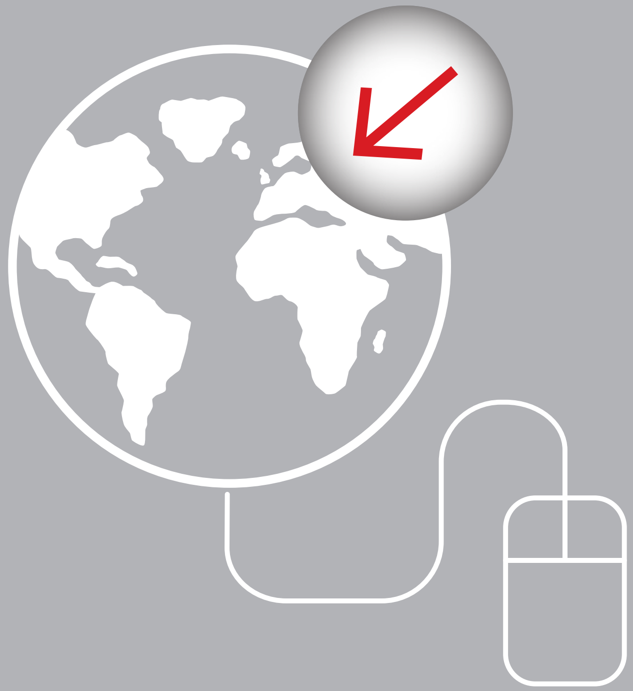
DATA PROTECTION FOR SOCIAL PROTECTION: KEY ISSUES FOR LOW- AND MIDDLE-INCOME COUNTRIES

giz
Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

An issue paper, developed for the Social Protection Interagency Cooperation Board (SPIAC-B), to discuss key issue areas concerning middle- and low-income countries

AUGUST 2020



CONTENTS

ACKNOWLEDGEMENTS

This issue paper was commissioned by GIZ's Sector Initiative Social Protection and benefited from reviews and inputs by external experts. The authors wish to thank the GIZ team, especially Dominique Leska, Kelvin Hui, Ralf Radermacher, Christian Merz and Tatjana Schock, without whom this report would not have been possible. We would also like to acknowledge the valuable contribution of the experts we interviewed during the process of elaboration of this paper: Valentina Barca, Conrad Daly (World Bank), Sameer Khatiwada (Asian Development Bank), Juergen Hohmann (EU-DEVCO), Dirk Homann (EU-DEVCO), and Raul Ruggia-Frick (International Social Security Association – ISSA). Finally, a sincere thank you to Chloe Messenger, Rachael Steller and Ric Goodman (Development Alternatives Incorporated – DAI) for their comments and suggestions in a previous version of this article, which helped us to improve it.

ACRONYMS

COE	Council of Europe
DPIA	data protection impact assessment
GDPR	General Data Protection Regulation
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit
ID	identity document
ILO	International Labour Organization
ISPA	Interagency Social Protection Assessment
MIS	management information system
MSI-NET	Committee of Experts on Internet Intermediaries
OECD	Organisation for Economic Co-operation and Development
SPIAC-B	Social Protection Interagency Cooperation Board
SPIS	social protection information system

PREFACE

New technologies can bring advantages to social protection systems. However, they also carry inherent challenges and risks. In this issue paper, we discuss the risks to privacy and personal data, particularly adapted to the context of social protection systems in low- and middle-income countries. We argue that if the necessary safeguards are put in place there is no contradiction between the right to privacy and providing effective social protection systems. However, social protection authorities and practitioners around the world may face challenges in complying with national and international data protection and privacy standards and legal frameworks. Consequently, social protection authorities and practitioners need special attention and support.

This issue paper was drafted by Ben Wagner and Carolina Ferro from Enabling-Digital.eu and commissioned by GIZ's Sector Initiative Social Protection to encourage broader debate among the members of SPIAC-B[1] on key issue areas of data protection and privacy. Therefore, it is not a document intended to be adopted by the many agencies and organisations gathered within SPIAC-B. Instead, it is a work-in-progress benefiting from the discussions and comments of members in the workstream on data protection in SPIAC-B's working group on digital social protection.

The authors hope that this living text contributes to raising awareness and deepening and advancing the much-needed discussion on data protection and privacy in the social protection field. Based on our extensive experience working on digital technologies, governance and human rights, any introduction of new technology needs to be met with an increased level of transparency and accountability, as well as effective redress mechanisms. In this context, we encourage social protection authorities and practitioners to embrace data protection and privacy principles and ensure respect for the data rights of any individual, group, family or household that applies or registers for social protection benefits or services.

[1] The Social Protection Inter-Agency Cooperation Board (SPIAC-B) is a light, lean and agile inter-agency coordination mechanism – composed of representatives of international organisations and bilateral institutions – to enhance global coordination and advocacy on social protection issues and to coordinate international cooperation in country demand-driven actions. SPIAC-B includes a working group on digital social protection, among other things its members discuss and comment on data protection issues.

1 INTRODUCTION: DATA PROTECTION IN SOCIAL PROTECTION PROGRAMMES IN LOW- AND MIDDLE-INCOME COUNTRIES

Digital technologies are enabling a major shift in how social protection systems are designed and implemented and benefits and services delivered, with the introduction of ID systems, digital payments, management information systems (MISs)[2], social protection information systems (SPISs), and biometrics, among other things. While new technologies may simplify and accelerate processes, reduce some costs, increase efficiency and effectiveness, and improve transparency and inclusiveness, they also bring with them inherent challenges and risks, including high technological costs, complexity (requiring a different skills set from e.g. administrative staff), challenges in relation to maintenance and sustainability, possible trade-offs (such as a reduction in overall effectiveness), and severe risks to privacy and personal data.[3, 4]

In light of the automated nature of data processing and the data-driven decision-making processes being adopted by social protection programmes, the need to ensure data security and data quality, as well as respect for personal data (while enabling human rights through social protection), is more critical than ever. The use of new technology does not need to create a contradiction between the protection of personal data and social protection. However, social protection authorities and practitioners from low- and middle-income countries face additional challenges in complying with national and international data protection and privacy standards and legal frameworks. Some of these issues are: How to avoid dependence on external technology providers? How to ensure that automation enables, rather than hinders, social protection programmes? How should host governments assess new technologies offered by external donors? These are just some of the questions that countries need to address.

This issue paper was commissioned by GIZ's Sector Initiative Social Protection to support the Social Protection Interagency Cooperation Board's (SPIAC-B's) working group on data protection for the social protection field. It has two main objectives. First, it seeks to encourage broader debate among SPIAC-B members on data protection and privacy by raising critical questions that every government and practitioner should address when designing and implementing social protection programmes. These questions aim to enrich the debate and facilitate the formation of a collective opinion towards reaching some *minimum agreement* on some of the major issues of concern.

The second objective of this issue paper is to promote discussion among SPIAC-B members regarding the importance of creating a *domain-specific guideline* on data protection, especially adapted to social protection systems in low- and middle-income countries. Our analysis suggests that such a guideline would be a practical and easy-to-access contribution, increasing awareness and supporting people on the ground (such as policymakers, host governments, social protection authorities, and practitioners) in the decision-making process, while dealing with the country-specific challenges involved in complying with data protection and privacy principles and legal requirements. This practical resource would address the 'what now' question social protection practitioners face when discussing issues in a non-technical, graphic and simplified way.

The methodology used to produce this issue paper was an extensive literature review on the topic of data protection for social protection, together with semi-structured interviews with some SPIAC-B stakeholders – Valentina Barca, Conrad Daly (World Bank), Sameer Khatiwada (Asian Development Bank), Juergen Hohmann (EU-DEVCO), Dirk Homann (EU-DEVCO), and Raul Ruggia-Frick (International Social Security Association – ISSA) – between September and December 2019. These interviews were intended to understand these organisations' views on the topic, collect the written materials already produced, and capture the interviewees' perceptions of any gaps and their opinion on what kind of material would make a good contribution to the field.

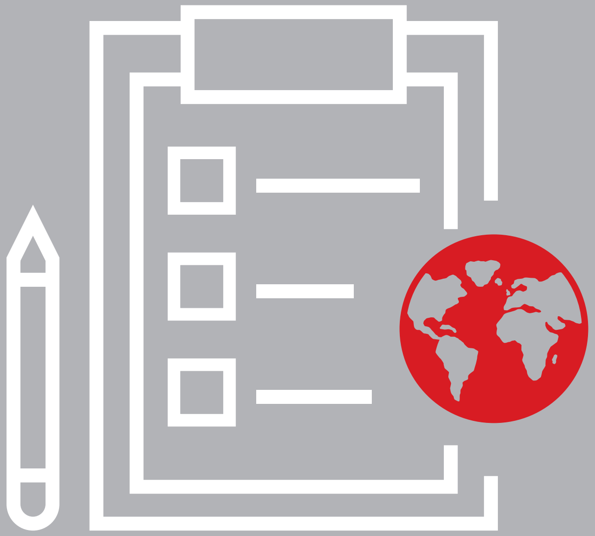
[2] The World Bank is moving towards calling these beneficiary operations management systems (BOMS).

[3] For further information on the advantages and disadvantages of adopting new technologies for social protection and the specific case of a digital and integrated information system see Barca and Chirchir (2019).

[4] According to the General Data Protection Regulation (GDPR), Art. 4. (1), "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

2

THE MAIN CHALLENGES



The use of digital technologies and digitalised data is increasing rapidly in policy areas, as well as in society as a whole, transforming how citizens, governments, civil society and companies engage with one another. This is also true for social protection systems. Digital technologies are deployed in different aspects of the social protection delivery chain, including information systems (e.g. building a digital and integrated information system is a critical milestone in developing a national social protection system),[5] financial services, and grievance and accountability mechanisms.

The challenges for the social protection field are enormous, with automation, biometrics, ID systems, and other technologies being adopted swiftly. It is essential to assess the necessity and risks but, sometimes, these technologies are adopted with insufficient assessment. In particular, the adoption of new technologies may impose considerable challenges to data protection and privacy. For instance, ID systems and biometric databases may allow for certain links to be made between databases, including enabling interoperability with other government systems or information-sharing across international borders, exacerbating the risks in terms of personal data protection (ISPA, 2016, p. 4). Therefore, although technically possible, the linking of different databases is not automatically justified, but must be balanced against an assessment of the inherent risks to data protection and privacy.

Social protection programmes process substantial amounts of personal information (name, age, gender, address, health status, biometrics such as fingerprints, and much more), which are collected from individuals, families and households. The personal information processed during the implementation of these programmes can be sensitive,[6] such as biometric data and health status. As pointed out by Sepúlveda Carmona (2018, p. 1):

> *The information is often stored in complex, integrated databases as well as elaborate management information systems (MISs), yet with few privacy and data security safeguards. In most cases, data subjects have little or no information about what data is collected, how it is used or for how long it will be retained.*

The right to privacy is guaranteed in several international human rights instruments, regional frameworks and national laws, and nearly 130 countries have adopted data protection/privacy laws and bills to ensure the protection of personal data (see Chapter 3; Banisar, 2019). However, Privacy International signals that there is an absence of robust and adequately enforced data protection laws in most countries in Africa, for instance. "In fact, only 43% of African countries have any data privacy laws. In countries that do have data privacy laws, critics and advocates have raised concerns about the lack of sufficient protections and safeguards."[7] Additionally, even when in place, "especially in developing countries, data protection laws and principles are not consistently applied in social protection systems" (Sepúlveda Carmona, 2018, p. 2).

Whether we agree with Sepúlveda Carmona or not (there is no comprehensive study that can provide us with detailed information on how social protection systems in various countries are dealing with data protection and privacy issues), it is generally agreed that low- and middle-income countries face additional challenges regarding the development and operationalisation of data protection and privacy and policies for social protection systems. These challenges include, for instance: the absence of national data protection laws; authoritarian governments (which increases the potential for the abuse of data and discrimination/persecution of certain citizens based on, for example, political ideology); weak administrative capacity; scarcity of resources (technical and financial) to develop, purchase and adequately implement new technologies; the

[5] For further information see Barca and Chirchir (2019).
[6] Sensitive personal data is a special category of personal data which, when processed, may lead to encroachments on the interests, rights and freedoms of the data subject. This is the case in relation to information that reveals personal characteristics such as sexual orientation, racial or ethnic origin, political opinions, religion, health status, payment of welfare benefits, and so forth (Council of Europe, 2018; Sepúlveda Carmona, 2018).
[7] See: https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion

imposition of new technologies by donors without assessing in detail need or risks; lack of technical capacity to provide long-term support for the new technologies implemented, leading to dependence on external technology providers; lack of appropriate judicial protections in case of breach; absence of data sharing policies among government agencies and private actors; and low awareness and/or political will regarding data protection and privacy issues, among other things.

It is also important to recognise the influence of cultural factors on the definition of data protection and privacy. The inherent notions that individuals and societies hold impact on how they look at data protection and privacy issues, and on the drawing of 'red lines' that should not be crossed. While international and regional frameworks may serve as a reference to develop national or sectorial laws, each country's specific context must be considered, and norms and principles should be adapted to fit local cultural standards. If cultural factors are acknowledged as a factor affecting how data protection and privacy are defined, the logical consequence is to accept that there is no universal definition of data privacy and protection.

In the absence of a legal framework to protect the privacy and personal information contained in their social security data systems, states must commit to establishing one.[8] Although preferable to legislate a larger, standalone data protection law and regime, essential elements that would apply might be operationalised by incorporating data protection and privacy principles with social protection laws and regulations, policy guidelines, programme directives and operational manuals. By developing a *domain-specific guideline* on data protection (as described in the introduction of this paper) it might be possible to influence and guide local authorities to integrate such principles and certain essential procedures into social protection systems.

Understanding how domestic and international data protection and privacy norms and principles are applied within their specific social protection system is a fundamental step for practitioners when designing, implementing and evaluating their programmes. In addition, it is extremely necessary to assess the specific risks to data protection and privacy within a particular social protection programme. Hence, a significant challenge is to define the minimum requirements for ensuring data protection and privacy in social protection programmes (e.g. to develop privacy policies and specific operational guidelines for data protection, provide access to personal data, and regulate data-sharing between government agencies etc.).

Social protection authorities must ensure that their programmes comply with national and international rules that protect privacy and govern information processing if they want to ensure that these programmes reach their goals (e.g. universal accessibility of services, quality of services, and protection of minorities and vulnerable populations). The lack of consideration of data protection and privacy rights in the design and management of these programmes (e.g. disclosure of personal information such as health conditions, disability or refugee status) may expose individuals, families or households that apply or register for social protection benefits or services to harm, stigmatisation or discrimination, undermining programme objectives.

Any new technology should only be adopted if it complies with data privacy and security regulations, which must explicitly state the rights of data subjects. And it is important to remember that "[i]ndividuals do not waive their rights to data protection and privacy by becoming beneficiaries of social protection programmes" (Sepúlveda Carmona, 2018, p. 12). The data subject's rights limit how the government or private companies can access and use personal data. Hence, there are critical questions regarding data protection and privacy that practitioners, governments, donors, multilateral development banks, other development partners and the private sector should address while designing and implementing social protection programmes and before implementing new technologies in social protection systems. And the specific challenges that low- and middle-income countries face require special attention from social protection authorities in order to properly address them.

[8] For further information, see: International Labour Organization (ILO) Social Protection Floors Recommendation, 2012 (No. 202).

3 DATA PROTECTION AND PRIVACY PRINCIPLES

The *right to privacy* is an internationally recognised human right, enshrined in several international human rights treaties, widely ratified by states (e.g. the United Nations' Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights), and contained in many conventions at the regional level, as well as national constitutions and bills-of-rights (see Annex 1). Privacy and data protection are different rights, although intrinsically linked. The right to privacy is broader and includes the right to the protection of personal data, yet covers many elements beyond personal information. The *right to data protection* safeguards "the fundamental right to privacy by regulating the processing of personal data: providing the individual with rights over their data, and setting up systems of accountability and clear obligations for those who control or undertake the processing of the data" (Privacy International, 2018, p. 12). Therefore, data protection is essential to the exercise of the right to privacy. In this paper we will refer to it as the right to 'data protection and privacy', a particular type of privacy, meaning the appropriate and permissioned use and governance of personal data.

DATA PROTECTION AND PRIVACY WORKS THROUGH KEY 'PRINCIPLES' THAT GIVE INDIVIDUALS RIGHTS OVER THEIR DATA. THESE SO-CALLED 'DATA PROTECTION AND PRIVACY PRINCIPLES' ARE RECOGNISED IN SEVERAL SOURCES, INCLUDING:

- Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data, 1980, as amended in 2013 (herewith referred to as the OECD Privacy Framework)
- Council of Europe (CoE) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981, as amended in 2018 (herewith referred to as CoE Convention No. 108+)
- United Nations Guidelines for the Regulation of Computerized Personal Data Files, 1990 (herewith referred to as UN Resolution 45/95)
- General Data Protection Regulation (EU) 2016/679 of the European Parliament and the Council of Europe, 2016 (herewith referred to as the GDPR)
- United Nations Personal Data Protection and Privacy Principles, 2018

These instruments have influenced the development of national data protection laws worldwide, translating some of the data protection and privacy principles into domestic legislation that regulates the processing of personal information. According to a comprehensive global study, as of November 2019, 130 countries have adopted data protection/privacy laws (and almost 40 countries and jurisdictions have bills and initiatives pending) to protect the personal data held by private and public bodies (Banisar, 2019; see Annex 1), although some existing data protection and privacy laws are out-of-date (Privacy International, 2018, p. 10).

THE CORE DATA PROTECTION AND PRIVACY PRINCIPLES ARE AS FOLLOWS:[9]

- Accountability (GDPR; OECD)
- Data minimisation (GDPR) or collection limitation (OECD)
- Purpose limitation (GDPR) or purpose specification and use limitation (OECD)
- Lawfulness, fairness and transparency (GDPR) or openness (OECD)
- Accuracy (GDPR) or data quality (OECD)
- Storage limitation (GDPR)
- Integrity and confidentiality (GDPR) or security safeguards (OECD)
- Individual participation (OECD)

These principles are interrelated and overlap. Each one contains several points of guidance, and it is essential to treat them together, as a whole. While they can receive different names, the basic principles are similar across the different data protection and privacy frameworks.

The data protection principles establish the conditions under which processing personal information is legitimate, limiting the ability of both public authorities and private actors to collect, publish, disclose and use individual personal information without the data subject's consent. These principles also establish the rights that data subjects hold, such as the ability to determine who holds information about them and how that information is used. Additionally, they entail several obligations imposed on those processing personal data – the data controller and processor – in both public and private sectors, forcing them to handle this data according to local data protection laws. Hence, "A strong data protection framework can empower individuals, restrain harmful data practices, and limit data exploitation" (Privacy International, 2018, p. 10).

In this paper, these data protection and privacy principles and the issues they address – the rights of data subjects, obligations of data controllers and processors, and the adoption of and risks involved in new technologies, among other things – will be discussed in relation to their implementation in social protection systems around the world, particularly in low- and middle-income countries. A set of questions is discussed, compiling key issues to do with data protection and privacy that every practitioner needs to think about when designing or implementing social protection programmes. These questions aim to enrich SPIAC-B's debate and facilitate the formation of a consensus on the main issues discussed, towards reaching a minimum agreement. The following chapter deals with each of these questions in turn.

[9] See GDPR, Art. 5., and OECD Privacy Framework, Paras 7–14.

4 KEY ISSUES: QUESTIONS FOR PRACTITIONERS

WHO IS RESPONSIBLE FOR DATA? WHAT HAPPENS WHEN THINGS GO WRONG?

There are two entities that have control over personal data and/or process personal data: data controllers and data processors. The data controller is the natural person (e.g. social protection minister) or the legal entity (e.g. government department), public or private, that, alone or jointly with others, is competent under to the law to determine the means of, and purposes for, processing personal data. That means that the data controller has decision-making power with respect to data processing and is responsible for safeguarding and handling personal information on computers or structured manual files. The data processor is the individual or legal entity that processes data on behalf of data controllers (which is often limited to technical solutions – the 'methods and means' of processing).

According to good international data protection practice, and as seen in most laws, conventions and guidelines, there should be several legal responsibilities and obligations imposed on data controllers and processors in social protection programmes. Social protection authorities that process personal data, in their capacity as either data controllers or processors, must be able to demonstrate how they are complying with data protection requirements at any given time, including data protection principles, fulfilling their obligations, and upholding the rights of individuals. This is the *accountability principle*, under which controllers and processors must take all appropriate measures to comply with the obligations under the data protection regime. These obligations entail the acknowledgement of the data rights of any individual or family that applies or registers for social protection benefits or services, such as the right to access their data at all times, have their data rectified if it is inaccurate and express objections if data processing leads to disproportionate or unfair results.

What happens in the event of a data breach (e.g. unauthorised access, misuse or disclosure of personal data)?[10] Is there a clearly established procedure to follow? Unfortunately, "[m]ost developing countries do not support effective grievance and redress mechanisms for social protection programmes" (Sepúlveda Carmona, 2018, p. 32). A personal data breach, if not addressed in an appropriate and timely manner, may result in physical, material or non-material damage to individuals, including loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymization, damage to reputation, loss of confidentiality of personal data protected by professional secrecy and other economic or social disadvantages.[11] Accountability mechanisms play an important role in investigating breaches and holding entities to account according to the law. It is extremely important that social protection programmes set up mechanisms that beneficiaries can access when their privacy or personal data has been breached. Furthermore, programmes should be obliged to investigate breaches, as well as to inform the relevant supervisory authority and affected data subjects.

Social protection programmes should ensure that impact assessments are undertaken prior to collecting and processing personal data, and should establish enforcement and compliance monitoring mechanisms that establish/address the following (ISPA, 2016; Sepúlveda Carmona, 2018): (a) how the system will detect unauthorised access or misuse; (b) how the database will be kept secure, especially from misuse, hackers, and unauthorised use and personnel; (c) bodies to monitor programme-internal data protection compliance (which can include a chief privacy officer for the programme); (d) a data-breach complaint protocol; (e) penalties in the event of data breaches; (f) data-breach redress measures in the event of unauthorised access, use or disclosure; and (g) a privacy management programme that is integrated into its governance structure and establishes internal oversight mechanisms, ensuring that data protection principles are covered.

[10] According to GDPR, Art. 4 (12), a 'personal data breach' is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

[11] For further information, see GDPR, Para. 85.

POINTS FOR DISCUSSION:

- What are the good international practices to follow when dealing with a data breach? What is the obligation of the database operator in notifying the data subject, including the timing and content of the notification as well as remedial measures?
- What are the accountability mechanisms that need to be put in place?
- In terms of regulatory agencies and enforcement capacity, what is the reality in low- and middle-income countries? Are there usually independent oversight bodies to monitor data protection compliance? Do they operate at the social protection programme or national level?
- In terms of data ownership, who should legally own personal data?
- In relation to the data protection and privacy 'literacy' of the data subjects, would they know what a breach is? Would they understand the implications of one?

HOW MUCH DATA DO SOCIAL PROTECTION PROGRAMMES NEED TO COLLECT AND FOR WHAT PURPOSES?

Data minimisation – also called *collection limitation* – is a fundamental data protection principle.[12] Unnecessary data collection cannot be justified and may increase costs and pose risks for data subjects' rights in both well-known and unpredictable ways. In addition, the collection of unnecessary data is likely to result in greater pressure to use data for purposes other than those originally intended and to which the data subject has consented (ISPA, 2016; Sepúlveda Carmona, 2018). Hence, "[d]ata minimisation is a key concept in data protection, both from an individual's rights and an information security perspective" (Privacy International, 2018). Thus, limiting the collection of personal data is essential, especially sensitive data such as religious affiliation, race, ethnicity, linguistic origin, sexual orientation, political opinions, philosophical and other beliefs, as well as membership of associations or trade unions.[13] This kind of data is at risk of being used for political purposes, giving rise to unlawful or arbitrary discrimination, and limiting or negating the rights of data subjects. Other types of information can be sensitive for certain groups in particular circumstances, such as refugees, people living in humanitarian crisis zones, asylum-seekers, or certain professions, such as social workers, judges, and police officers. In some cases, even information that appears inoffensive could be extremely sensitive and may create risks to a person's safety, either alone or in combination with other data held or publicly available. This subset of personal data is often referred to as 'sensitive personal data'.

[12] See OECD Privacy Framework; CoE Convention No. 108, Art. 5 (4) (c) and Paras 55–61; and GDPR, Art. 5 (1) (c).
[13] See United Nations' Guidelines for the Regulation of Computerized Personal Data Files (1990) and CoE Convention No. 108, Art. 6.

In order to prevent adverse effects for the data subject where sensitive personal data is implicated, data processing – even when done for legitimate purposes – needs to be accompanied by appropriate safeguards such as, for instance: the data subject's explicit consent needs to be obtained; laws must be promulgated covering the intended purpose and means of processing, including indicating the exceptional cases where processing such data would be permitted; there needs to be a commitment to maintaining professional secrecy; measures must be put in place following a risk analysis; and a particular and qualified organisational or technical security measure (e.g. data encryption) must be adopted.[14] In addition, an individual's ability to apply for the suppression of their data (i.e. name and/or address information) is a necessary right.

Social protection programmes need to be aware that even information that appears harmless may have major security and privacy dimensions, and the tendency to include information that might be useful in the future (but is currently not needed) must be avoided at all costs. The principle of data minimisation is even more central in the age of big data where "[w]ith the promise and hope that having more data will allow for accurate insights into human behaviour, there is an interest and sustained drive to accumulate vast amounts of data" (Privacy International, 2018, p. 41). There is an urgent need to challenge this paradigm and ensure that only data that is necessary and relevant for a specific purpose is collected and processed. Contrary to this, "many [social protection] programmes around the world collect excessive amounts of beneficiary information, much of which is of little use and is often inaccurate" (Chirchir & Kidd, 2011, p. 7, cited in Sepúlveda Carmona, 2018, p. 22). According to the author, limiting information collection is particularly relevant in countries with weak administrative capacities, as they may face difficulties in collecting and managing registration datasets, which could translate to inclusion and exclusion errors and increase security risks.

Social protection programme designers should always evaluate the amount of data to be collected, processed, stored, and shared. Collecting minimal information is critically important, especially when programmes use biometric identification systems and other technologies that handle highly sensitive data. Good criteria for defining which data should and shouldn't be collected is to follow the *purpose limitation* – also called *purpose specification and use limitation* – principle.[15] All personal data should be collected for a determined, specific, and legitimate purpose, stated (and consented to by the beneficiary) at the time of collection, and further processing should also be compatible with this purpose.

Therefore, the *data minimisation* principle works in synchronicity with the purpose limitation principle. Information collected in a social protection programme, across and regardless of the stage, should be the minimum necessary to meet the established purposes. Specifying and informing the beneficiary of the purposes for processing any personal data is a way to ensure that certain data collected for one objective will not be used for a different purpose. It would be unethical – and also contrary to the discussed data protection principles – to ask a beneficiary of a social protection programme "to provide personal information for a given activity and then to use that information for another purpose without either notice to, or the consent of, the individual" (ISPA, 2016, p. 42). Therefore, personal data must not be shared, made available or used for purposes other than those specified at the time of data collection.

The OECD Privacy Framework foresees two general exceptions to the use limitation principle: personal data may be used for purposes not originally intended either with the consent of the data subject or when authorised by law (e.g. data that have been collected for the purposes of administrative decision-making may be made available for research, statistics and social planning purposes that are not considered incompatible with the initial purpose).[16] However, these two broadly recognised exceptions are often abused and misused, a pertinent example being India's national biometric identification database, Aadhaar, which bypasses this data protection principle (Privacy International, 2018).

[14] See CoE Convention No. 108, Para. 56.
[15] See OECD Privacy Framework; CoE Convention No. 108, Art. 5 (4) (b); and GDPR, Art. 5 (1) (b).
[16] See OECD Privacy Framework, Para. 10; CoE Convention 108, Art. 5 (4) (b); GDPR, Art. 5 (1) (b).

POINTS FOR DISCUSSION:

- How can the adherence of social protection programmes to the data protection principles of data minimisation and purpose limitation be improved?
- Is 'the less data you collect, the better' a good strategy? What is the most appropriate paradigm?
- Is it possible or practical to specify in detail and in advance each purpose for which personal data are intended to be used? What would be a good strategy to do so for social protection programmes?
- What are the main questions that social protection programme designers should address before starting to collect personal data?

HOW TO ENSURE DATA IS FAIR, TRANSPARENT AND LAWFULLY PROCESSED?

Personal data must be processed in a *lawful, transparent and fair* manner. This is a primary principle of many data protection laws, conventions and guidelines, also called the *openness* principle.[17] This means that all personal data a social protection programme collects should be obtained and processed following this principle. No personal information should be secretly processed unless expressly permitted and detailed by law and, whenever such is the case, must be reduced to a strict minimum.

Fairness and transparency mean that personal data is not used in ways that data subjects would not expect, are not aware of and did not give consent for.[18] It is also related to the form/method by which the information was obtained. It implies that nobody is coerced into giving personal information to social protection authorities or has no choice due to their situation (e.g. in desperate need of aid), and also that no unfair practices will be used, such as the use of hidden data registration devices (e.g. tape recorders) or deceiving data subjects into supplying information. The beneficiaries (or applicants) should be clearly informed and aware of how their data is going to be processed, the legal basis and purpose of the data processing, by whom (the identity of the controller and, if relevant, the processor), and how long it will be held: "If there is an intention to share the data of an individual with a third party but the data controller is not transparent about this fact and the data subject is not clearly informed, it is likely that their personal data was obtained unfairly, and the process will not be considered transparent" (Privacy International, 2018, p. 38).

To be fair and transparent also implies that people must give their free, informed, and specific consent for processing their personal data, which may be given by way of a statement or, in certain circumstances, by clear affirmative action.[19] It should be explicit and require an active process by the individual, rather than a passive opt-out process. Informed consent requires that information and communication related to the processing of personal data be accessible and easy to understand. Data subjects must understand all implications related to the information they provide. Given the vulnerability of some beneficiaries, especially those of non-contributory social protection programmes, the information presented should be easily accessible, legible, understandable and adapted to the relevant data subjects (i.e. in simplified language or in a way that illiterate people can comprehend). Accordingly, "programme data collection forms may feature consent clauses and accessible information about the purpose of the data" (Sepúlveda Carmona,

[17] See OECD Privacy Framework; CoE Convention No. 108, Art. 5 (3) and (4) (a); GDPR, Art. 5 (1) (a).

[18] According to GDPR, Art. 4 (11), 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

[19] See OECD Privacy Framework, Art. 10 (a); CoE Convention No. 108, Art. 5 (2) and Paras 41–45, 68; GDPR, Art. 4 (11), Art. 6 (1) (a), Para. 32.

2018, p. 26). Finally, for consent to be freely given, and therefore to be a valid legal basis for data collection and processing, applicants and beneficiaries must be offered alternatives that will allow them to continue receiving assistance. If this is not possible, another legal basis for data collection and processing is required (Kuner, 2017, Chapter 3: Legal bases for personal data processing).

When processing sensitive personal data, further conditions must be met. Generally, sensitive personal data processing should be authorised and limited by law. Additionally, "[w]here consent is to be relied upon to justify the processing of sensitive personal data, it is extremely important that it is explicit and meets all the consent requirements […] (i.e. informed, free, specific)" (Privacy International, 2018, p. 67).

However, it is often impractical and costly to rely on consent, particularly when there are many activities involving personal data and a large number of data subjects, in which case "[it]may be appropriate to use consent for some activities" (ISPA, 2016, p. 45). The OECD Privacy Framework (Para. 7) contains a reminder that data should be obtained by lawful and fair means and 'where appropriate' with the knowledge or consent of the data subject, justifying that there are situations where for practical or policy reasons the data subject's knowledge or consent can be considered unnecessary (e.g. criminal investigation activities and the routine updating of mailing lists). This is a lively discussion in the data protection and privacy debate. The reality of low- and middle-income countries needs to be considered, as does the digital and data 'literacy' of data subjects. The operationalisation of consent requirements should be context specific, and discussed and adapted for each particular social protection programme.

Processing personal data in a lawful way means that it meets the legal basis (or grounds) for processing this kind of information and that it will be done in a way that respects the rule of law. The term 'legal ground' is defined as "a limited justification for processing people's data set out in law (i.e. consent)" (Privacy International, 2018, p. 37). A data controller or processor must identify the legal basis on which their processing of personal data is permitted. The law may provide many grounds for processing personal data, for instance: consent of the data subject; a need to process the data for the performance of a contract with the data subject or to take steps to enter into a contract; for compliance with a legal obligation; to protect the vital interests of a data subject or another person; for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject; and the processing of personal data for scientific, historical, or statistical purposes (Privacy International, 2018).

The fair, transparent and lawful processing data protection principle should be respected in all programme implementation phases and, ideally, be considered from the design phase of the social protection programme onward.

POINTS FOR DISCUSSION:

- If a legal basis for data protection and privacy does not exist in a certain country, how should social protection authorities proceed? How to develop sufficient legal frameworks in the total absence of a larger/broader data protection policy, law or other instrument and, in such cases, what instruments can be adapted to give a basis, and what would the subsequent, programme-specific ones look like?
- What constitutes consent?
- What steps need to be taken if consent is lacking?
- In what ways can information be presented in an easy and accessible way, including for illiterate people?

HOW AND WHY DO WE NEED TO ENSURE DATA ACCURACY? FOR HOW LONG SHOULD DATA BE KEPT?

In all phases of social protection programmes, data should be accurate, complete and, where necessary, up-to-date. This is called the *accuracy* or *data quality* principle for data protection.[20] Increasingly, social protection programmes rely on data. However, if personal data is inaccurate, incomplete or outdated, it could lead to poor decision-making, which could have severe implications (e.g. wrongly denying access to a social protection service or benefit).

From the data subject side, the *individual participation principle* [21] seeks to ensure that applicants and beneficiaries have access to and control of personal data. All personal data that social protection programmes hold should be made available to data subjects upon request:

> *Each individual should have a right to know whether a data controller has data pertaining to him or her, a right to see and/or copy that data, a right to be given a reason if a request for access is denied and to challenge the denial, and a method to challenge and correct data that are not accurate or complete.* (ISPA, 2016, p. 47)

The right to access should be simple to exercise (OECD, 2013). Therefore, beneficiaries should be able to request access to their data contained in social protection programme databases or MISs, through non-complicated and accessible mechanisms. As well as ensuring that the data subject has control over their own data, it "also provides additional tools that check programme information accuracy. Knowing that beneficiaries can easily access information may prevent officials from falsifying it" (Sepúlveda Carmona, 2018, p. 31).

Unfortunately, social protection programmes around the world often keep inaccurate beneficiary information (Sepúlveda Carmona, 2018, p. 22), which undermines the reliability of the decisions made using that data. This is the reason why social protection authorities should be obliged to conduct regular checks on the accuracy and relevance of the data recorded and ensure that they are kept as complete as possible – to avoid errors of omission and ensure that data are updated regularly, or at least when the information a file contains is used, for the duration of their processing (United Nations, 1990). Defining who is responsible for updating the data and the procedures for that to happen is an important task that social protection authorities must undertake.

And how long should social protection programmes hold data? The *storage limitation* data protection principal[22] advocates that personal data should be retained in a form that permits identification of data subjects no longer than required for the purpose for which it was obtained. After the necessary time period, when information no longer serves the original purpose, personal data should be securely deleted or given an anonymous form (that does not permit data subject identification).[23] Control over data may be lost when data are no longer of interest. The storage of such data increases security risks (e.g. theft or unauthorised copying), which raises concerns that it could be used for new purposes merely because it is still available and accessible (OECD, 2013; Privacy International, 2018). In addition, inaccurate data should be erased or rectified without delay. Therefore, the data protection principles of purpose specification, accuracy and storage limitation are intertwined.

This means that social protection programmes should ensure that the period for which personal data are stored is limited to a strict minimum, establishing a retention policy and schedules specifying the retention periods for all the data that they hold. They should clearly indicate time-limits for processing and storing personal data, as well as how it will be subsequently deleted from databases or anonymised. Any exceptions to this must be very limited and clearly defined by law.[24] Just because social protection authorities might come across another use for the data does not justify general or indefinite retention (Privacy International, 2018). For individuals to be fairly informed about the processing of their data, they must be informed about how long their data will be retained.

[20] See OECD Privacy Framework; CoE Convention No. 108, Art. 5 (4) (d); and GDPR, Art. 5 (1) (d).
[21] See OECD Privacy Framework, Para. 13; ISPA (2016).
[22] See OECD Privacy Framework (p. 57); CoE Convention No. 108, Art. 5 (4) (e); GDPR, Art. 5 (1) (e).
[23] It is extremely important to be cautious about the potential to deanonymize data, particularly when combined with datasets held by other entities or data that is publicly available.
[24] "Any interference with the right to data protection and privacy requires to be necessary and proportionate. Blanket data retention completely fails to respect this – as confirmed in 2014, when the European Court of Justice struck down the Data Retention Directive, calling mandatory data retention, 'an interference with the fundamental rights of practically the entire European population…without such an interference being precisely circumscribed by provisions to ensure that is actually limited to what is strictly necessary'. This decision represented a strong authoritative recognition of the safeguards that must be in place to protect our right to privacy" (Privacy International, 2018, p. 44).

POINTS FOR DISCUSSION:

- What are the good international practices for keeping data accurate, complete and up-to-date in social protection programmes?
- How can beneficiaries easily exercise their right to access and correct inaccurate data?
- How can social protection programmes deal with governments that wish to retain data and use it for different purposes other than the one(s) specified during collection?

HOW CAN WE BEST ENSURE THE SECURITY OF DATA AND SYSTEMS? WHO SHOULD BE AUTHORISED TO ACCESS PERSONAL DATA?

Personal data – during storage, transmission and use – as well as the infrastructure relied upon for processing, should be protected by security safeguards against risks such as unlawful or unauthorised access, use and disclosure, as well as loss, destruction, modification or damage of data. The controller and, where applicable, the processor must take reasonable security safeguards using appropriate technical and organisational measures. Processing sensitive personal data, such as biometric data, requires even higher security levels. The *integrity* and *confidentiality principle* – also called the *security safeguarding principle* – is an extremely important data protection principle.[25]

Beneficiaries’ personal data must be handled securely in all social protection programme phases: collection, registration, storage, use, sharing and disposal. This involves ensuring data security demands by having the appropriate equipment (i.e. hardware and software) and also having the necessary procedures and organisational guidelines in place. In addition, it is important to protect access to data, social programme installations, hardware and software.

SECURITY SAFEGUARDS COULD INCLUDE (PRIVACY INTERNATIONAL, 2018):

- Physical measures, e.g. locked doors and identification cards
- Organisational measures, e.g. access controls
- Informational measures, e.g. enciphering (converting text into a coded form), and threat-monitoring
- Technical measures, e.g. encryption, pseudonymization, anonymization

Other organisational measures should include: regular testing of the adequacy of these measures; implementation of data protection and information security policies; adherence to approved codes of conduct; clear distribution of data-processing responsibilities; and information for and training of social protection personnel about data security rules, confidentiality obligations, and any other obligations that data protection legislation may stipulate (Privacy International, 2018; Sepúlveda Carmona, 2018).

[25] See OECD Privacy Framework; CoE Convention No. 108, Art. 7 (1); and GDPR, Art. 5 (1) (f).

Security issues must be considered from the design phase of social protection programmes, or urgently implemented once the social protection team is aware of its importance. The lack of sensitivity of social protection authorities and practitioners to the security of personal data is, usually, directly related to their limited understanding of the implications of this lack and the absence of organisational measures. When security measures, either for the data or for infrastructure safety and security, go unimplemented, data remains vulnerable to threats and is at risk of breach and unlawful access. Weak security standards have resulted in several data breaches in recent years.[26]

Social protection authorities bear a significant burden in protecting their data subjects from criminal activity, and must regularly undertake risk assessments of the appropriate security requirements. The consequences of a data breach are potentially disruptive and significant. In many data protection laws, it is mandatory to notify data subjects about the loss of, or even just unauthorised access to, personal data (breach notification). In particular, databases with personally identifiable information should have a policy and procedure in place for breach notification, as well as a contingency plan for responding to an actual data breach (ISPA, 2016).

Security mechanisms should be adapted to the technology that social protection programmes use. For instance, "[in] the case of a 'smart' ID card, e.g., security considerations centre on (1) can it be forged; (2) can information stored on the card be accessed, and if so, by whom; (3) can the card be remotely blocked if stolen; and (4) what other information can be accessed by the card" (ISPA, 2016, p. 46).

Social protection programmes, in many countries, use MISs to manage programme datasets and automate core business processes. However, "[w]hile MISs enable countries to more efficiently manage information and monitor it more effectively, strict security protocols should be in place to ensure data protection for each MIS component" (Sepúlveda Carmona, 2018, p. 30). Special attention should be given in the case of integrated MISs (the so-called SPISs),[27] in which different social protection programme MISs are integrated into a single registry (the 'social registry'), and sometimes beyond to include other sectors (e.g. education, health, national ID systems, civil registries). Social protection authorities are responsible for establishing measures for compliance with data protection rules in the context of their MIS and/or SPIS processing operations. Additionally, they should establish data-sharing protocols.

Data-sharing is a major topic in personal data security. Who has access to the data? What data should or should not be shared, and with whom?

> *The greatest threat to the integrity of an information system may arise not from external hackers, but from people within the system – those who have been trusted with access, including government agencies and persons or organizations registered under the scheme – in accessing personal data.*
> (ISPA, 2016, p. 40)

It is worth noting this is not just related to purposeful misuse (i.e. mistrust) of those trusted with access, but also with the likelihood of human error, and potentially cultural factors which may make people more likely to see sharing data with a friend or colleague as a normal practice. It reinforces the importance of setting appropriate operating procedures. It also raises concerns about abuse (of power or system, at low and high levels – individual agents or by the state); corruption; and targeted hacks (where external actors take advantage/compromise the system's personnel).

[26] Take, for instance, the examples of the Philippines (in 2016 the personal information of over millions of voters were leaked following a breach on the Commission on Elections' database) and Brazil (in 2016, due to security failures, a database of the Municipality of São Paulo was published exposing personal data of an estimated 650,000 patients and public agents from the public health system) (Privacy International, 2018).

[27] An MIS is a system that transforms retrieved data from a programme's database into information that can be used for efficient and effective management. A SPIS (previous referred as IMIS) refers to the broader system that enables the flow and management of information within and between social protection programmes, integrating the different MISs from each programme (Barca & Chirchir, 2019, p. 18).

Strictly speaking, “only social protection authorities should access information collected for social protection purposes. Sharing that information with other national authorities or the private sector could infringe beneficiaries’ rights to personal security, data protection and privacy and must be carefully assessed” (Sepúlveda Carmona, 2018, p. 27). Although government agencies may wish to share personal data for a range of good reasons, it is important to build in protections and limitations to guard against the potential for abuse. Here the main concern around the linking of databases or systems is that, especially when artificial intelligence (AI) is used, it could create a much larger image of the data subject than they would like, and to which they could not have consented at the time of data collection.

Following the purpose limitation principle, information between various databases can only be integrated if unambiguously authorised by laws that have been established preceding the event (e.g. if law enforcement authorities have appropriate cause to access certain data in a social protection database).[28] Legislation must designate what information can be disclosed, under what circumstances, to which agencies or programmes, and what are the conditions for disclosure (ISPA, 2016). Additionally, according to the fairness and transparency principle, social protection programme applicants and beneficiaries should be informed, at the time of data collection and before they give their consent, whether or not data will be shared with other government agencies and give their consent. Even stricter rules should apply when sharing or disclosing information with non-governmental entities such as private companies, non-governmental organisations (NGOs) or independent consultants (ISPA, 2016, p. 43).

POINTS FOR DISCUSSION:

- Could challenges arise for social protection from sharing too much social protection data with other government entities?
- What concerns are raised by connecting national identity systems (which of themselves raise rights concerns) with social protection programmes?
- What are the minimum standards for data security to ensure that a social protection provider can prevent harm to its users?
- How can we avoid dependence on external technology providers?
- Are biometrics a necessary component? Giving that the adoption of biometrics (especially in ID systems) has been happening and most probably will increase, how do we frame their application/integration with social security programmes in a way that reduces risks?
- What forms of communication should be adopted so that beneficiaries feel that their data is safe and their privacy not compromised?

[28] “Determining whether a data protection and privacy rights interference is reasonable (i.e. not arbitrary) requires balancing each case’s circumstances precisely. […] integrating social protection databases with law enforcement registries (e.g. local, national, regional and international policing agencies) – even when legally authorized and justified on national security and counter-terrorism grounds – is likely to be arbitrary (i.e. the resultant limitation of rights may be disproportionate to programme goals, unnecessary in democratic societies or simply discriminatory)” (Sepúlveda Carmona, 2018, p. 28).

WHAT ARE THE MAIN RIGHTS OF DATA SUBJECTS TO BE CONSIDERED?

The rights of individuals, or data subjects, are a central component of any data protection law. They connect directly with the data protection principles previously discussed. Social protection programmes must ensure that the rights of individuals and families who apply or register for social protection benefits or services are respected. These rights impose positive obligations on social protection authorities (data controllers) and should be enforceable by independent data protection authorities and courts.

AT A MINIMUM, THESE RIGHTS SHOULD INCLUDE THE:[29]

- Right to information
- Right to access
- Rights to rectify, block and erasure
- Right to object
- Right to data portability
- Rights related to profiling and automated decision making
- Right to an effective remedy
- Right to compensation and liability

Given that social protection programmes collect and process significant amounts of personal information, authorities should ensure applicants' and beneficiaries' (data subjects') access to and control of personal data, whether or not this information has been collected directly from them or from other sources. The *right to information* consists of the obligation of social protection authorities to provide individuals and families, at the moment of collection of the data, with the information necessary for them to make an informed decision about whether or not to share their data.[30]

The *right to access* means that beneficiaries must be able to obtain (request and be given) information about the processing (collection, storage, or use) of their personal data. For this to happen, a good management system for data processing is needed. Accessing their data enables data subjects to check whether their data is being processed in line with the law and their expectations, whether it is accurate and whether they want to take further action, such as exercising their right to object: "This can help them uncover why decisions were made and also expose abusive data practices" (Privacy International, 2018, p. 53). It is also important to note the risks and challenges associated with the right to access, such as the risk of fraudulent access requests.[31]

[29] See OECD Privacy Framework, Paras 12 and 13; CoE Convention No. 108, Art. 9; GDPR, Chapter 3; and Privacy International (2018).

[30] Social protection programmes should provide applicants and beneficiaries with at least the following information: identity of the controller (and contact details); purpose(s) of the processing; legal basis for processing; categories of personal data; recipients of the personal data; whether the controller intends to transfer personal data to a third country and the level of protection provided; period for which the personal data will be stored; existence of the rights of the data subject; right to lodge a complaint with the supervisory authority; existence of profiling, including the legal basis; the existence of automated decision-making; source of the personal data (if not obtained from the data subject); whether providing the data is obligatory or voluntary; and the consequences of failing to provide the data (Privacy International, 2018; GDPR).

[31] See, for example: https://www.newstatesman.com/science-tech/internet/2018/09/gdpr-easier-access-data-hackers-access-online-security-spotify

Beneficiaries of social protection programmes should have the *right*, free of charge and without excessive delay, to *rectify* (correct, update, or modify) and *block* (restrict) data processed about themselves to ensure the data is accurate, complete and up-to-date. Some data protection frameworks, such as the GDPR (European Parliament & Council of Europe, 2016) and the CoE Convention No. 108, include the *right to erasure* ('right to be forgotten'), permitting data subjects in certain circumstances (e.g. when there is no lawful basis for processing) to request that the data controller erase their personal data. An example of a possible situation in social protection programmes would be when a beneficiary drops out of a programme.

Additionally, beneficiaries should have *the right to object*, at any time, to the processing of their personal data. If they object, the onus must be on the social protection programme to demonstrate legitimate grounds for the processing that override his or her interests or rights and fundamental freedoms.

The *right to data portability* allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability (e.g. allowing someone to change mobile service provider without changing mobile phone number). When it comes to social protection programmes, administered by local or state authorities, usually there is only one provider possible. Therefore, the right to data portability only makes sense for social protection beneficiaries if interpreted in a particular sense: ensuring that their data can be transferred to different municipalities and that they will be able to access social protection benefits and services regardless of where they are. Interoperability at the national level can facilitate the portability of benefits across the country (ISPA, 2016).

Rights related to *profiling*[32] *and automated decision making* should include the right to request human intervention (in a simple way) and to challenge a decision. Beneficiaries should also have the *right to an effective remedy* against a social protection data controller, where they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law. They must have the right to submit a complaint to the independent supervisory authority, as well as to have access to an effective judicial remedy via the courts. Finally, beneficiaries of a social protection programme whose rights are found to have been violated should have a *right to compensation* for the damage suffered – material or non-material (e.g. distress).

After the implementation of the GDPR, a debate ensued regarding the ownership of data, with the question of how to ensure that data subjects 'own' the collected data (where they become custodians of their own data). Social protection authorities may face several challenges (e.g. technical and political issues) in ensuring beneficiaries remain in control of their personal data. However, particularly with respect to providing access to and enabling them to correct their personal data, these challenges may be addressed effectively through technical standards and tools.

[32] According to the GDPR, Art. 4 (4), 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. "Profiling occurs in a range of contexts and for a variety of purposes; from targeted advertising and healthcare screenings to predictive policing. Profiling as a process recognises the fact that data can be derived, inferred and predicted from other data" (Privacy International, 2018, p. 57).

POINTS FOR DISCUSSION:

- What are the key data rights of individuals that need to be considered by social protection providers?
- How do the rights of data subjects and the ability to receive social protection conflict with each other? How to best overcome these challenges and provide genuine alternatives for applicants and beneficiaries?
- How do we reconcile the 'right to be forgotten' with the accountability principle? Concerns about corruption (payment to political supporters rather than intended beneficiaries, for example) could potentially go unchallenged through the application of this principle if the recipients successfully have their details deleted before an investigation.

WHICH PROCESSES MAY BE AUTOMATED, AND WHICH MAY NOT?

As a result of the significant increase in data generated and advancements in technology, new ways of processing personal data are emerging. Data can now be processed by automated means, without any human involvement:

> *Automated data processing techniques, such as algorithms, do not only enable internet users to seek and access information, they are also increasingly used in decision-making processes, that were previously entirely in the remit of human beings. Algorithms may be used to prepare human decisions or to take them immediately through automated means.* (MSI-NET, 2018, p. 3)

With the intention of improving and accelerating data collection and analysis and reducing costs, there is a growing reliance by social protection programmes on *automated systems*. As part of automated data processing, social protection data controllers should assess if their data processing techniques comply with data protection and privacy frameworks. It is essential to address key question regarding automation. Which processes should be automated and which should be manual? Which processes can be automated, but need human oversight? Who should make these decisions? Where does oversight come in, and by whom?

Automation can offer convenience and save costs for applicants and beneficiaries. At the same time, it may also have data protection and privacy implications. Special concerns arise when considering *automated decision-making*; namely, the process of making a decision by automated means (no manual processing) without any human involvement. Profiling can be part of an automated decision-making process.

Automated decisions can be based on any type of data, for instance, data provided directly by beneficiaries, data observed about them, or derived or inferred data, such as a profile of an individual that has already been created. One challenge of automated data processing techniques (in particular, algorithms) is the generation of new data that can be inferred or constructed from the original data given by data subjects. This raises major issues around notions of consent, transparency and personal autonomy (MSI-NET, 2018). Another major concern is related to new data processing methodologies like AI, where decisions are based on machine learning from a potentially-biased data set. Consequently, automated decision-making can produce decisions that are inaccurate, unfair or discriminatory, and makes it more difficult to interpret or audit decision-making processes.[33]

Therefore, data controllers should carry out a data protection impact assessment (DPIA) in order to evaluate if any processing – via an automated decision technique process – is likely to result in risks to data subjects and define what safeguarding measures must be applied.

In a recent example (5 February 2020), the District Court of The Hague concluded that the use of the System Risk Indication (SyRI) – a system designed by the Dutch government to process large amounts of data collected by various Dutch public authorities to identify those most likely to commit benefits fraud – is unlawful as it violates human rights, especially the right to privacy (Privacy International, 2020). The 'SyRI case' is a landmark ruling for benefit claimants around the world, and the judgment is likely to resonate well beyond the Netherlands: "The case was seen as an important legal challenge to the controversial but growing use by governments around the world of artificial intelligence (AI) and risk modelling in administering welfare benefits and other core services" (Henley & Booth, 2020). Indeed, the UN Special Rapporteur on extreme poverty, in his report on digital welfare released at the end of last year, noted the appetite of governments worldwide to invest in digital welfare and warned against the grave risk of "stumbling, zombie-like, into a digital welfare dystopia" (UNOHCHR, 2019).

Data protection laws and frameworks should impose restrictions and safeguards on how data may be used to make automated decisions due to the intensified risks these decisions present to human rights and freedoms, as well as to issues such as fairness, transparency and accountability.

On the one hand, if social protection programmes assess that there are risks involved in implementing automated decisions, some human control must be present (semi-automated process). On the other hand, beneficiaries of social protection programmes should have the right not to be subject to purely automated decision-making that produces legal or other significant effects concerning him or her, such as the automatic refusal of a social benefit.[34] For instance, the GDPR, Article 22 (1), "establishes a general prohibition for decision-making based solely on automated processing. This prohibition applies whether or not the data subject takes an action regarding the processing of their personal data" (Article 29 Working Party, 2018, p. 19).

Automated decision-making without human intervention should be subject to very strict limitations. If the automated decision is authorised by a law to which the data controller is subject, then social protection authorities should implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, such as the right of an individual to human intervention on the part of the controller, to express his or her point of view and to obtain an explanation of the decision reached after such assessment ('right to explanation'), and to challenge the decision.[35] One significant concern is the time it can take to challenge these decisions, and the harm beneficiaries can suffer in the interim. To address this, maybe it would be helpful to ensure that decisions to cut off benefits or other decisions of similar severity either cannot be made solely through automated decision-making (i.e. human intervention is required before they are implemented), or that if a beneficiary challenges such a decision, the benefits are reinstated while the challenge is pending. Compensation after the fact will be little comfort to someone who has lost their home, for instance, while working their way through the process.

[33] A well-known example is COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), a risk assessment system software that produces automated risk scores in the criminal justice system, calculating a score that predicts the likelihood of an individual committing a future crime. Even though the final decision is formally made by a judge, the automated decision made by a programme can be decisive and has led to inaccurate, discriminatory and unfair decisions (for further information, see Privacy International, 2018).

[34] See CoE Convention No. 108, Art. 9 (1) (a); GDPR Art. 22. According to GDPR, Art. 22 (2), "Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent".

[35] See OECD Privacy Framework, Para. 75.

As part of their DPIA, social protection programmes should identify and record the degree of human involvement in the decision-making process and at what stage this takes place. According to the Article 29 Working Party:

> *To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision. As part of the analysis, they should consider all the relevant data.* (Article 29 Working Party, 2018, p. 21)

In addition, social protection authorities should carry out regular checks to make sure that their systems are working as intended regarding the decision-making process.

POINTS FOR DISCUSSION:

- Which types of social protection processes are suitable for automation, and where should automation be avoided? When is human involvement indispensable?
- How can we ensure that automation enables rather than hinders social protection?
- How is automated decision-making being used by social protection programmes in low- and middle-income countries? Are authorities willing to evaluate and take into account such aspects when developing a programme?
- Who is responsible when human rights are infringed based on algorithmically-prepared decisions?

5 FINAL THOUGHTS

The introduction of new technologies in social protection programmes must not happen at the expense of human rights. There are numerous examples where development and humanitarian aid initiatives are enabling surveillance in developing countries by pushing the adoption of biometric systems or integration of single registries inside or between countries (i.e. social protection registries with law enforcement registries) (Hosein & Nyst, 2013). During our research, we have also encountered examples where the introduction of new technologies harms the core mission of the social protection programme (e.g. to support the most vulnerable) and any additional technology should be measured against its ability to fulfil that mission, to ensure it enables rather than hinders social protection systems.

Crucially, any potential interference with human rights in areas such as data protection or discrimination needs to be met with an increased level of transparency. This is to ensure that the beneficiaries and their representatives are able to understand and scrutinise such decisions fully and, if necessary, challenge them in court. Without the ability to challenge these decisions and ensure meaningful accountability for them, any additional introduction of new technologies, or the ongoing use of existing technologies that fail this test, is difficult to justify within a human rights framework. Additionally, effective redress mechanisms for individuals whose rights are infringed by new technologies (e.g. automated decision-making systems) are also essential.

Data protection and privacy by design[36] is definitely desirable and ideal – in other words, these rights must be integrated from the outset in the design stage of social protection systems. However, the reality in different countries is diverse: some have no national data protection laws; others have national laws, but they have not yet been effectively implemented by the social protection authorities; social protection programmes may be already underway in the country and authorities are trying to incorporate the principles of data protection and privacy along the way; or the country may be just beginning to design social protection programmes.

Each of these realities requires different approaches. When a 'privacy by design' approach is not possible, other measures must be developed to raise awareness and ensure compliance with data protection and privacy principles. Fundamental, and recurring, questions include: What would be the minimum requirements for ensuring data protection and privacy in the specific context of social protection programmes? What ought to be minimum standards of transparency and accountability for those programmes?

Finally, our analysis suggests that the most significant contribution to the current discussion in low- and middle-income countries could be to provide an easily accessible guideline on data protection for the social protection field, discussing issues in a non-technical and simplified way. The guideline's primary aims would be to increase awareness regarding data protection and support actors (mainly local governments, social protection authorities, policymakers and practitioners) in the decision-making process in the different stages of social protection programmes: design, implementation and evaluation.

[36] See GDPR and Privacy International (2018).

REFERENCES

Article 29 Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01, European Commission, Brussels, 2018.

Banisar, David, *National Comprehensive Data Protection/ Privacy Laws and Bills 2019*, 2019.

Barca, Valentina & Chirchir, Richard, *Building an Integrated and Digital Social Protection Information System*, GIZ, Bonn, 2019.

Council of Europe, *Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (No.108)*, 2018.

European Parliament & Council of Europe, *Regulation (EU) 2016/679 of the European Parliament and of the Council of Europe on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation – GDPR)*, 2016.

Henley, John & Booth, Robert, 'Welfare Surveillance System Violates Human Rights, Dutch Court Rules', *The Guardian*, 5 February 2020, https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules

Hosein, Gust & Nyst, Carly, *Aiding Surveillance: An Exploration of How Development and Humanitarian Aid Initiatives Are Enabling Surveillance in Developing Countries*, Privacy International, 2013.

ISPA, *Identification Systems for Social Protection. "What Matters" Guidance Note*, Inter Agency Social Protection Assessments Partnership, Washington, DC, 2016.

Kuner, Christopher, *Handbook on Data Protection in Humanitarian Action*, ICRC, Geneva, 2017.

MSI-NET, *Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications. Prepared by the Committee of Experts on Internet Intermediaries (MSI-NET)*, DGI(2017)12, Council of Europe, Strasbourg, 2018.

OECD, *The OECD Privacy Framework*, Organisation for Economic Co-operation and Development, 2013.

Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection*, Privacy International, London, 2018.

Privacy International, 'The SyRI Case: A Landmark Ruling for Benefits Claimants Around the World', 24 February 2020, https://www.privacyinternational.org/news-analysis/3363/syri-case-landmark-ruling-benefits-claimants-around-world

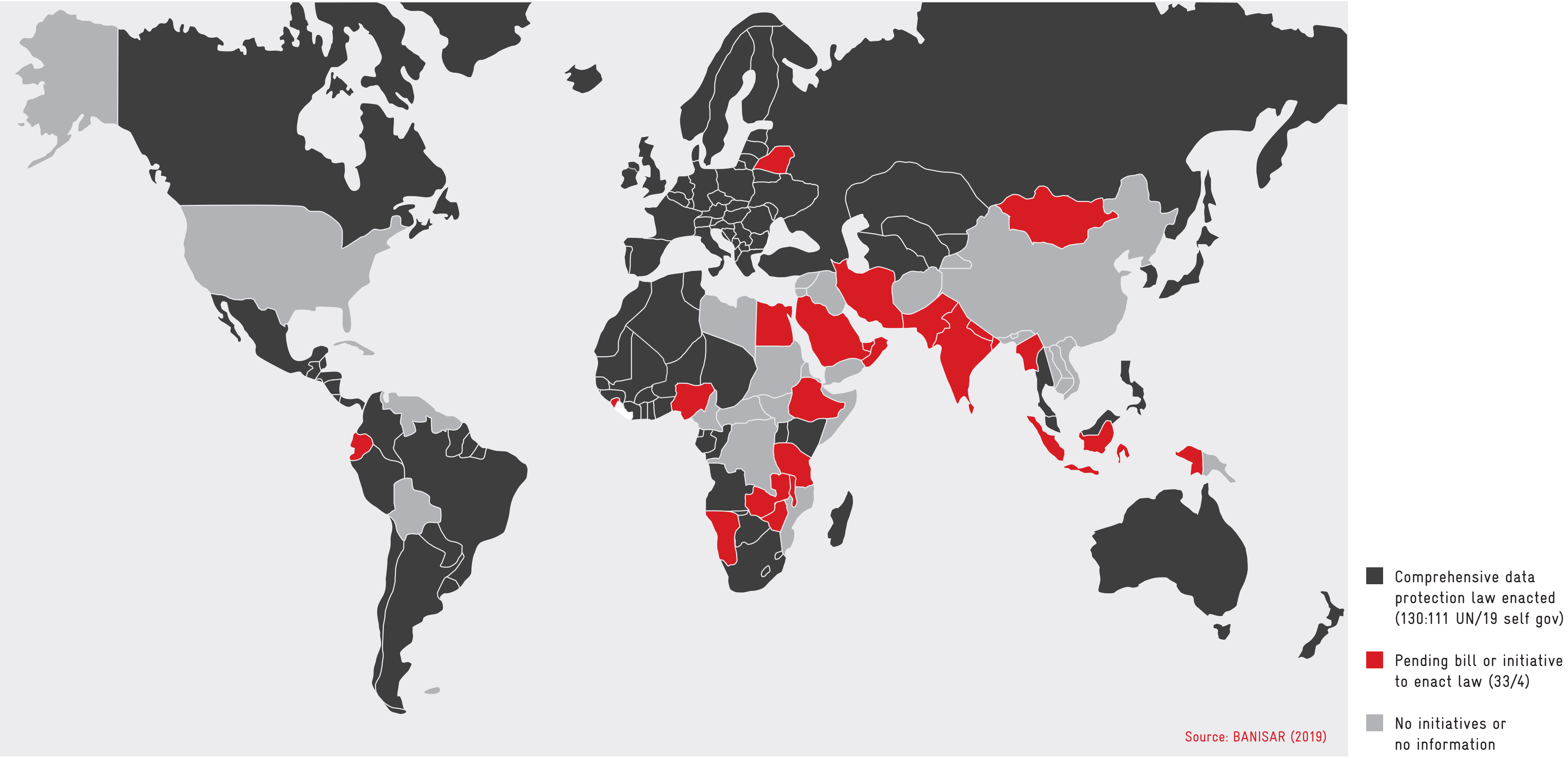
Sepúlveda Carmona, Magdalena, *Is Biometric Technology in Social Protection Programmes Illegal or Arbitrary? An Analysis of Privacy and Data Protection. Extension of Social Security (ESS)*, Working Paper No. 59, International Labour Organization, Geneva, 2018.

United Nations, *Guidelines for the Regulation of Computerized Personal Data Files*, 1990.

United Nations, *Personal Data Protection and Privacy Principles*, 2018.

UNOHCHR, 'World Stumbling Zombie-Like into a Digital Welfare Dystopia, Warns UN Human Rights Expert', United Nations Office of the High Commissioner for Human Rights, 17 October 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156

ANNEX 1:
NATIONAL COMPREHENSIVE DATA PROTECTION/PRIVACY LAWS AND BILLS, 2019



Source: BANISAR (2019)

⬛ Comprehensive data protection law enacted (130:111 UN/19 self gov)

🟥 Pending bill or initiative to enact law (33/4)

⬜ No initiatives or no information

IMPRINT

As a federally owned enterprise, GIZ supports the German Governmentin achieving its objectives in the field of international cooperation for sustainable development.

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices:
Bonn and Eschborn

Address:

Friedrich-Ebert-Allee 32 + 36
53113 Bonn / Germany
T +49 228 44 60 - 0
F +49 228 44 60 - 17 66

Dag-Hammerskjöld-Weg 1-5
65760 Eschborn / Germany
T +49 61 96 79 - 0
F +49 61 96 79 - 11 15

E info@giz.de
I www.giz.de

Programme/project description:
Data protection for social protection: key issues for low- and middle-income countries

Authors:
Ben Wagner, Carolina Ferro, Enabling-Digital.eu

Responsible for the content:
Ralf Radermacher (GIZ)

Coordination:
Dominique Leska, Christina Betting, Kelvin Hui,
Ralf Radermacher, Christian Merz and Tatjana Schock

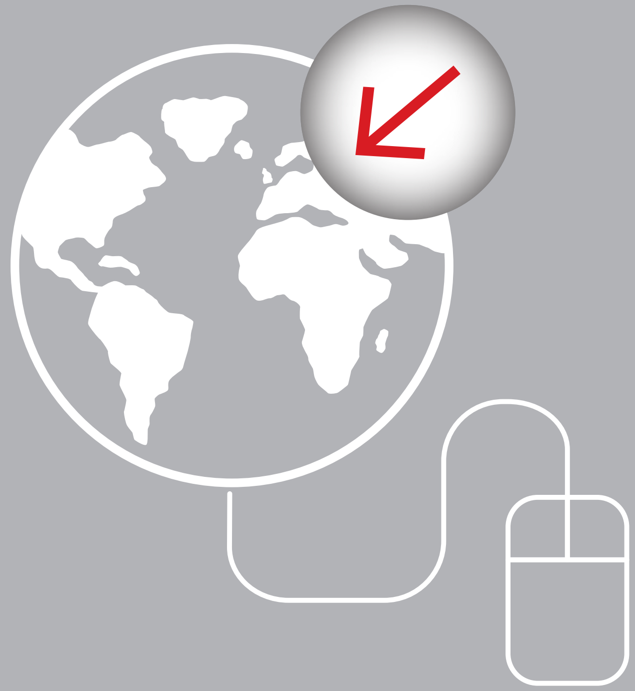
Editing:
Susan Sellars

Layout / Illustrations:
Kommunikationsagentur GmbH
Scheufele Hesse Eigler
Frankfurt am Main

Maps:
The maps printed here are intended only for information purposes and in no way constitute recognition under international law of boundaries and territories. GIZ accepts no responsibility for these maps being entirely up to date, correct or complete. All liability for any damage, direct or indirect, resulting from their use is excluded.

On behalf of:
German Federal Ministry for Economic Cooperation and Development (BMZ)

Bonn, August 2020



Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices:
Bonn and Eschborn

Friedrich-Ebert-Allee 32 + 36
53113 Bonn / Germany
T +49 228 44 60-0
F +49 228 44 60-17 66

Dag-Hammarskjöld-Weg 1–5
65760 Eschborn / Germany
T +49 61 96 79-0
F +49 61 96 79-11 15

E info@giz.de
I www.giz.de

f www.facebook.de/gizprofile
t twitter.com/giz_gmbh

On behalf of

Federal Ministry
for Economic Cooperation
and Development