SPACE Social Protection Approaches to COVID-19: Expert advice helpline

LINKING HUMANITARIAN & SOCIAL PROTECTION INFORMATION SYSTEMS IN THE COVID-19 RESPONSE AND BEYOND

EMRYS SCHOEMAKER, WITH REVIEWS FROM VALENTINA BARCA, DANIEL LONGHURST, REBECCA HOLMES AND EXPERTS ON THE SOCIAL PROTECTION APPROACHES TO COVID-19: EXPERT ADVICE HELPLINE (SPACE) - CONTACT: SPACE@DAI.COM

August 2020

This briefing document was developed alongside others – most importantly a Strategy Decision Matrix and a Delivery System Decision Matrix – as a technical tool used to structure an independent and unbiased analysis of COVID-19 response options. It does not necessarily represent FCDO or GIZ views or policies. It builds on two FCDO supported publications: Goodman et al, 2020, Review And Analysis Of Identification And Registration Systems In Protracted And Recurrent Crises, DAI/Caribou Digital and Schoemaker et al. 2018, and Identity at the Margins, Caribou Digital.

This note provides a background briefing and five key questions for humanitarian programme staff to consider when making decisions regarding the use of their Information Systems in COVID-19 responses, and beyond. It focuses in particular on contexts of transition from humanitarian to longer-term, state-led social protection systems. It has been written to accompany and complement a forthcoming SPACE piece focused exclusively on social protection information systems.

These issues, and contexts, are complex and raise challenging questions, some of which are beyond the scope of this document – including the challenge of reforming technology and data use by stakeholders outside the influence of aid actors. These challenges remain an ongoing discussion amongst practitioners and other stakeholders.

SPACE recommends the following, based on five underlying questions (see section 4):

- From efficiency to 'digital dignity': broaden scope of Value for Money (VFM) considerations when designing and transitioning information systems, beyond efficiency and limited abbreviations of effectiveness – instead focus on equity, and considerations linked to 'digital dignity' and protection, and evaluate trade-offs explicitly;
- From 'single' systems to standards and interoperability between systems: consider carefully the benefits and risks of creating 'standalone' versus interoperable registries/systems, noting that interoperability is often more feasible and preferable especially in FCAS and contexts of transition;
- From 'blind faith' to critical consideration of sharing information and technologies: consider opportunities and implications of different approaches to sharing information and technologies – assess different kinds of information access and different kinds of technologies, and what these imply;
- From 'firefighting' to anticipating and pre-empting inevitable risks – pragmatically: anticipate inevitable risks and implications and pre-empt these with appropriate planning and budgetary considerations, while adopting a pragmatic, realist approach to risk mitigation. Consider mitigating risk through a Do No Harm approach, including measures such as

beneficiary literacy for informed consent and data rights; data protection by design; political risk analysis; etc. Also acknowledge that 'ideal' approaches to managing risk are demanding. Although we recommend optimum approaches, implementation is likely to adopt a minimally sufficient, progressively realised, sequential approaches – though shouldn't detract from pursuing the highest possible standards in the future.

- From 'piecemeal' support to ecosystem building: realising what counts is the broader government context and its 'building blocks'

BOX 1: ACRONYMS

API	: Application Programming Interface
DPIA	: Data Protection Impact Assessment
EU	: European Union
FCAS	: Fragile and Conflict Affected States
GDPR	: General Data Protection Regulation
HA	: Humanitarian Assistance
HXL	: Humanitarian Exchange Layer
ICT	: Information Communication Technologies
ISPA	: Interagency Social Protection Assessments
MIS	: Management Information System
NGO	: Non-Governmental Organisation
SP	: Social Protection
SPIAC-B	: Social Protection Inter-Agency Cooperation Board
UN	: United Nations
UUID	: Unique User Identity
VfM	: Value for Money

1 WHAT ARE INFORMATION SYSTEMS, AND WHAT ROLE DO THEY PLAY IN SOCIAL PROTECTION?

1.1 What are information systems?

This brief uses this broad, catch-all definition to refer to the so-called Management Information Systems (MIS) and Identification systems (see below) that together enable the digital flow and management of information within the humanitarian and social protection sectors, and between these sectors and other sectors such as education and health. From a practical point of view, digital information systems for humanitarian response and social protection are the product of a set of 'components' that work together as a system. These components[1] include the ICT infrastructure, software applications, the underlying registry/database, the human resources – and the institutional and political setting in which these components exist. They are critical in managing public, development and humanitarian services.

[1] Richard Chirchir and Valentina Barca, 'Building an Integrated and Digital Social Protection Information System', Technical Paper (Bonn: GIZ / DFID, January 2020), https://socialprotection.org/sites/default/files/publications_files/GIZ_DFID_IIMS%20in%20social%20protection_long_02-2020.pdf

BOX 2: FOUNDATIONAL VS FUNCTIONAL IDENTIFICATION SYSTEMS

There are two kinds of identification systems – foundational and functional. Foundational ID systems provide general identification of the population, such as civil registries, national IDs, and population registers. These have a larger population. Functional identification systems manage identification for a particular service or transaction, such as voting, tax administration, social programmes – and have a smaller, defined population. The lack of interconnection or universal coverage can cause problems for programme managers (e.g. duplication, incomplete population) and for individuals (multiple registration, inconsistent data treatment, exclusion from service access). This is particularly the case for already marginalised and vulnerable groups - e.g. women, girls, refugees and disabled – who have lower coverage of IDs and birth registration. An ecosystem approach can help provide a holistic view to mitigate these blind-spots.

1.2 What role do these play in Humanitarian relief and Social Protection?

Information systems are critical to the delivery of benefits and services because the ability to register and identify recipients underpins everything in a targeted distribution system. In humanitarian contexts, data collection for these systems is often the first contact point between crisis-affected populations and responders. In humanitarian contexts data is often collected when people are at their most vulnerable and their options are limited.

An effective information system is expected to better serve the needs of the people, by focusing on inclusion; efficiency and effectiveness; accuracy and integrity; accountability and citizen empowerment and stakeholder coordination. These benefits are part of the wider vision of digital ID and inclusion that international development and private sector engagement is orientating towards.

2 WHY FOCUS ON LINKING INFORMATION SYSTEMS?

2.1 Recent trends prior to COVID-19

Growing interest in the links between humanitarian aid and social protection[2] as well as recent trends in the delivery of aid (increasingly via cash transfers)[3] have led to increased focus on the technologies and specifically data and information systems involved in the delivery of assistance to households. The rationale behind this push – according to recent research – has been a focus on increased 'effectiveness' and 'efficiency', both for institutions and individuals,

[2] For example, the UN and the World Bank have set up the New Way of Working, the OECD has made the nexus a priority and DAC members are showing some signs of changing how they fund programmes. The World Humanitarian Summit 2016 committed to reinforce, rather than replace, national and local systems.

[3] For example, the Grand Bargain and the Good Humanitarian Donorship initiative have all made commitments to further the use of cash transfers. Similar trends are also notable in the social protection sector.

more than other core Value for Money considerations such as equity and other advantages and trade-offs[4]. In practice, this has translated into:

- **A trend towards digital cash in aid delivery introducing digital technologies to manage identification distribution and management.** Aid is increasingly delivered digitally (though it remains dwarfed by in-kind assistance). Cash and voucher assistance grew as a percentage of international humanitarian assistance from 7.9% in 2015 to 17.9% in 20195. This move increases data collection to meet Know Your Customer (KYC) and anti-money laundering (AML) obligations[6], that potentially adversely impact beneficiary privacy.
- **A push for greater interoperability *within* the humanitarian sector and with private sector providers.** Increased interoperability could form the basis of a coordinated response (collectively aiming to achieve the same outcomes, without overlap and duplication – sharing basic information on who, what, where, when). This is an important area of work with a great deal of activity (see Box 3 for more) but is *not* the focus of this paper.
- **A push for interoperability *beyond* the humanitarian sector, with government-led Social Protection (SP).** The rationale being that an integrated humanitarian sector response could better support transition to state-led systems. Alternatively, a centralised humanitarian transfer information system (or parts of such a system, or just data from it) may form the basis of a longer-term/government-led Social Assistance Information System – supporting national capacity over time. This push must be read in the context of increasing investments in such systems by a vast number of governments worldwide, as extensively documented in recent literature.[7] There is also evidence of SP systems and data being relevant to humanitarian responses[8].

In this context there is also growing awareness of the risks. Recent data breaches[9], concerns amongst humanitarian actors[10], together with concerns about increasingly digital welfare states[11] have prompted concerns about biometrics, unnecessary data collection and technology security. As well as the risks posed by increasingly removing the human element from SP (or

[4] Goodman, R., 2020 Review And Analysis Of Identification And Registration Systems In Protracted And Recurrent Crises, BASIC - Better Assistance in Crises (DFID funded) here

[5] Jose Jodar et al., 'The State of the World's Cash 2020 - Cash and Voucher Assistance in Humanitarian Aid' (CALP, July 2020), https://www.calpnetwork.org/publication/the-state-of-the-worlds-cash-2020-executive-summary/.

[6] FATF (2012-2019), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France, www.fatf-gafi.org/recommendations.html; FATF (2020), Guidance on Digital Identity, FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

[7] Richard Chirchir and Valentina Barca, 'Building an Integrated and Digital Social Protection Information System', Technical Paper (Bonn: GIZ / DFID, January 2020), https://socialprotection.org/sites/default/files/publications_files/GIZ_DFID_IIMS%20in%20social%20protection_long_02-2020.pdf.

Lindert, Kathy, Tina George Karippacheril, Inés Rodríguez Caillava, and Kenichi Nishikawa Chávez, eds. 2020. Sourcebook on the Foundations of Social Protection Delivery Systems. Washington, DC: World Bank. doi:10.1596/978-1-4648-1577-5.

Philippe Leite et al., 'Social Registry Information Systems for Social Assistance (and Beyond): Framework, Definition, Typology, and Trajectories for Integration', 2016.

[8] Valentina Barca and Rodolfo Beazley, 'Building on Government Systems for Shock Preparedness and Response': 2019, 55.

[9] Ben Parker, 'Donor Details Hacked in NGO Data Breach', News, Aid and Policy (Geneva: New Humanitarian, 4 August 2020), https://www.thenewhumanitarian.org/news/2020/08/04/NGO-fundraising-database-hack; Nathaniel A. Raymond, Daniel P. Scarnecchia, and Stuart R. Campo, 'Humanitarian Data Breaches: The Real Scandal Is Our Collective Inaction', Opinion, Solutions and Innovations (Geneva: New Humanitarian, 8 December 2017), https://www.thenewhumanitarian.org/opinion/2017/12/08/humanitarian-data-breaches-real-scandal-our-collective-inaction.

[10] ICRC Data Protection Framework: https://www.icrc.org/en/document/icrc-data-protection-framework

[11] Alston, P., 2019 Report of the Special rapporteur on extreme poverty and human rights: Digital Welfare State, OHCR / A/74/48037 here

HA) processes and decision making, and some of the inherent faults and biases in algorithmic and automated systems and processes[12].

BOX 3: TRENDS TOWARDS INTEGRATION WITHIN THE HUMANITARIAN SECTOR

This trend is evident in the Joint Donor Statement on Humanitarian Cash Transfers, which envisages "solutions whereby interoperable, non-proprietary, data registries can allow a level of data sharing between humanitarian agencies and private sector service providers"[13]. The UN is pushing for common approaches to cash and the scale-up of collaboration amongst agencies, from "no-regrets moves" including information sharing, such as the exchange of data between WFP Somalia and UNHCR Kenya to allow Somali returnees from Kenya to continue receiving cash entitlements. At the other end of the spectrum, it sees "game-changers" as solutions where delivery is co-designed, or one UN agency uses services of another, such as a central interoperable data repository; or UNICEF and WFP both utilising SCOPE for delivery[14].

2.2 The role of COVID-19

The COVID-19 pandemic, and the ensuing scale-ups of humanitarian and social protection responses, have accelerated this interest in digital systems for the delivery of assistance, for several reasons:

- **The digitalisation of delivery has been central to the COVID-19 response in many countries,** enabling rapid and remote registration and enrolment of caseloads – and payment of beneficiaries[15] in the face of severe movement restrictions. Specifically, countries with advanced digital identification and government-to-person (G2P) payment systems have been able to identify populations reliably and remotely, and to make emergency cash transfers to eligible or targeted population groups[16]. For example, in Thailand, where more than 28 million people applied for a new benefit for informal workers affected by the pandemic, the government was able to filter out those who would receive assistance from other schemes[17].
- **The widespread focus on 'pay now, verify later'** has allowed the release of assistance faster than the bottlenecks imposed by identity and eligibility verification[18] - for example many states in the US reported initial claims growth of over 1,000%[19].
- **The rapid deployment of digital technologies to support contract tracing, health status and innovative social protection targeting methodologies** such as mobile phone usage

[12] Feeny, Thomas, Elson, Olivia, 2019, Artificial Intelligence in International Development – A Discussion Paper. The International Development Innovation Alliance (IDIA) / Results for Development

[13] Joint Donor Statement on Humanitarian Cash Transfers, June 2019, Cash Learning Partnership here

[14] BCA, 2018 Cash Digitization: UN Collaboration, Coordination, and Harmonization Opportunities here

[15] Jose Jodar et al., 'The State of the World's Cash 2020 - Cash and Voucher Assistance in Humanitarian Aid' (CALP, July 2020), https://www.calpnetwork.org/publication/the-state-of-the-worlds-cash-2020-executive-summary/.

[16] World Bank (2020) Scaling up social assistance payments as part of the COVID-19 pandemic response here; CGDEV (2020) Digital Technology in Social Assistance Transfers for COVID-19 Relief: Lessons from Selected Cases here;

[17] Michal Rutkowski et al., 'Responding to Crisis with Digital Payments for Social Protection: Short-Term Measures with Long-Term Benefits', *World Bank Blogs - Voices* (blog), 31 March 2020, https://blogs.worldbank.org/voices/responding-crisis-digital-payments-social-protection-short-term-measures-long-term-benefits.
Mari Pangestu, 'Harnessing the Power of Digital ID | by Mari Pangestu', *Project Syndicate*, 19 August 2020, sec. Technology & Society, https://www.project-syndicate.org/commentary/digital-identification-systems-promote-inclusive-economic-growth-by-mari-pangestu-2020-08.

[18] 'Pay Now, Verify Later to Loosen the Unemployment Insurance Bottleneck', *Economics for Inclusive Prosperity* (blog), accessed 31 August 2020, https://econfip.org/policy-brief/pay-now-verify-later-to-loosen-the-unemployment-insurance-bottleneck/.

[19] 'The Coronavirus Crisis Led to a Record-Breaking Spike in Weekly Unemployment Insurance Claims: An Estimated 3.4 Million Workers Filed for Unemployment Last Week', *Economic Policy Institute* (blog), accessed 31 August 2020, https://www.epi.org/blog/coronavirus-record-breaking-spike-in-ui-claims/.

data, often in ways that invade privacy and contravene existing regulation[20], has led to new guidance around proportionate, transparent and accountable and responsible data use[21].

The response to COVID-19 has fuelled interest in digital identity, payment and governance systems as critical public infrastructure. It has also strengthened recognition of the challenges involved in the use of these systems, for example differentials of mobile ownership and use of mobile payments, especially between men and women, and people with disability[22].

Now is the time to ensure that this interest and these recognitions are translated into digital architectures that enable social protection whilst protecting public interest, as discussed in the next Section.

3 KEY RECOMMENDATIONS EMERGING

3.1 From efficiency to 'digital dignity'

Digital information systems are commonly assumed to offer efficiency gains, but it's important to measure these claims, as well as focus on wider considerations, guided by the concept of 'digital dignity'[23]. There is increased interest in information systems because these are seen as offering the possibility of achieving more coherent and joined up responses, which are believed to lead to increased efficiency through reduced processing cost, fraud reduction and increased accuracy[24]. Of course, this has been – and can be the case. However, rather than a narrow focus on efficiency, it's important to focus VfM analyses on a wider understanding of effectiveness – which could be framed as 'digital dignity'.

The concept of 'digital dignity' recognises the importance of beneficiary rights, and that individuals need to be respected as active data agents, and not purely as a passive data subject. They need to be given the opportunity (and capacity) to request data erasure and rectification, as well as be informed about data use and implications – and crucially to manage consent, especially as interoperability introduces changes to data use. Consent is a fundamental right in data protection law and regulations, though its complexity is increasingly recognised – see for example ICRC's position on consent in their Data Protection Policy. Digital dignity thus provides

[20] See for example Privacy International's tracker of privacy threatening interventions: https://privacyinternational.org/examples/tracking-global-response-covid-19

[21] OECD, 'Ensuring Data Privacy as We Battle COVID-19', OECD Policy Responses to Coronavirus (COVID-19) (Paris: OECD, 14 April 2020), http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/.

[22] Bill and Melinda Gates Foundation, World Bank Group, CGAP, August 2020, Women's World Banking, DIGITAL CASH TRANSFERS IN THE TIME OF COVID 19 - Opportunities and Considerations for Women's Inclusion and Empowerment. https://www.cgap.org/research/publication/digital-cash-transfers-times-covid-19-opportunities-and-considerations-womens

[23] Digital Dignity in Practice: Existing Digital Dignity Standards, Pursuing Digital Dignity and Current Gaps in Digital Dignity https://www.alnap.org/help-library/digital-dignity-in-practice-existing-digital-dignity-standards-pursuing-digital-dignity

[24] Goodman, R., 2020 Review And Analysis Of Identification And Registration Systems In Protracted And Recurrent Crises, BASIC - Better Assistance in Crises (DFID supported) here

a framework to consider data protection (vulnerability context and risk of unauthorised access and unintended use of data); Value for Money (measures beyond efficiency in systems design, with more focus on effectiveness and equity); Do No Harm (the implications and risks for civilian protection) and Leave No-One behind (inclusiveness of transfer modalities, targeting approaches).

3.2 From 'single' systems to standards and interoperability

Efforts to improve data sharing are welcome but should be pursued through standards and interoperability rather than 'single' or specific information systems and registries. There is a widespread perception that the efficiency goals promised by specific information systems can best / only be achieved through a single, consolidated system that integrates multiple services[25], leading to demand for different organisations to use an existing shared system – a common example is the Lebanon One Unified Inter-Organisational System for E-card (LOUISE), which enabled UNHCR, WFP, UNICEF and the Lebanese Cash Consortium (LCC) of NGOs to share a common platform for cash and voucher assistance.[26] While this approach introduced new efficiencies it did not introduce true interoperability between LOUISE member systems. Further value can be achieved through supporting interoperability by agreeing common standards for data collection and management.

This is particularly important when considering a future transition to state-led social protection systems, which often rely on the use of multiple systems[27]. Establishing standards that enable interoperability can support the transition of systems as well as data from humanitarian to social protection systems. When social protection systems are built to accommodate humanitarian systems and data, ensuring standards maintain the principles of Digital Dignity can help uphold these principles across the nexus between humanitarian and social protection.

Greater collaboration and data sharing within the humanitarian sector should be supported through standardisation in the form of interoperability of secure information systems. There are existing examples of standards for data exchange in the humanitarian sector, such as the Humanitarian Exchange Language (HXL)[28]. Interoperability to support future transitions to state-led-led social protection systems should also be furthered through opening 'closed' systems, such as SCOPE, ProGres, PRIMERO and BRAVE, using APIs to enable third parties to unlock data monopolies and enabling the development of further services. Other sectors have also made progress in this direction (Box 4).

BOX 4: LESSONS FROM OTHER SECTORS PROVIDE INSIGHTS AROUND STANDARDS AND TECHNOLOGIES THAT SUPPORT INTEROPERABILITY.

[25] Goodman, R., 2020 Review And Analysis Of Identification And Registration Systems In Protracted And Recurrent Crises, BASIC - Better Assistance in Crises (DFID supported) https://medium.com/caribou-digital/digital-identity-and-management-information-systems-for-humanitarian-and-social-protection-response-b1b25e5623a2

[26] Isabelle Pelly and Helene Juillard, 'Lebanon One Unified Inter-Organizational System for E-Cards (LOUISE) Learning Review' (Keyaid Consulting: for UNICEFon behalf of the LOUISE member agencies, February 2020).

[27] Valentina Barca, 'Integrating Data and Information Management for Social Protection: Social Registries and Integrated Beneficiary Registries.' (Canberra: Commonwealth of Australia, Department of Foreign Affairs and Trade., 2017), http://dfat.gov.au/about-us/publications/Documents/integrating-data-information-management-social-protection-full.pdf.

[28] HXL is a shared standard for data categorisation, such as the Humanitarian Exchange Layer (HXL[28]), to which UNHCR, IOM, IFRC and others are signatories, as well as the Humanitarian Data Exchange (HDX[28]) which employs HXL and is used by over 260 organisations in various ways. See ttps://hxlstandard.org/; https://data.humdata.org/

The health care sector has seen multiple efforts at developing industry-wide frameworks for sharing patient identity and medical information – for example the Joint Learning Network (JLN) established a cross-learning platform for countries that are in the midst of implementing health reforms, that produced a set of practical common information, tools, and resources, which can guide country decision-makers as they develop national-level health insurance information system plans. A similar common platform should be established amongst humanitarian and social protection actors.

There are also lessons about how specific technologies can enable or constrain interoperability. For example, the digital identity sector has suffered from 'vendor lock-in' to proprietary systems that result in increased cost and reduced flexibility to accommodate changes. These risks can be mitigated by using open standards, interoperability in architecture, and strong procurement processes that avoids unnecessary conditions in the choice of technology and supplier. Examples include open standards approaches such as the Open Identity Exchange and open source software initiatives such as the Modular Open Source Identity Platform (MOSIP) and the open source civil registration platform OpenCRVS.

3.3 From 'blind faith' to considering the opportunities and implications of sharing information and technologies

No matter what, whether sharing data or information, it's vital to assess some key considerations that emerge when sharing data and technologies across different actors – especially between humanitarian and state-led systems. These are summarised below, stressing implications will vary depending on the answers to your questions.

Table 1. Considerations for sharing data and technology

If sharing	Consider whether:
Data Particularly beneficiary lists, but also 'third party' data sources such as existing social registries (health, education) or third-party mobile phone data)	The information shared has the following permissions: • create/write: is the data controller and information trustworthy? • read/retrieve: who has access? Are access records accountable? • update/write: are updates recorded? Are they reversable? • delete: who has authority? Are deletions reversable? • real time, batch processing: is original data preserved? Is batch data monitored? No matter what: If sharing with new system or programme, to maintain user consent, new consent is required to authorise transfer of data to a new system or programme.[29]
Technologies	• are technologies open source or proprietary? • are systems adaptable (e.g. agile design)? • are systems dynamically accessible (e.g. APIs)? • are data formats interoperable (e.g. HXL)?

3.4 From 'firefighting' to anticipating and pre-empting inevitable risks – pragmatically

[29] Goodman, R., 2020 Review And Analysis Of Identification And Registration Systems In Protracted And Recurrent Crises, BASIC - Better Assistance in Crises (DFID supported) https://medium.com/caribou-digital/digital-identity-and-management-information-systems-for-humanitarian-and-social-protection-response-b1b25e5623a2

The use of digital information systems introduces new risks and potential harms. It's important for practitioners to reflect on whether and when it is suitable to interconnect databases. In many contexts there is limited legal, technical, ethical and programmatic knowledge and guidance to adequately answer this question, which can lead to risky or inappropriate decisions. It may not be appropriate to connect databases or create a standalone database, unless certain pre-conditions are met.

Data breaches are inevitable[30], and any support to the development of information systems requires appropriate measures to mitigate institutional and individual risk. The collection and management of personal data presents risks, which increases as more data are collected and as more data management is centralised. There have been a number of recent examples – such as the hacking of Red Rose - a provider of a closed loop registration and transfer software used by a range of NGOs, and an unreported major breach of UN staff data in Geneva and Vienna in late 2019[31]. The inadvertent and deliberate leaking and sharing of personal and anonymised data is inevitable. This introduces fiduciary and reputational risk to institutions and to individuals through misuse of personal data – as well as risk to the broader humanitarian response, for example in the form of a loss of community trust and challenges to humanitarian access. Risks can be mitigated through a minimal data collection policy – see ICRC's Data Protection policy[32] and the EU guide to conducting Data Protection Impact Assessments (DPIA)[33] to inform assessment of risk and potential harms arising from data collection and management[34] and M&E requirements should be aligned with DPIA results.

Increased use of information systems requires commensurate capacity, systems and standards that better support data protection. The collection, storage and sharing of data in humanitarian settings carries heightened risks (threats, abuse, bias, corruption, loss of life) that are greater than other settings. These risks are heightened by the complexity of MIS and ID system, which is exacerbated by integration and interoperability, introducing new stakeholders, the private sectors, and technology actors such as cloud and financial service providers, potentially across several jurisdictions. The use of MIS and ID technology have uses and consequences that at present are poorly understood by many humanitarian practitioners, project managers and policy advisers. This is especially significant in contexts where enforcement mechanisms for legal and ethical frameworks are weak. However, there is growing recognition of the risks involved in processing personal data. Risk mitigation strategies include pausing the use of some technologies, for example, Oxfam concluded in a review of biometrics that the risks to beneficiaries from their use outweighed their benefits[35] while ICRC recommend biometric technologies that place beneficiary data on ID cards rather than centralised data bases.[36] More broadly, frameworks such as the Principles for Digital Development[37] and the Principles on Identification for Sustainable Development[38] provide helpful guidelines, though as they are voluntary and indicative are unenforceable, whilst the

[30] See for example: The New Humanitarian, Security lapses at aid agency leave beneficiary data at risk, 27 November 2017, https://www.thenewhumanitarian.org/investigations/2017/11/27/security-lapses-aid-agency-leave-beneficiary-data-risk

[31] https://www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack

[32] ICRC Data Collection Policy - https://www.icrc.org/en/publication/4261-icrc-rules-on-personal-data-protection

[33] See EU's GDPR DPIA guidelines: https://gdpr.eu/data-protection-impact-assessment-template/

[34] https://gdpr.eu/data-protection-impact-assessment-template/; see ICRC guidance on DPIAs, chapter 5 of the Data Protection handbook

[35] Engine Room, 2018 Biometrics in the Humanitarian Sector https://www.theengineroom.org/wp-content/uploads/2018/03/Engine-Room-Oxfam-Biometrics-Review.pdf

[36] ICRC Data Protection Framework: https://www.icrc.org/en/document/icrc-data-protection-framework

[37] https://digitalprinciples.org/

[38] https://id4d.worldbank.org/principles

European Union's General Data Protection Regulation (GDPR) is a recognised gold standard in enforceable data protection regulation – though beyond many humanitarian contexts, where the basics have to be addressed first.

Risk mitigation measures should therefore be adopted – acknowledging that your approach will have to be pragmatic: 'ideal' approaches to managing risk are demanding. Possible strategies may include:

- Processing of personal data in a distributed manner, such that personal data, biometric templates, and biometric images are always physically and logically separated from each other.
- Adopting privacy preserving technologies such as zero-knowledge proofs and hashed personal data (see Box 5) and adopting data minimisation and deletion policies (including deletion as a default after a certain time).
- Developing a full Data Protection Impact Assessment (DPIA) to help inform assessment of the risks and potential harms arising from data collection and management[39]
- Ensuring a privacy by design default approach to help ensure these are all integrated into plans and designs[40].

No matter what, the operating assumption must be that all collected data are likely to be exposed at some point. Even the most secure cryptographic technologies are at risk with contemporary computing advances.

BOX 5: PRIVACY INNOVATIONS

Zero-knowledge proofs (ZKPs) are mathematical methods used for verification without sharing or revealing underlying data[41] – enabling one party to prove to another party that they know a value x, without conveying any information apart from the fact that they know the value. For instance, Organisation A could state they have Beneficiary A in their system, without sharing the details of that Beneficiary with Organisations B.

'Hashed' personal data: Organisations such as ICRC and Mastercard are exploring approaches that create algorithmically generated encrypted 'hashes'[42] of biometric data – in other words, encrypted representations of personal data are used as proxies for the actual data, with the encryption algorithm being the proprietary technology that ensures data protection and security. Authentication and verification would be carried out by comparing the hashes, not the actual data – using a proprietary algorithm to match the hash presented by the beneficiary against the hash held by the organisation.

3.5 From 'piecemeal' support to ecosystem building

The short-term nature of humanitarian funding and lack of coordination with the broader social protection (and government) long-term vision risks resulting in a piecemeal approach that builds standalone, discrete systems that lack the wider components required to establish a digital ecosystem capable of supporting dynamic and responsive social welfare systems. An ecosystemic response encompasses the underlying digital identification and civil registration systems, the institutional and human capacity to manage and lead system reform and

[39] https://gdpr.eu/data-protection-impact-assessment-template ; see ICRC guidance on DPIAs, chapter 5 of the Data Protection handbook

[40] See Privacy by Design principles from the International Association of Privacy Professionals: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/

[41] 'What Are Zero-Knowledge Proofs?' Wired. Accessed 19 January 2020. https://www.wired.com/story/zero-knowledge-proofs/

[42] A hash converts one value to another, for instance a person's name becomes an identifying number

implementation, the legal and regulatory mechanisms to support data protection and system governance and engaged and knowledgeable population of system users. This wider ecosystem approach is holistic– and one that requires further guidance and support, as will be tackled in a forthcoming SPACE paper on 'digital backbones. Key steps will include, but not be limited to:

- Ensuring coverage and robustness of the underlying foundational digital identity system – this should be a design priority (see also World Bank, 2018).[43]
- Prioritising inclusiveness at every stage
- Ensuring appropriate legal and regulatory frameworks – specifically data protection legislations, grievance redress mechanisms, and public communication exercises – particularly to explain what and how data will be used, what people's rights are and what consent means.
- Strengthening human capacity – e.g. data protection officers. Failure to do so can limit success and sustainability.

4 KEY QUESTIONS TO ASK WHEN MAKING DECISIONS ABOUT LINKING DATA AND INFORMATION SYSTEMS ACROSS HUMANITARIAN AND SOCIAL PROTECTION

4.1 What is the nature of the intervention? Building for the long-term.

Defining the primary goal of the intervention can help inform what approach will be most appropriate. However, regardless of whether the intervention is a short-term emergency response or intended to support the transition from humanitarian to longer term state-led social protection, deployment should consider the potential for system integration, and appropriate data protection measures.

4.1.1 Short term response

In these cases, an existing, stand-alone system may be the easiest choice. However, most stand-alone systems are difficult to integrate with other systems and as a result offer limited capabilities for de-duplication and comparison against existing systems. While using existing stand-alone intervention specific information systems can enable rapid deployment and protect already collected data, ensuring the potential for integration should be part of choosing MIS and ID systems, especially as most humanitarian contexts are protracted.

[43] *ID4D Practitioner's Guide (English).* Identification for Development Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide

4.1.2 Longer-term response

In these cases, it is important to determine if the necessary financing, commitment and strategy is in place to support what can be a lengthy and complex process. Foundational systems and technologies can take years to develop and implement, while strengthening or reform of existing systems also takes time. If deduplication of multiple systems and beneficiaries in multiple programmes is needed, then some of kind a linked identification, such as a form of foundational ID, will be required. One way to achieve this is through linking several different ID numbers to a single foundational ID ("tokenization").[44] Building for future social protection also requires establishing digital systems that are resilient, sustainable and adaptive for future shocks. Best practice in social protection emphasises the importance of building national identification systems and strengthening, or establishing, civil registration and vital statistics systems, which are critical foundations for effective, inclusive social protection response.

The trade-offs to be resolved are between the speed and cost of implementation to meet short term needs, and the time and cost required to lay foundations for longer term programming and systems that can operate independently of external, donor support. Regardless, there is a need for further investment in building staff and partners' capacity and in appropriate consent mechanisms and processes. In practice, short term emergency response can become protracted, strengthening the case for longer term investment for all responses.

Things to do:

- Clarify interventions goals - specifically around longer term transition.
- Cost intervention - and ensure adequate funding and capacity for the medium-long term.

4.2 What is the political context?

Is the country context conducive to good data governance? This is important because personal data in Information Systems can make individuals vulnerable, so assessing the political and vulnerability context can help assess whether this data can be misused, and whether aligning with government systems as part of a longer-term transition is desirable. Political leadership and ownership are vital to new or reformed identification systems. These assessments can guide efforts to mitigate risks to local communities and promote digital dignity.

4.2.1 What are the politics and vulnerability

Do the authorities (state or non-state actor) with control over the MIS have an interest in misusing the data? For example, in the context of fragile or conflict affected states, political authorities are often a party to the conflict and see opportunities in using the data to further their own interests[45]. Identifying specific groups that are already vulnerable can help anticipate who may be further at risk from being excluded from a Management Information System - often women and girls, people with disability, migrants or refugees and other minority groups. Data and identification systems can exacerbate exclusion and risk - for example through heightening barriers to access services or increasing visibility for vulnerable groups[46]. A

[44] Bhadra, S., 2019 Five Surprisingly Consequential Decisions Governments Make About Digital Identity, Omidyar Network https://medium.com/positive-returns/five-surprisingly-consequential-decisions-governments-make-about-digital-identity-bb37d4d128db

[45] Goodman, R., 2020 Review And Analysis Of Identification And Registration Systems In Protracted And Recurrent Crises, BASIC - Better Assistance in Crises (DFID funded) https://medium.com/caribou-digital/digital-identity-and-management-information-systems-for-humanitarian-and-social-protection-response-b1b25e5623a2

[46] Caribou Digital, Kenya's Identity Ecosystem, Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2019 https://www.cariboudigital.net/wp-content/uploads/2019/10/Kenyas-Identity-Ecosystem.pdf

gender equality and social inclusion risk and vulnerability assessment[47] can help identify and find ways to overcome these possible risks of exclusion (see GESI implementation paper).

4.2.2 Is there ownership and choice

Deploying the right technology requires ownership and flexibility for system owners to make appropriate, meaningful choices over every aspect of information systems - in terms of policy direction, technology, and data collection and management. Barriers can include vested interests or technological constraints - for example, there is widespread recognition that 'vendor lock in' can reduce choices and increase costs. Examples of mitigating measures include support to open source alternatives, such as MOSIP[48] and OpenCRVS[49], open source national identity and civil registry systems, respectively.

Things to do:

- Conduct a MIS/ ID risk and vulnerability assessment which collects, and analyses disaggregated data to identify risks by gender, age, disability etc. – e.g. ISPA Assessment[50]; National ID Ecosystem Mapping tool[51].
- Identify political leadership and ownership: integrate leaders / owners into planning.
- Enable systems owners to make choices: delegate responsibility, e.g. for system choice.
- Strengthen individual agency: increase individual awareness and knowledge of systems, data use and rights, particularly through partnership with local organisations.

4.3 What is the policy context?

Once intervention objectives and the political context are clear, it is helpful to understand the wider policy context:

4.3.1 Are policy objectives shared?

Firstly, it is helpful to know if other stakeholders – particularly government – share the same policy objectives, as shared policy objectives can form the basis for collaboration, which is particularly important for the longer-term work of building data systems that can serve as the foundation for nexus-based transitions to state-led social protection programmes. Within the humanitarian system, different humanitarian organisations have different mandates that provide the basis for different approaches to data collection and processing, and the systems to support this.[52] For example, some organisations have legal commitments to share datasets, while others have made commitments to limit data sharing. Clarity around the policy objectives and context can inform choices such as whether to adopt standalone or shared, interoperable information systems.

[47] See Caribou Digital's National Identity Ecosystem Mapping tool: https://medium.com/caribou-digital/emrys-schoemaker-and-tom-kirk-introduce-caribou-digitals-new-project-to-develop-an-identity-8ec31ba61c9b

[48] MOSIP (Modular Open Source Identity Platform) is a vendor neutral, interoperable open source identity platform: https://www.mosip.io/about.php

[49] OpenCRVS is an open source, free to use civil registration platform: https://www.opencrvs.org/

[50] ISPA, Identification Systems for Social Protection: What Matters Guidance Note, ISPA https://ispatools.org/id/

[51] See Caribou Digital's National Identity Ecosystem Mapping tool: https://medium.com/caribou-digital/emrys-schoemaker-and-tom-kirk-introduce-caribou-digitals-new-project-to-develop-an-identity-8ec31ba61c9b

[52] Goodman, R., 2020 Review And Analysis Of Identification And Registration Systems In Protracted And Recurrent Crises, BASIC - Better Assistance in Crises (DFID supported) https://medium.com/caribou-digital/digital-identity-and-management-information-systems-for-humanitarian-and-social-protection-response-b1b25e5623a2

4.3.2 Is there political will and leadership?

This is equally important in relation to decisions about systems that might support transitions to integrated, state led social protection systems. Integrated approaches to information and data management are based on political will, so assessing whether there is a shared set of policy objectives is critical if data integration is part of a long-term transition from humanitarian to social protection. Within the humanitarian sector, are potential humanitarian actors coordinating together, do they have appropriate agreements around roles, responsibilities and data management in place? In the context of transitions to domestic social protection systems, joined up governance can support a systems approach and the potential for an integrated approach to social protection.[53]

4.3.3 Who owns the system?

The policy context will also determine where the data system can or should be situated. The institutional home of the Management Information System is a critical early decision because it impacts its ability to scale beyond the first use case.[54] According to the 2016 World Bank ID4D dataset, the Ministry of Interior or Home Affairs runs the ID system in 109 countries. The different mandates and data processing guidelines for humanitarian organisations also have implications for how and whether organisations such as WFP, UNHCR and ICRC are able to share data and data systems.

Things to do:

- Assess key stakeholder's policy positions and political will.
- Clarify system ownership - current or intended.

4.4 What is the legal and regulatory context?

The legal and regulatory framework that applies to personal data protection is an integral part of any information and identification system, and best practice guidance recommends an assessment of an ID systems governance.[55] This should include attention to risks, as the OHCR notes that the risks of the digital transformation of the welfare state have not received the same attention as the benefits, and without care, risks 'stumbling zombie-like into a digital welfare dystopia'.[56] As the guiding principles on Extreme Poverty and Human Rights notes, States should: (a) Revise legal and administrative frameworks to protect persons living in poverty from inappropriate intrusion into their privacy by the authorities. Surveillance policies, welfare conditionalities and other administrative requirements must be reviewed to ensure that they do not impose a disproportionate burden on those living in poverty or invade their privacy.[57] Political accountability, legal independence and data and privacy protection are elements of a legal and regulatory context that can mitigate against the misuse of personal data.

[53] Valentina Barca and Richard Chirchir, 'Single Registries and Integrated MISs: De-Mystifying Data and Information Management Concepts' (Australia Department of Foreign Affairs and Trade, 2014), http://socialprotectionet.org/sites/default/files/report-dfat-single-registries-report_0.pdf.

[54] Bhadra, S., 2019 Five Surprisingly Consequential Decisions Governments Make About Digital Identity, Omidyar Network https://medium.com/positive-returns/five-surprisingly-consequential-decisions-governments-make-about-digital-identity-bb37d4d128db

[55] ISPA, Identification Systems for Social Protection: What Matters Guidance Note, ISPA https://ispatools.org/id/

[56] Alston, P., 2019 Report of the Special rapporteur on extreme poverty and human rights: Digital Welfare State, OHCR / A/74/48037 https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx

[57] OHCHR (Office of the High Commissioner for Human Rights). 2012. Guiding Principles on Extreme Poverty and Human Rights. Geneva: OHCHR.

4.4.1 Rule of law, or rule by law?

It's important to assess whether the law is independent and able to hold political authorities accountable, or whether it is used by authorities to further their own interests - this will indicate whether any existing laws and regulations will be meaningful and upheld. Where the law is subservient to political authority, research indicates that ID systems can be exploited for political gain.[58] Where data risks are identified, approaches should minimise data collection where possible.

4.4.2 Does the regulatory context allow for data systems integration?

Some countries effectively prevent integration in order to minimise the potential for linking different databases and thus mitigate the risk of data theft or misuse.[59] If integration is required but is prevented by regulations, then special legal mechanisms, with appropriate oversight, will be required together with amendments to the legal framework.

4.4.3 Is data protection legislation in place, and appropriate?

In many humanitarian contexts, particularly fragile and conflict affected states, there may be limited or no data protection and privacy regulations in place. The Principles on Identification for Sustainable Development note that trust and individual rights may be compromised "in the absence of strong data protection laws, regulatory frameworks, and practices".[60] Inconsistent or lacking regulatory frameworks can be barriers to developing integrated or interoperable systems.[61] In the transition from humanitarian to social protection responses, particularly when the goal is an integrated approach that connects different databases, the risk of data breaches or unintended use is greater.[62] It can be helpful to ensure that humanitarian actors have appropriate data protection policies in place, and to ask whether authorities follow best practice around data processing and protection – a good source is the World Bank's Identification for Development (ID4D) Digital Identity Diagnostics, which exist for a growing number of countries[63].

4.4.4 Are regulations and best practice consistent?

Even where regulations or best practice are in place, there may be contradictions in recommended best practice for data protection in humanitarian and social protection programmes. For example, biometrics use is widespread in humanitarian response with most systems holding data in centralised databases, yet ISPA best practice is for biometric data to be stored exclusively as encrypted templates on devices such as smart cards rather than central databases. [64] It can be helpful to assess whether they follow the International Association of Privacy Professionals Fair Information Practices[65]

[58] Mushtaq Khan and Pallavi Roy, 'Digital Identities: A Political Settlements Analysis of Asymmetric Power and Information', Working Paper, ACE: Anti-Corruption Evidence (London: SOAS, October 2019). https://goodid-production.s3.amazonaws.com/documents/ACE-WorkingPaper015-DigitalIdentities-191004.pdf

[59] ISPA, Identification Systems for Social Protection: What Matters Guidance Note, ISPA https://ispatools.org/id/

[60] World Bank (2017). Principles on identification for sustainable development. Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-English-ID4D-IdentificationPrinciples.pdf

[61] Valentina Barca, Paul Makin, and Apurva Bamezai, 'Integrating Digital Identity into Social Protection An Analysis of Potential Benefits and Risks', Discussion Paper (Oxford, UK: Oxford Policy Management, 2018).

[62] Barca V. (2017). Integrating data and information management for social protection: social registries and integrated beneficiary registries. Canberra: Commonwealth of Australia, Department of Foreign Affairs and Trade; Hosein G. & Nyst C. (2013). Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives are Enabling Surveillance in Developing Countries. London: Privacy International.

[63] See: https://id4d.worldbank.org/country-action/id4d-diagnostics

[64] ISPA, Identification Systems for Social Protection: What Matters Guidance Note, ISPA https://ispatools.org/id/

[65] IAPP, Fair Information Practice Principle, https://iapp.org/resources/article/fair-information-practices/

Things to do:

- Assess legal and regulatory context - both stated and practiced. Check if there is a WB ID4D Diagnostic, if not, assess using ISPA guidelines.
- Assess implications of regulations for intervention / system goals (e.g. integration), by analysing conclusions from ID4D Diagnostic, National Identity Ecosystem Map.
- Assess data protection practices: check against Fair information Practices[66].

4.5 What is the technological context?

The policy perspective shapes the available technological choices. Short term emergency and humanitarian response are characterised by fragmented identity and data management systems[67] - for example in Somalia there are 13 different registration systems used to support cash transfers. [68]

4.5.1 What functionality exists in the current ecosystem?

For longer term transitions to social protection responses, the first step is to take stock of the existing system or systems that could be used or leveraged.[69] This should include assessing what foundational systems exist - for example, the national identity systems and civil registration and vital statistics CRVS. These are important because an existing Unique User Identifier (UUID) can serve as the foundation for verification and authentication across databases. Each system should be assessed to determine the functionality of registration (human resource, processes, technology) and management (human capacity, defined roles and responsibilities) – see ISPA assessment guidelines for detail. Many places, particularly fragile and conflict affected states, lack these foundational systems and the functionality or capacity will have to be built.

4.5.2 How flexible are existing information and data systems?

Assessing whether existing systems are capable of interoperability will help inform decisions about building new or reforming existing system. Some systems are already interoperable – such as UNHCR's ProGres and WFP's SCOPE – but most are not. Sometimes organisations collaborate in the use of a shared systems and in other cases, programmes develop bespoke systems. Open source systems can allow for adaptability and flexibility to context and change, such as UNICEF's adaptive and agile MIS used to manage the Social Welfare Fund in Yemen. There are few examples of humanitarian systems being used as part of a transition to state led social protection - WFP's SCOPE is one, where for example it provided technical capacity and support to state social safety net programme providers in Iraq, tying the government into the use of SCOPE for social protection response.[70] Increasing interoperability introduces a tension between achieving benefits such as efficiency, deduplication and ease of use, and increased threats to data protection and privacy.[71]

[66] Gellman, Robert. 2016. "Fair Information Practices: A Basic History." Version 2.16.

[67] Caribou Digital, Identity at the Margins: refugee identity and data management, Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2018

[68] Owino, B., 2019 Harmonising registration and identification in emergencies in Somalia, Development Initiatives https://devinit.org/resources/cash-transfer-somalia/

[69] ISPA, 'Identification Systems for Social Protection' (Washington, D.C.: Inter-Agency for Social Protection Assessments - World Bank, 2016).

[70] WFP, 2017 WFP & Social Protection Iraq case study https://docs.wfp.org/api/documents/0b040759c2af45e48e72379a267aca13/download/

[71] Caribou Digital, Identity at the Margins: refugee identity and data management, Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2018

4.5.3 What data, and what kind of data, do systems hold?

Being clear about what specific data different systems hold can also help guide decisions about information systems. For example, knowing if the systems contain a sufficient number of beneficiaries to form the basis of a new programme will determine whether an existing registry is sufficient, or a re-registration exercise is required. Assess the characteristics of the data on the following dimensions[72]: completeness (of target population and considering gaps by gender, disability etc.), relevance (does data contain required information?), currency (is it up to date?), accessibility (is data sharable, are agreements in place), accuracy (error and omission free) and data protection (is data secure and privacy protecting?).

BOX 6: BIOMETRICS

Biometrics: Commonly used biometrics include finger and thumbprint, retina scans and there is growing interest in face and voice recognition.

Biometrics provide a number of benefits – they are unique to an individual and difficult to lose or fake. They do not require user literacy and they can increase anonymity when replacing personal identifiers such as names and addresses.

However, biometrics have limits, including increasing concerns about security. They are immutable, and misuse of this data can place individuals at risk. Biometrics can be spoofed[73] or data bases hacked – placing individuals at risk. Biometric systems have limitations – for example scanners that can't read worn prints from manual labourers, while biometrics software struggles to recognise infants under 3[74], and facial recognition software is biased against and fails to recognise non-Caucasians[75]. Hacked data can lead to permanent risk, as biometrics, unlike passwords or signatures, cannot be changed.

Biometrics are widespread in the humanitarian sector – UNHCR and WFP both use biometrics in their registration and identity management systems. However, there is growing concern about their security – Oxfam limits use[76], and ICRC's data policy cautions against their use, and recommends off-line card storage for biometric data[77]. Developed countries limit biometrics use mainly to security, while lower/middle income countries use biometrics for civil registries, voter rolls, health records, and social protection.[78]

Existing datasets will most likely need to be adapted unless they are already linked through a shared unique identifier or interoperable data formats. Harmonising multiple data sets to support interoperability will almost certainly require data to be 'cleaned' to ensure accuracy, currency, completeness, and relevance to the business processes it supports. This entails clear processes for verifying, validating, updating and reporting on data - which can be

[72] See Barca and Beazley (2019) for detailed breakdown of data characteristics

[73] Fenker, Samuel P., and Kevin Bowyer. 2012. "Analysis of Template Aging in Iris Biometrics." In IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops.

[74] Best-Rowden, L., Hoole, Y. and Jain, A., 2016, September. Automatic face recognition of newborns, infants, and toddlers: A longitudinal evaluation. In *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)* (pp. 1-8). IEEE.

[75] Grother, P., Ngan, M. and Hanaoka, K., 2019. *Face Recognition Vendor Test (FVRT): Part 3, Demographic Effects*. National Institute of Standards and Technology.

[76] Zara Rahman, Paola Verhaert, and Carly Nyst, 'Biometrics in the Humanitarian Sector' (Oxfam / Engine Room, March 2018), https://policy-practice.oxfam.org.uk/publications/biometrics-in-the-humanitarian-sector-620454.

[77] ICRC, 'The ICRC Biometrics Policy', Policy (Geneva: ICRC, 28 August 2019), https://www.icrc.org/en/document/icrc-biometrics-policy.

[78] Gelb, Alan, and Julia Clark. 2013. Identification for Development: The Biometrics Revolution. Washington, DC: Center for Global Development.

expensive tasks taking months or even years[79] - sometimes longer than a new registration process.

Assessing technological context should also consider administrative capacity, as adapting, reforming or building new systems will require appropriate staff, procedures, roles and responsibilities.

Things to do:

- Conduct an information and data ecosystem mapping to assess the full technological context – see ID4D Diagnostic, National Identity Ecosystem Map.
- Assess the quality, content and capacity of key information and identity systems – see ISPA Identification Assessment Guidelines and identify groups at risk of exclusion.
- Assess data and data quality against agreed criteria – see Fair Information Principles.

[79] Barca, V., and Chirchir 2014, Single registries and integrated MISs: Demystifying data and information management concepts, Australian Department of Foreign Affairs and Trade, p46 https://www.opml.co.uk/files/2018-05/barca-chirchir-2014-data-information-management-social-protection.pdf?noredirect=1

ACKNOWLEDGEMENTS AND DISCLAIMER
This document was developed as part of SPACE - Social Protection Approaches to COVID-19: Expert advice helpline, implemented by the UK Foreign, Commonwealth & Development Office (FCDO) and Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH, and funded by UK Aid and the German Federal Ministry for Economic Cooperation and Development (BMZ). SPACE is managed by DAI Europe Ltd contracted through the FCDO framework agreement EACDS Lot B service 'Strengthening resilience and response to crises', and the helpline advice is provided by independent consultants contracted by FCDO, GIZ and other partners.

The views expressed in this document are entirely those of the authors and do not necessarily represent FCDO or GIZ own views or policies.

Published by FCDO and GIZ