, digital literacy provides an indication of the initial level of demand for services that would utilize a digital ID system. A society with high use of digital financial, e-government and e-health services has the potential to benefit quickly from the introduction of a digital national ID.

108. *Attitudes towards ID systems:*

a. *Is there general public support for the existing or any planned ID system(s)? ..... [Y/N]*

b. *If not, identify the reasons for the lack of support:*

_____

c. *Identify any population groups who are less supportive than others and any concerns specific to them:*

_____

d. *Have there been substantial objections to the collection or use of personal data from any sector of the public? ..... [Y/N]*

e. *If so, describe the information and the basis for the objections:*

_____

Background

The value of an ID system is diminished if a population distrusts or actively avoids usage. If a population, or a particular group, is not supportive of an existing or planned ID system, the reasons behind the lack of support may inform how to approach introducing or improving the ID system. In some cases, the system can be designed (or if it already exists, modified) to address legitimate concerns. For example, if concerns over data privacy are undermining support, the system can incorporate robust privacy protections. If certain groups fear discrimination, measures can be taken to ensure the ID system is inclusive and non-discriminatory. In other cases, the lack of support may be based on lack of information or even misinformation. There outreach and education campaigns could be implemented to educate the public on the ID system and assuage any concerns.

Examples

In the **United Kingdom**, in 2002 the government outlined plans to introduce ID cards to combat fraud and illegal activities which would be compulsory for certain individuals, such as foreign nationals. The plans were implemented but amidst declining public support, the ID cards were scrapped entirely in 2011. [263] However, the debate over whether national ID cards should be introduced for UK citizens has recently resurfaced in light of the UK's possible departure from the EU.

109. ***Media and civil society:*** *Are the media and civil society and media active in holding government bodies, vendors and the private sector accountable to the laws and principles?..... [Y/N]*

f. *If so, describe and significant instances:*

_____

Background

[263] BBC News, Timeline: ID cards, 27 May 2010; UK Government, Identity cards

The media and civil society may play a significant role alongside courts and enforcement authorities in monitoring the weaknesses and abuses of an ID system and more broadly use of personal data.

Example

The media in **India** has been extensively involved in exposing gaps in the Aadhaar system. The New York Times and other media institutions have been highly instrumental in the 2018 exposure of Cambridge Analytica's activities in the **USA and UK**.

Annex II. GDPR's Key Principles and ID

GDPR Article 5	Relevance to ID systems
1. Lawfulness, fairness and transparency Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. Generally, under the GDPR, personal data is processed lawfully when it is: (i) necessary for performance of a contract; (ii) necessary for compliance with a legal obligation; (iii) necessary for the legitimate interests of the controller; (iv) necessary in order to protect the vital interests of the data subject or of another natural person, (v) necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or (vi) the consent of the data subject has been obtained. The GDPR seeks to achieve fairness in a number of ways, for example, when assessing whether it can rely on its legitimate interests to lawfully process personal data, the controller is required to override its competing interests if the fundamental rights and freedoms of the data subject require protection of their personal data. The GDPR also seeks to ensure transparency by requiring controllers to provide transparent information about their processing activities to data subjects by way of an information notice when they obtain personal data.	Lawfulness in the ID context would involve the processing of personal data being carried out pursuant to clear and detailed legal authority or consent that is freely given. Fairness would involve issues of inclusion, exclusion and non-discrimination. Transparency would require that the law should specify the data which is being collected, the purposes of the data collection, who will have access to the data, and what safeguards are provided against abuse.
2. Purpose limitation Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. Generally, this means that personal data should only be collected where the purpose of such collection is made clear to the data subject, and not be used for any other purpose. 3. Data minimization Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Generally, this means that the quantity and nature of the personal data collected should not exceed what is necessary to achieve the stated purpose. 4. Accuracy Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Generally, this means that data controllers have a responsibility to ensure that the personal data is up-to-date and accurate. Under the GDPR, data subjects have a right to require that controllers rectify or erase their personal data without undue delay.	In the context of ID systems, the collection of personal data should have the purpose of serving the ID system and its related functions. Government agencies and other organizations collecting personal data should explicitly state the purpose of collection of personal data to individuals. Further processing of the personal data collected should be compatible with the purpose of the ID system. Processing for statistical purposes would generally not itself be viewed as incompatible. Only the information relevant and required to achieve the purpose of the ID system should be collected. An ID system should have processes to ensure that changes of name, address and other attributes comprising or linked to the ID are accurate and kept up to date.
5. Storage limitation Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal	Certain information kept in civil registration files may need to be permanently identified with the data subject, since it is of historical

GDPR Article 5	Relevance to ID systems
data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of appropriate technical and security measures in order to safeguard the rights and freedoms of the data subject. Generally, this means that data controllers should implement processes to ensure personal data is only stored for as long as necessary for the stated purpose.	importance for constructing genealogies. However, other data associated with the ID system or with separate databases (such as databases on health or voter registration) which use unique ID numbers as identifiers should be disassociated with the identity of the data subject when such personal data is no longer required for the stated purpose. This is to ensure that the data subject is not able to be identified through merging, combining or triangulating information.
6. Integrity and confidentiality Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. Generally, this means that data controllers should implement technical and organizational security measures (i.e. physical security and cybersecurity) to protect personal data against such risks. In order to do this, controllers should consider conducting risk assessments and develop organizational policies and procedures to mitigate the risk of a security breach.	In respect of ID systems, the law should provide measures to ensure that officials with access to data collected for ID purposes have an enforceable duty of confidentiality. Government agencies and organizations should also be required to implement appropriate physical and technical security measures to safeguard personal data against unauthorized or unlawful processing and accidental loss, destruction or damage.
7. Accountability The data controller shall be responsible for, and be able to demonstrate compliance with the above principles. However, under the GDPR the data processor is also required to comply with certain obligations which reflect the above principles. (For background, the controller is the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. The processor is the entity which processes personal data on behalf of the controller.) For example, under Article 32 of the GDPR, the processor is required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Further, under Article 28 of the GDPR, the data processor is required to assist the data controller in ensuring compliance with the data controller's obligations under Articles 32 to 36.	In respect of ID systems, the relevant government agency would be expected to take responsibility for ensuring that these principles are observed. Any third-party organizations should also be required to demonstrate compliance with such principles and to assist the government agency in its compliance efforts. Effective supervision and reporting should be part of the ongoing governance process.

Id4d.worldbank.org