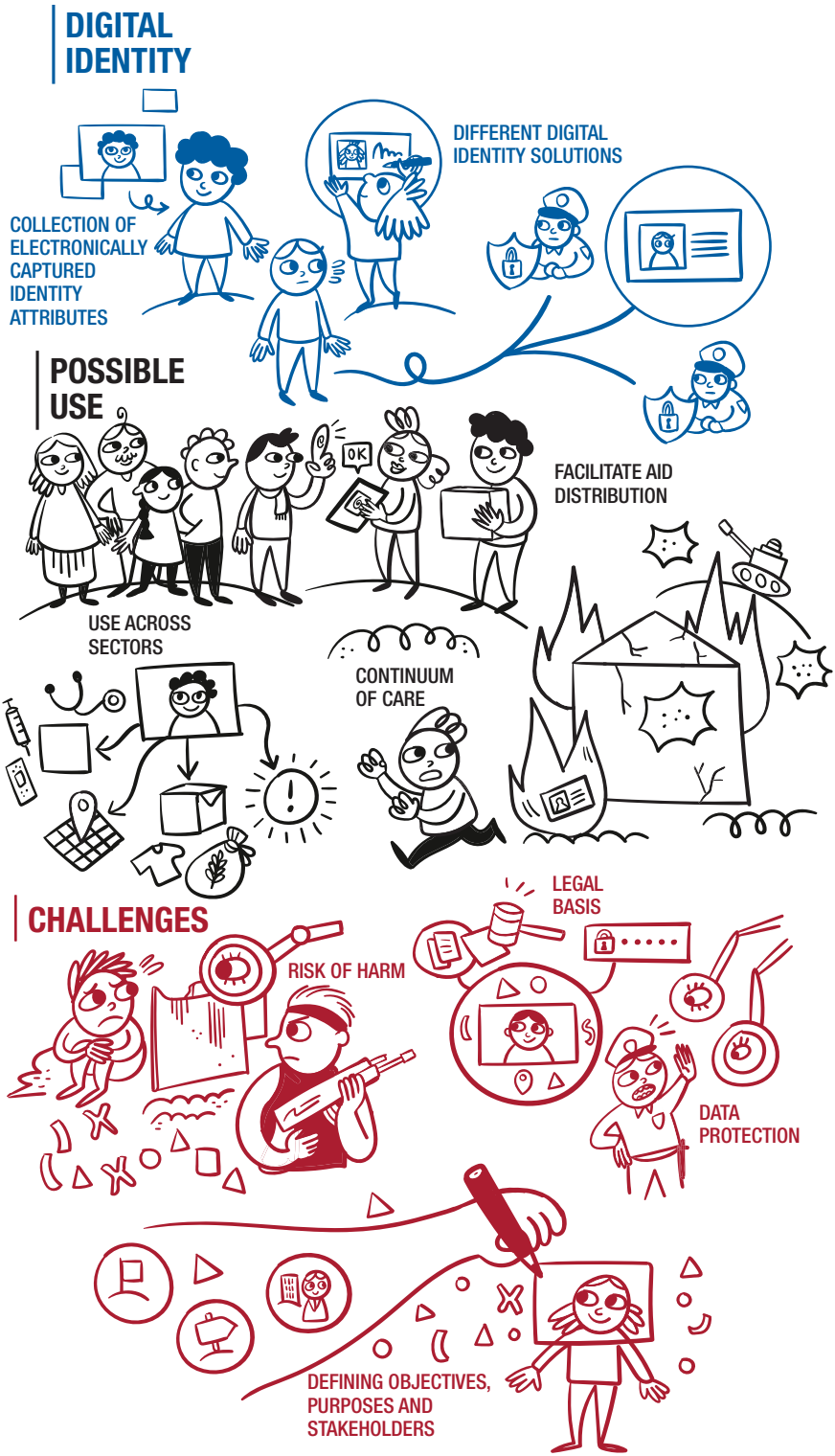

CHAPTER 13

DIGITAL IDENTITY

Vincent Graf Narbel*

* The author would like to thank Aiden Slavin (ID2020), Giulio Coppi (Norwegian Refugee Council), Dr Tom Fisher (Privacy International) and Robert Riemann (European Data Protection Supervisor) for their contributions to this chapter.

13.1 INTRODUCTION

Every human being has an identity. The right to identity is undisputed and recognized in international declarations and conventions.[1] But not all human beings have a way to prove their identity. In this regard, everyone should have a means to prove who they are through an identity tool.[2] The form such a tool should take remains a matter of dispute. Yet no matter what its form – document, card, token, mobile app or something else – it needs to be produced and managed. The mandates of Humanitarian Organizations frame their action, and this is particularly acute with Digital Identity as we will see in this chapter.

In most cases, Humanitarian Organizations need to use identity management systems to facilitate programmatic goals (e.g. a beneficiary management system set up to ensure aid is provided to the intended individual(s)).[3] Some organizations have been involved in initiatives that aim to develop identity management systems that go beyond simply supporting a programmatic goal and, in practice, provide a legal identity[4] (sometimes in a digital form) to those who lack identification documents and who, because of that, can be made "invisible, discounted, and left behind".[5]

Sometimes, however, an identity tool that was initially designed and deployed to support programmatic goals shifts with time towards a broader use (such as to prove someone's legal identity). This shift introduces a significant function creep of the identity tool, necessitating a complete reevaluation of the data protection and privacy risks.

Against this background, this chapter analyses the data protection implications of setting up a Digital Identity management system for beneficiaries. The discussion covers, among other issues, the way in which Humanitarian Organizations collect and store data in such a system and how they manage information about participants, users and/or beneficiaries.

1 See for example: Universal Declaration of Human Rights, Article 6, and UN Convention on the Rights of the Child, Article 7.

2 See SDG target 16.9: "By 2030, provide legal identity for all, including birth registration": https://sustainabledevelopment.un.org/sdg16.

3 Strategy & Research team, "Identity in a Digital Age: Infrastructure for Inclusive Development", USAID, 2017, 1: www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf.

4 Throughout this chapter, the expression "legal identity" follows the UN operational definition of the term: "Legal identity is defined as the basic characteristics of an individual's identity, e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally-recognized identification authority. This system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death. In the case of refugees, Member States are primarily responsible for issuing proof of legal identity. The issuance of proof of legal identity to refugees may also be administered by an internationally recognized and mandated authority." "UN Legal Identity Agenda", UN Stats, accessed 10 March 2022: https://unstats.un.org/legal-identity-agenda.

5 Strategy & Research team, "Identity in a Digital Age", 1.

To start the discussion, it should be noted that there is no universally accepted definition of the term "Digital Identity", although it can generally be agreed that Digital Identities consist of "a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions".[6] As a multifaceted concept, however, Digital Identity can relate to a number of other important concepts, such as identification, functional identity, foundational identity and personal identity.[7] Since these terms are used throughout this chapter, a simplified explanation of each of them is given in the Table 13.1.

Table 13.1

Term	Objectives	Typical characteristics	Examples
Functional identity	Enables a specific service (function) to authenticate participants.	Contextual, duplication of information.	Every individual can have multiple functional identities and these can be transnational, such as a student ID, a voter ID or a food distribution programme ID.
Foundational identity (legal identity)	Provides a legal identity to a broad population as a public good without specifying a specific service. It allows individuals to prove who they are. The issuer of such an identity is considered a trusted source of identity – sometimes referred to as an authoritative source of identity.	Generates a legal identity that can be referenced by others. Within its given scope, every person can have only one such identity. However, the same person may have several legal identities (e.g. passports issued by different countries).	Typically, legal identities which are government-based and covering the whole population of a country,[8] such as social security number, a birth certificate or an Aadhaar number (a 12-digit number that, in India, uniquely identifies people based on their biometric and demographic data).
Conceptual identity (personal identity)[9]	Defines an individual's identity in relation to others within a given societal structure, determining how they view themselves and how they are perceived by the society around them.	Intangible, variable and heavily defined by personal and societal perception.	Defining attributes (such as ethnicity, sexuality, religion, or political orientation), according to which individuals define themselves and are defined by others within their society.

6 World Bank Group, GSMA and Secure Identity Alliance, "Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation", Mobile for Development, GSMA, Washington, DC, 26 July 2016, 11: www.gsma.com/mobilefordevelopment/resources/digital-identity-towards-shared-principles-public-private-sector-cooperation.

7 Jonathan Donner, "The Difference between Digital Identity, Identification, and ID", Medium (blog), 19 December 2018: https://medium.com/caribou-digital/the-difference-between-digital-identity-identification-and-id-41580bbb7563.

8 Strategy & Research team, "Identity in a Digital Age", 12.

9 This chapter will not address conceptual identity as this cannot be encompassed by an identity system.

In view of these different types of identity, it is important for Humanitarian Organizations to clarify from the outset whether they require a functional or a foundational identity for beneficiaries, since this choice affects the design of the identity system and the associated management processes (e.g. collaboration with a Third Party, links to other existing systems, etc.). On many occasions, various legal frameworks will impose significant constraints and requirements on the design of the identity system. It is crucial to comply with these requirements while upholding data protection principles.

13.1.1 AUTHENTICATION, IDENTIFICATION AND VERIFICATION: WHO ARE YOU AND HOW CAN YOU PROVE IT?

Humanitarian Organizations do not always need to know someone's legal identity. This is true, for example, when the purpose of the interaction is to provide aid. Consequently, before developing a Digital Identity system, Humanitarian Organizations need to identify what information they need from beneficiaries for a specific humanitarian programme. Here, there is an important distinction to be made between authentication, identification and verification.

Identification answers the question: "Who are you?" But when setting up an identity management system, organizations should start by asking a different question, namely: "What do I need to know from that person to provide aid or protection?" Knowing who the person is can be important in some cases. For instance, when reuniting unaccompanied minors with their parents, it is critical to ascertain that the alleged parents are indeed who they purport to be. But quite often – possibly in most cases – it is enough to know that the person is entitled to access a service because they meet a certain criterion or have a particular set of attributes (e.g. they can prove they are under 12 in order to receive a particular vaccine). This is also known as authentication – or being able to prove a claim of who you are.

Even when Humanitarian Organizations only need authentication, they should carry out a verification process when registering beneficiaries in the identity management system. Verification, therefore, is the act of checking someone's identification (such as confirming a person's name on their identity document) or some of their identity attributes (such as confirming that a person is a member of the community that will receive aid by checking with the community leader). When a simple authentication system is used to ensure aid is delivered to affected individuals, verification at the time of enrolment can help to ensure that the people who were entitled to receive it were the ones registered. However, it should be noted, that some aid services may not need verification at all. This is true, for instance, when a Humanitarian Organization makes information available on an online platform where anyone can register.

When Humanitarian Organizations enrol and register beneficiaries, some data about them will need to be collected and stored in the identity management system. As will become clear below, deciding what attributes need to be recorded, and for what

purpose(s), is a key decision from a data protection perspective. In particular, only attributes that are necessary to achieve the activity's purpose (e.g. supporting the delivery of aid) should be collected. For example, in most cases, an organization would probably not need to store a copy of an identity document to record the fact that a registered person was verified to be a minor. Once enrolled, the beneficiary may receive some record of their identity, such as an attestation, a card, a pin code, or a digital certificate they can access and manage on a mobile device. There is no need for further verification at the point of delivery, since the beneficiary already has proof that they are entitled to access the service in question.

13.1.2 DIGITAL IDENTITY

Digital Identity is a set of attributes stored digitally that uniquely describe a person in a given context (see the types of identity described previously: functional, foundational and conceptual). In some cases, individuals could have more than one, and potentially hundreds of Digital Identities, each serving as a functional identity. This type of system would allow beneficiaries to access services, assistance or protection in a similar way to a username and password access model or a token system, without having to prove their legal identity.

In other cases, however, organizations may need to distinguish one individual from another with a high degree of certainty, and perhaps have only one Digital Identity for each person. In these scenarios, the identity system should allow a Digital Identity to be linked to a physical person. The aim here is to make it easier to distinguish between individuals, for instance when the organization is providing personalized aid (e.g. health care). Yet even when such a link is necessary, the organization might not need to obtain legal identity documents from beneficiaries. For instance, people might be able to register with their name only, without needing to confirm that the name they have given matches their legal identity (e.g. by checking it against their birth certificate or other identity documents).

Lastly, there may be cases where the Humanitarian Organization needs a system that also allows it to ascertain and verify the individual's legal identity. This is very similar to the previous case, except that a legal identity document (or a foundational entity) will be required in order to formally identify the person in question.

In summary, these are the main steps that a Humanitarian Organization should follow when setting up a Digital Identity management system:

First, the organization decides what it needs to know about the affected people so it can implement a specific humanitarian programme. This will determine whether identification is required or whether authentication alone is sufficient. From a data protection standpoint, the latter option should be preferred wherever possible.

Second, the organization determines, based on programme needs, whether it requires a functional or foundational identity, bearing in mind that only a handful of Humanitarian Organizations have a mandate to establish and/or manage foundational identities, and only for specific purposes.

Third, the organization designs a verification process to cross-check the information provided at the enrolment stage. Depending on the chosen identity system, it can involve no particular formality, some due diligence or an authoritative legal document. The organization should also determine whether or not it needs to retain the information assessed in the verification phase.

13.1.3 SYSTEM DESIGN AND GOVERNANCE

Once the Humanitarian Organization understands its objectives (authentication, identification and verification), it needs to decide how the Digital Identity system will be designed to achieve its intended purposes, and how it will be governed. The Humanitarian Organization (or other body) can control the system centrally, or control can be shared across multiple parties in a decentralized way.[10] Some current initiatives aim to give individuals control over their own identity systems by deciding who can access their identity credentials and when. In this sense, the governance structure is sometimes influenced by where the data will be hosted. When multiple parties access the same system, for instance, there needs to be a shared platform. Likewise, when efforts are made to shift control to individuals, it may be possible to allow them to store their credentials on their own devices or to use a service provider of their choosing.

The following decision tree summarizes both the questions that Humanitarian Organizations should answer, and the factors they should consider, when deciding whether to implement an identity system:

1/ Identity system type:

- Can you rely on authentication only, or do you really need to identify the beneficiaries?
- Are you aiming to generate functional or foundational identity? (Remember: only some organizations have the mandate to generate foundational identity.)

10 The difference between decentralized and distributed architecture and a federated identity system is described in detail in the literature. While this is an important point, it is beyond the scope of this chapter and will therefore not be discussed here. For a more detailed description of decentralized identity, refer to the following sources: "DIF – Decentralized Identity Foundation", accessed 22 February 2022: https://identity.foundation; "Decentralized Identifiers (DIDs) v1.0", World Wide Web Consortium, accessed 22 February 2022: https://w3c.github.io/did-core; World Economic Forum, *Trustworthy Verification of Digital Identities*, White Paper, Inclusive Deployment of Blockchain for Supply Chains (World Economic Forum (WEF), April 2019: www3.weforum.org/docs/WEF_Trustworthy_Verification_of_Digital_Identities_2019.pdf.

- Do you need to verify the information at enrolment? If not, is a system without verification acceptable? If so, does verification require a formal, legal identity document (or is a simpler form of verification acceptable)? Do you need to retain the information assessed during the verification process?

2/ Design choices:

- What information should be stored? By whom? And where?
- Note that verifying a particular attribute (such as nationality, to determine whether the person is eligible for inclusion in a humanitarian programme) does not mean that this information has to be stored in the identity system. The system can simply confirm that a person has the necessary attribute without further details.
- In some cases, there may be no need for verification in the first place. This applies, for example, to a generally accessible digital service, where an account can be created freely without disclosing any personal information, or to cases where an individual's mere presence in a place where people are displaced entitles them to access aid (when cards are distributed without collecting information, for instance).
- How will the data be controlled and governed? Who needs to access what information, at what point and for what purposes?

Importantly, Digital Identity programmes are not limited to specific technologies or systems. Such programmes can be designed using one of many technologies or a combination of solutions. Technologies frequently associated with Digital Identity include:

- **Biometrics:**[11] Enrolling beneficiaries in Digital Identity schemes in the humanitarian sector may include the use of Biometrics such as fingerprints or iris scans.
- **Blockchain:**[12] Blockchain is one possible way for individuals with limited access to digital technology and infrastructure to prove their identity.[13] Despite its promise, however, the challenges that come with Blockchain technology demand serious consideration.
- **Data Analytics:**[14] Digital Identities can be created from digital behavioural attributes (also called algorithmic ID) without using official credentials. Here, a person's online activity (social media use, browsing history, online purchases, call history, etc.) could be used to verify their identity.[15] Although the potential of

11 See Chapter 8: Biometrics.

12 See Chapter 15: Blockchain.

13 Ana Beduschi et al., *Building Digital Identities: The Challenges, Risks and Opportunities of Collecting Behavioural Attributes for New Digital Identity Systems*, Open Research Exeter, University of Exeter & Coelition, 2017, 15–16, 26: https://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Buiding_Digital_Identities_with_Behavioural_Attributes.pdf.

14 See Chapter 17: Artificial Intelligence for issues related to the use of Data Analytics.

15 Beduschi et al., *Building Digital Identities*, 8.

profile-based identity systems is not yet fully realized, this approach does raise data protection concerns.[16]

13.1.4 DIGITAL IDENTITY IN THE HUMANITARIAN SECTOR: POSSIBLE SCENARIOS

The following four scenarios shed light on the interplay between various Digital Identity systems in the humanitarian sector.

Scenario 1: A Humanitarian Organization issues an identity credential (for example, a registration card or document) to a registered beneficiary of aid. In this scenario, the beneficiary – a Data Subject – would use a functional identity, which enables them to receive aid. In some situations, however, such an identification system could be accepted as proof of the identity of the beneficiary – in other words, as a foundational identity (see scenario 4). Yet under some humanitarian programmes, individuals only have to authenticate to prove that they are legitimately entitled to access certain aid services, without the need for identification.

Scenario 2: A Humanitarian Organization offers multiple services to beneficiaries. In order to provide these services, each unit of the organization needs to have access to a certain part of the data collected from beneficiaries. For example, to provide in-kind aid, the unit may need to access aid distribution records linked to the beneficiary. Another unit, meanwhile, may need to access medical records to provide a follow-up treatment, while a third unit may need information about the individual to restore family links.

Scenario 3: Several Humanitarian Organizations provide multiple services to beneficiaries through a unified identity system. Under this type of shared identity solution, each organization can access the data that are necessary and relevant for the provision of its services. This scenario would entail both authentication and identification. Interoperability between the various bodies and organizations involved could prove beneficial, with the system acting as a single gateway for humanitarian assistance. This would entail applying the "once-only" principle[17] in Humanitarian Action to facilitate the provision of physical or digital services directly to beneficiaries through online platforms and/or the exchange of information or documents (automatically or on request) between various Humanitarian Organizations.[18] Yet organizations will

16 For example, Facebook shadow accounts. See: Russell Brandom, "Shadow Profiles Are the Biggest Flaw in Facebook's Privacy Defense", The Verge, 11 April 2018: www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy.

17 The once-only principle implies that individuals provide their personal information to the authorities only once and that afterwards, at their request or with their Consent, government departments may exchange the information for the fulfilment of their public duties instead of collecting it again.

18 See: European Data Protection Supervisor (EDPS), *Opinion 8/2017: EDPS Opinion on the Proposal for a Regulation Establishing a Single Digital Gateway and the 'Once-Only' Principle*, Opinion, EDPS, Brussels, 1 August 2017: https://edps.europa.eu/sites/edp/files/publication/17-08-01_sdg_opinion_en.pdf.

need to consider a range of factors when opting for such solutions. For example, they should identify the applicable governance framework and ensure that the roles played by those involved in the system (Data Controllers and Data Processors) are clear. Since appropriately segregating access to data can be technically difficult, it is not uncommon for Data Breaches to occur in unified commercial solutions. Likewise, in a unified system, the complex relationships between organizations can make it hard to ensure that data are only used for the purposes for which they were collected. In addition, complex systems such as these can lead to the *de facto* exclusion of certain groups who may lack the requisite digital literacy skills.

Scenario 4: In some contexts, Humanitarian Organizations may issue functional identity documents to beneficiaries, such as registration cards allowing affected people to access their services. These may end up serving as foundational identity documents for authorities or financial institutions that accept them as proof of ID.

EXAMPLE:
In Jordan and Egypt, two countries that receive a large influx of refugees, local authorities require a valid passport or government-issued identification, such as a Jordanian Ministry of Interior service card for refugees and asylum seekers, to meet mobile SIM registration and Know Your Customer (KYC) requirements. UNHCR argues that its own identification documents should also be accepted, as these may be the only forms of ID that asylum seekers and refugees have.

13.1.5 DIGITAL IDENTITY AS FOUNDATIONAL IDENTITY

Various ongoing initiatives are aiming to develop Digital Identity systems that serve as a form of foundational identity for people without ID documents.

These initiatives are inspired by the fact that people who cannot prove who they are find it harder to assert their rights, access public services, and claim benefits and entitlements based upon their age, nationality, circumstances or any other identity and status attributes.[19] Since proof of ID has become a prerequisite for accessing many services, the identity gap is a major barrier to participation in political, social and economic life. For example, private service providers often require a proof of ID to comply with legal requirements or as part of their due diligence processes (such as KYC, prevention of fraud and impersonation, and transaction risk and cost reduction). Digital Identity systems could be one way to help people in need but who lack

19 Guglielmo Verdirame and Barbara E. Harrell-Bond, *Rights in Exile: Janus-Faced Humanitarianism*, Berghahn Books, New York, 2005, 59–63.

identity documents. As mentioned above, however, very few Humanitarian Organizations have the mandate – and therefore the legitimate basis – to develop and deploy foundational systems of this type.

13.2 DATA PROTECTION IMPACT ASSESSMENTS

A Data Protection Impact Assessment (DPIA) involves identifying, evaluating and addressing the impacts on Data Subjects and their Personal Data of a project, policy, programme or other initiative that entails the Processing of such data. It should ultimately lead to measures that minimize the risks to the rights and freedoms of individuals and should follow a project or initiative throughout its life cycle. In light of the large-scale Processing that Digital Identity systems involve, and of other potential risks and harm to Data Subjects arising from their use, Humanitarian Organizations should carry out a DPIA both before and during system and programme implementation. In addition, the DPIA process should analyse not just compliance with data protection requirements, but also the potential adverse impacts of the system on a variety of fundamental rights, as well as the ethical and social consequences of the data Processing.[20]

The use of identity systems for multiple humanitarian purposes – some of which are not always identified from the outset – poses the risk of so-called function creep. This occurs when Humanitarian Organizations – intentionally or otherwise – misuse beneficiaries' data by using the identity system for purposes that were not originally foreseen. Moreover, governments and non-State armed groups that do not respect human rights could access identification and other systems to identify enemies or opponents, or to target and profile certain groups based on their ethnicity, political opinion, nationality or other characteristics. This information can then be used to control, discriminate against and harm these individuals or groups in different ways, for instance by excluding them from essential services and aid, depriving them of their liberty and their right to a fair trial, or even committing atrocities (such as the Rwandan genocide or the persecution in Nazi Germany, where identification and profiling played an essential role).

13.3 DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by design and by default is a practice that should feature throughout the life cycle of applications that process Personal Data.[21] It involves designing a

20 Alessandro Mantelero, "AI and Big Data: A blueprint for a human rights, social and ethical impact assessment", *Computer Law & Security Review*, Vol. 34, No. 4, August 2018, 755: www.sciencedirect.com/science/article/pii/S0267364918302012?via%3Dihub.

21 Lina Jasmontaite et al., "Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR", *European Data Protection Law Review*, Vol. 4, No. 2, 2018, 168–189: https://doi.org/10.21552/edpl/2018/2/7.

Processing operation, program or solution in a way that implements key data protection principles from the outset, and that provides the Data Subject with the greatest possible data protections (see Chapter 6: Designing for Data Protection). The key data protection principles in this sense are:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimization;
- accuracy;
- storage limitation (limited retention);
- integrity and confidentiality (security);
- accountability.

When designing an identity system, Humanitarian Organizations should therefore start by considering their needs, and then examining whether an identity system is necessary and proportionate to solve the identified problem. If an organization determines that it does require an identity system, it should think carefully about which type of system best fits its needs and is appropriate in the particular circumstances. Following this process will help the organization apply the principles of data minimization and proportionality, as explained in Section 13.6 – Application of basic data protection principles, below.

Data protection by design also requires an organization to conceive systems in a way that makes it possible, and easier, for a Data Subject to exercise their rights (see Section 13.5 – Rights of Data Subjects, below). For example, in a Digital Identity system, Data Subjects should, by default, have access to information notices, to all information linked to their identity, and to logs detailing who has accessed their data and for what purposes.

13.4 DATA CONTROLLER/DATA PROCESSOR RELATIONSHIP

Digital Identity systems can involve a wide range of bodies and entities, including Humanitarian Organizations, governments, and commercial entities such as banks, payment system providers, IT network providers and Biometrics companies. Consequently, it can be difficult to ascertain which parties should be treated as Data Controllers and Data Processors. Likewise, it can be hard to determine where the boundaries of responsibility and liability lie among the parties. To counter this problem, a Digital Identity system must be designed in a way that clarifies who the stakeholders are, what responsibilities and obligations they have, and what data categories and flows each one uses and for what purposes. When a Humanitarian Organization determines the means and purposes of the identification programme, it will act as the Data Controller and, therefore, will be potentially liable for breaches, misuse and other types of harm that may arise from the programme. In situations

where joint controllership is established, or where a Data Processor processes Personal Data only on behalf of the Data Controller, it is best practice to allocate responsibilities among the parties in a written agreement.

13.5 RIGHTS OF DATA SUBJECTS

The possibility of developing Digital Identity systems that are controlled by the Data Subject is currently being explored through various initiatives. Such systems aim to shift control to individuals by allowing them to store identity data on their own devices without relying on a central repository and, when necessary, providing credentials to those who need to verify them.[22] As discussed above, this could be achieved, for example, by building a system in which beneficiaries store their personal information on their own devices or in another storage medium of their choosing, and are able to decide when to share it with bodies and organizations involved in the humanitarian response. Some functional or foundational identity initiatives also aim to shift control to individuals, again by allowing them to store their Personal Data on their own devices and sharing them with others if and when they wish. However, whether a control shift would actually happen in practice is still matter of dispute. When pursuing such initiatives, it is important to ensure that individuals are aware of their rights and the risks of having this information stored on their personal devices, and that they are sufficiently equipped to be able to use such tools safely.

EXAMPLE:
The ID2020 Alliance was set up to influence the development of so-called "good" Digital Identities, under which individuals have full control of their identity and can determine which data are shared and with whom. According to the Alliance, "Today, most personal data is stored in silos. The more siloed and numerous your data becomes the less control you have over it." To solve this, the Alliance proposes that individuals "must have control over their own digital identities, including how personal data is collected, used, and shared".[23]

While such initiatives are not yet commonplace, Humanitarian Organizations can give beneficiaries more control over and access to their data by providing them with a login to access all information relating to their identity credentials and, if applicable, a personal profile created by the organization in question. The potential benefits and risks associated with this solution still need to be fully explored, so as to determine

22 Michael Pisa and Matt Juden, *Blockchain and Economic Development: Hype vs. Reality*, CGD Policy Paper, Center for Global Development, Washington, DC, July 2017, 25: www.cgdev.org/sites/default/files/blockchain-and-economic-development-hype-vs-reality_0.pdf.

23 All quotes from the ID2020 website: https://id2020.org.

whether it works in practice and whether it genuinely shifts control to individuals. In theory, however, such a system could automatically inform beneficiaries of any Third Parties that have accessed their data, and whenever a Processing activity starts. It could also allow beneficiaries to update their Consent, when this is the legal basis for Processing, and to receive updated information about the Processing. With more control, beneficiaries could directly exercise their rights as Data Subjects through an online profile or platform. In cases where beneficiaries are not digitally literate, or do not have access to the necessary technology, Humanitarian Organizations must provide alternative ways for them to exercise their rights in respect of their Personal Data.

13.5.1 RIGHT OF ACCESS

Beneficiaries have the right to request access to information about the Processing of their data, and to the data that are being processed.[24] While this right can be limited in certain circumstances, Humanitarian Organizations, as Data Controllers, should reply to such requests by informing beneficiaries if their Personal Data are being processed and, if so, granting them access to the data in question. In practice, however, this right may be hard to implement in Digital Identity programmes as it can be difficult to verify that the person requesting access to information is the individual entitled to receive it (verification), particularly if the request is made by digital means (which is the most likely scenario in the case of Digital Identity). While this is an issue that applies to a wide range of digital systems, it must be given equal consideration in the case of Digital Identity. Humanitarian Organizations should therefore take steps to ensure that the rights of Data Subjects can be respected, both before deciding on the design of a Digital Identity system, and when deciding whether or not to implement it.

Another challenge to respecting the rights of Data Subjects in Digital Identity programmes stems from the fact that different units within the same organization might hold different pieces of information about the same Data Subject. Consequently, compiling all this information in order to respond to a request may prove challenging. It could even involve unnecessary effort, since beneficiaries often only request access to a specific category of data, or to data relating to a particular programme, as opposed to all the data about them that the organization holds. Organizations should therefore discuss this with the Data Subject, so as to understand the specifics of the request and avoid any superfluous effort. Humanitarian Organizations should factor this challenge into their thinking at the Digital Identity system design stage, so they can anticipate issues of this type and devise ways to prevent them. A login-based access system, such as the one envisaged above, could allow beneficiaries to access their profile at any time, check what information is held about them, and the purposes for which it is being used.

24 See Section 2.11.2 – Access.

13.5.2 RIGHTS TO RECTIFICATION AND ERASURE

Beneficiaries should be able to rectify incorrect data about themselves and, in certain circumstances, to have their data deleted. They could do this directly, for instance by logging into their account (as envisaged above). When beneficiaries do not have control over their data, exercising their rights can again prove challenging, not least when it comes to assessing and confirming the identity of someone requesting to have their data rectified or deleted. To address this problem, Humanitarian Organizations will need to implement a verification system that complies with the minimization principle and does not collect unnecessary Personal Data. Here again, having beneficiaries log into their account would be one way to achieve this aim.

13.6 APPLICATION OF BASIC DATA PROTECTION PRINCIPLES

While this section provides an overview of data protection concerns that may arise when dealing with Digital Identity systems, every case should be examined in detail and on its merits, taking into account the technology used and the type of identification needed to achieve the envisioned programme's objectives. Different programmes will have different requirements. Likewise, different technologies may have different data protection implications.

13.6.1 LEGAL BASES FOR PERSONAL DATA PROCESSING

Humanitarian Organizations need to process Personal Data in order to establish or verify the identity of a beneficiary. These Processing operations may be carried out on one or more legal bases. Under scenarios 2 and 3, for instance, a Humanitarian Organization will have to identify a separate legal basis for each Processing activity, e.g. vital interest for the Processing of medical records, and Consent for the Processing of Personal Data for restoring family links.

On the issue of Consent, it is important to recognize that beneficiaries receiving aid may not be in a position to give it validly.[25] Consent is a freely given, specific and informed indication that a Data Subject agrees to the Processing of their Personal Data. Similarly, while Humanitarian Organizations may use public interest as the legal basis for a programme that provides official identity credentials, failing to obtain Consent could lead to distrust among beneficiaries. They may feel that, because they have no say in the Processing of their Personal Data, their rights are being restricted. This is especially true when the data in question relate to their identity, which is an intrinsic part of a person's life.

25 See Section 3.2 – Consent.

13.6.2 PURPOSE LIMITATION AND FURTHER PROCESSING

Personal Data should be collected for specified, explicit and legitimate purposes, and Further Processing should only be undertaken when compatible with the initial purposes.[26] In this regard, it is important to consider whether Personal Data collected from a Data Subject in order to provide them with Digital Identity credentials under a specific humanitarian programme (e.g. with the aim of establishing beneficiaries' identity) could be further processed under a different programme (e.g. to provide assistance or services). Humanitarian Organizations should consider the following factors when applying the purpose limitation principle:[27]

- compatibility between the initial and further purposes;
- the context in which the data are collected, including the relationship between the individual and the controller;
- the nature of the data;
- potential consequences for beneficiaries;
- relevant safeguards (including data security safeguards, such as encryption or Pseudonymization).

As Digital Identity systems can have multiple uses, each with its own purpose, organizations must clearly specify all the purposes of a given Processing operation. If these purposes change or are subsequently clarified, the organization will need to give further notice to the Data Subjects.

13.6.3 PROPORTIONALITY

The principle of proportionality calls for the least intrusive means of Processing to be used in achieving the specified Processing aims. It is worth recalling that some humanitarian activities, such as the provision of aid, may require beneficiaries to prove only that they are entitled to receive the benefit (i.e. authentication), while others will demand a foundational (or "official") identity (i.e. verification). For this reason, Humanitarian Organizations, as Data Controllers, should consider which activities require identification and which ones do not. By limiting the Processing to authenticating the entitlement of beneficiaries to access services, organizations could avoid accidentally or unintentionally repurposing data or gathering unnecessary information, since beneficiaries' legal identities would not be collected or stored by the organization in the first place. In cases where authentication or identification is needed, organizations should also consider how much data they require, and of what type. For example, when using biometric data, organizations should process the least data points possible (e.g. one fingerprint instead of ten).

26 See Chapter 2: Basic principles of data protection.

27 EDPS, *Opinion on the Proposal for a Regulation Establishing a Single Digital Gateway and the 'Once-Only' Principle*, 9–10.

13.6.4 DATA MINIMIZATION

Humanitarian Organizations should only collect and process the minimum amount of data they need to fulfil the purpose of the Processing. For that reason, they must fully understand what information they need from beneficiaries before implementing any identification system that processes Personal Data. If an organization establishes that proving entitlement only is sufficient (i.e. authentication), it should not collect or process identity information in any way.

13.6.5 DATA SECURITY

Digital Identity systems such as the one envisaged in scenario 3 could allow beneficiaries to store their Personal Data on their own devices. The same applies to initiatives designed to provide an identity to those who lack identity documents. In such cases, malicious individuals or organizations would, in theory, only be able to access this information if they were able to breach device security. Yet beneficiaries could also be physically coerced into handing over their devices.

In other cases, such as the ones mentioned in scenarios 1 and 2, Humanitarian Organizations may store Personal Data in their own databases as part of a Digital Identity programme. These databases could become a target for malicious individuals or organizations. Consequently, Humanitarian Organizations must ensure that their Digital Identity systems preserve the confidentiality, availability and integrity of data in their systems and, in doing so, adequately protect the data from misuse, Data Breaches and liabilities.[28] Furthermore, the sensitive nature of certain types of Personal Data will generally require a very high level of security. Encryption techniques such as secret sharing (also known as secret splitting) systems can help increase security. In such systems, data are encrypted and the key is fragmented between multiple parties, which then need to work together to decrypt the data (e.g. different Humanitarian Organizations, as envisaged in scenario 3), thereby avoiding a single point of failure. Under this arrangement, the key can easily be destroyed if needed, since deleting a certain number of fragments (the number varies from system to system) would mean the data could no longer be used.

When implementing identity programmes, Humanitarian Organizations should also consider the security measures adopted by any partners. For instance, if beneficiaries' information is shared with other bodies or organizations, they must have appropriate security measures in place to protect the data and avoid the harmful consequences of a Data Breach.

28 Strategy & Research team, "Identity in a Digital Age", 25.

13.6.6 DATA RETENTION

Personal Data should be retained for a defined period, which should be no longer than is necessary for the purpose of the Processing. Where the main purpose of the Processing is to provide basic humanitarian assistance in the form of food, shelter and medical care, Personal Data should only be retained for as long as is needed to provide that assistance. Yet the situation is more complicated for Digital Identity programmes that seek to provide a form of identity credentials for beneficiaries who lack identity documents, since beneficiaries may wish to continue using their identity – which replaces or serves as an identity document – throughout their entire lives, as well as updating their status or situation as time passes. Here, determining an appropriate data retention period can prove challenging. Humanitarian Organizations should, however, provide an initial indication of the retention period that is consistent with the initial purpose for which the data are being collected. Once this period ends, organizations involved in programmes of this type should conduct periodic assessments to determine whether they still need to retain the data. Another option would be to allow beneficiaries to decide whether their data can be retained.

13.7 INTERNATIONAL DATA SHARING

Depending on the technical solution and the design chosen, data processed in Digital Identity systems may routinely flow across national borders. In scenario 3 above, for instance, multiple organizations may share information with each other, or beneficiaries may share their data with multiple organizations simultaneously. International Data Sharing raises data protection concerns.[29] Although some jurisdictions have recognized protection arrangements (such as the use of contractual clauses), Humanitarian Organizations operating Digital Identity programmes may struggle to implement these arrangements in practice because the system may involve multiple parties in different locations. As a general rule, Humanitarian Organizations are advised to take whatever steps they can to ensure that any transfer of Personal Data to a Third Party (and any subsequent onward transfer) does not lower the level of protection of individuals' rights. Because organizations are liable for all data transfers they conduct, they are responsible if data are unlawfully shared with other organizations in the envisaged scenario. Beneficiaries' Consent, however, could be an appropriate legal basis for organizations to transfer data in some situations. As mentioned above, however, it is questionable whether beneficiaries receiving aid can always give valid Consent.[30] In such cases, a different legal basis will have to be identified.

29 See Chapter 4: International Data Sharing.

30 See Section 3.2 – Consent.