SPIAC-B Workstream
on Data Protection
(Working Group on Digital Social Protection)

IMPLEMENTATION GUIDE

Good Practices for Ensuring Data Protection and Privacy in Social Protection Systems

A guide for practitioners working and advising in low and middle-income countries

Commissioned by GIZ's Sector Initiative Social Protection

Drafted by Ben Wagner, Carolina Ferro,

Jacqueline Stein-Kaempfe

September 2021

Contents

Acknowledgements **4**

Joint statement of the SPIAC-B's working group on Digital Social Protection **5**

List of Tables **7**

List of Figures **7**

List of Boxes **7**

Glossary of defined terms and abbreviations **10**

Introduction **17**

1. Personal data protection and privacy **19**

1.1. What is personal data protection and privacy? 19

1.2. International and regional data protection and privacy instruments 21

1.3. Key terms you should know 23

2. Why is personal data protection critical for social protection programmes? 25

2.1. Social protection and personal data 25

2.2. Why is data protection needed in social protection? 29

2.3. Main stakeholders and responsibilities 31

2.4. Digital technologies increase the urgency of data protection 32

2.5. There is no contradiction between the right to (data) privacy and the right to social protection 33

3. Good international practice of data protection and privacy **35**

3.1. Data protection and privacy standards 35

3.2. Data processing principles 36

3.2.1. Purpose specification 37

3.2.2. Data minimisation 38

3.2.3. Lawfulness, fairness and transparency 39

3.2.4. Accuracy 41

3.2.5. Retention limitation 42

3.2.6. Security 42
3.2.7. Accountability 45
3.3. Data subject rights 45
3.3.1. Right to information 46
3.3.2. Right to access 47
3.3.3. Right to rectification 48
3.3.4. Right to erasure 48
3.3.5. Right to withdraw consent and to object to data processing 49
3.3.6. Rights related to automated decision making and profiling 50
3.3.7. Right to complain to an independent body (administrative remedy) 53
3.3.8. Right to an effective judicial remedy 54
3.4. Accountability, oversight and enforcement 54
3.4.1. Accountability: Legal obligations of data controllers and processors 55
3.4.2. Independent oversight 58
3.4.3. Enforcement: Administrative and judicial redress 59
3.5. International data sharing 59
3.6. Sensitive personal data 61
4. How to implement data protection and privacy into social protection programmes? 64
4.1. How to promote and adopt standards for data protection and privacy? 64
4.1.1. National data protection and privacy law 64
4.1.2. Organisational data protection and privacy policy 65
4.1.3. Data management protocol for each social protection programme 69
4.2. How to conduct a data protection impact assessment (DPIA) and ensure privacy by design? 70

4.3. How to apply the data protection and privacy standards to social protection programmes? 74
4.3.1. How to limit processing in line with the data processing principles? 74
4.3.2. How to ensure that data subjects can exercise their rights? 106
4.3.3. How to be an accountable social protection controller? 115
4.3.4. How to share data? 119
4.4. How to work with providers of digital technologies? 123
4.4.1. Steps for ensuring privacy compliance by technology providers . 124
4.4.2. Data protection and privacy challenges of specific technologies . 127
References 147

`

Acknowledgements

(To be written after contributions of SPIAC-B's members).

Joint statement of the SPIAC-B's working group on Digital Social Protection

We—the subscribing United Nations system organisations, and bilateral development agencies, donor governments, and civil society organisations, gathered within the Social Protection Inter-Agency Cooperation Board (SPIAC-B),[1] under a dedicated working group on Digital Social Protection—stress the importance of ensuring that national social protection systems secure respect for the right to privacy and assure the protection of personal data.

Ideally, this aim should be achieved in conformity with a more extensive, nationwide data protection and privacy regime built upon constitutional rights and a national data protection law. However, even in the absence of the preceding, it should be accomplished by operating under protocols that give robust assurance of personal data and privacy protection to any individual, family or household that applies or registers for social protection benefits or services.

In this sense, the SPIAC-B members commit to supporting partner governments in their efforts to incorporate the data protection and privacy principles into the (further) development and management of their social protection systems. Accordingly, aiming to assist and guide national governments and other relevant actors in achieving the stated goal, we created an Implementation Guide of "Good Practices for Ensuring Data Protection and Privacy in Social Protection Systems" and are committed to promoting it in our respective work. It is a practical and sector-specific guide, specially adapted to the context of social protection systems in low and middle-income countries. It intends to support practitioners while facing some country-specific challenges to comply with national and international data protection and privacy standards and, as applicable, national legal frameworks.

While creating the Implementation Guide, we also endeavour to converge on a common SPIAC-B language and approach when communicating with partner governments to ensure data protection and privacy unites the international development community and is the basis of our cooperation.

---

[1] SPIAC-B is composed of over 20 members. The Board is a light, lean and agile inter-agency coordination mechanism to enhance global coordination and advocacy on social protection issues and to coordinate international cooperation in country demand-driven actions. For more information, see SPIAC-Ba (n.d.).

The absence of data protection and privacy regimes in the design and management of social protection programmes may expose individuals to harm, stigmatisation or discrimination, thereby undermining programmes' objectives. Therefore, we call on partner governments to establish comprehensive national data protection and privacy legal frameworks and on social protection authorities to develop organisational data protection policies and guidelines that assure the application of those regimes, establishing mechanisms that enable transparency, accountability and allow responsible and ethical data use.

We also call upon individuals and civil society organisations to become aware of and demand respect for personal data and privacy protection, including by participating in the formulation of the related policies and guidelines. Building trustworthy systems as a basis for social protection, raising awareness about the associated data protection and privacy challenges, and increasing individuals' participation in social protection systems are essential paths for developing a rights-based approach and the rigorous respect of personal data and privacy.

List of Tables

Table 1 - Obligations of data controllers and data processors

Table 2 - Obligations of entities and data subject rights

List of Figures

Figure 1 - Social protection delivery chain

Figure 2 - Data processing phases

List of Boxes

Legend:

- Definitions and explanations (green)
- Checklist of good practices (purple)
- Implementation tools (blue)
- Examples (yellow)

Box 1- The right to privacy as a fundamental human right 19
Box 2- A word on terminology 21
Box 3 - Most significant internationally agreed-upon data protection and privacy instruments 22
Box 4 - International organisations, non-governmental organisations and applicable law 28
Box 5 - Why should social protection practitioners care about data protection and privacy? 34
Box 6 - Legal bases for processing personal data 40
Box 7 - Security measures 44
Box 8 - Checklist of Good Practices: What information should be provided to data subjects? 46
Box 9 - Checklist of Good Practices: Exercising the right to access 47

Commented [ED1]: Would be great to add a few boxes (2-3) with concrete social protection examples given by the SPIAC-B members.

Box 10 - Checklist of Good Practices: When to exercise the right to erasure? 48
Box 11 - What is automated decision-making and profiling? 51
Box 12 - Checklist of Good Practices: Rights related to automated decision making and profiling 52
Box 13 - Independent supervisory authority/ data protection authority (DPA) 58
Box 14 - Data protection and privacy policy 66
Box 15 - Implementing an organisational data protection and privacy policy 67
Box 16 - Privacy-by-design 70
Box 17 - Data Protection Impact Assessment (DPIA) 71
Box 18 - Implementing a DPIA 71
Box 19 - Checklist of Good Practices: Purpose specification principle 74
Box 20 - Purpose specification and integration of programme databases 76
Box 21 - Purpose specification and social registries 78
Box 22 - Collection of metadata by commercial service providers 80
Box 23 - Checklist of Good Practices: Data minimisation principle 82
Box 24 - Data categories to fulfil data minimisation and purpose specification principles 82
Box 25 - Assessments and pseudonymised data 84
Box 26 - Assurance to donors and data minimisation 85
Box 27 - Checklist of Good Practices: Lawfulness, fairness, and transparency principle 86
Box 28 - Lawful processing of sensitive data 90
Box 29 - Consent: some specific conditions to be considered valid 91
Box 30 - Legal basis and joint programmes of international organisations and social protection authorities 93
Box 31 - Providing information to enable transparency 94
Box 32 - What if individuals do not want to provide their personal data or object to the processing? 95
Box 33 - Checklist of Good Practices: Accuracy principle 95
Box 34 - How to implement the data accuracy principle? 96
Box 35 - Checklist of Good Practices: Retention limitation principle 98
Box 36 - How to implement the retention limitation principle? 99
Box 37 - Erase or anonymise personal data? 100

Box 38 - Checklist of Good Practices: Data security principle 101
Box 39 - Breach notification to data protection authority and/or data subjects 106
Box 40 - Checklist of Good Practices: Rights of data subjects 106
Box 41 - CFM call centre: Compliance with data protection principles 111
Box 42 - Checklist of Good Practices: Accountability principle 115
Box 43 - Data protection office or officer (DPO) 118
Box 44 - Checklist of Good Practices: Data-sharing 119
Box 45 - Data-sharing agreement between controllers 120
Box 46 - Implementing data-sharing agreement between controllers 120
Box 47 - Exchange of data between ministries and integration of databases 122
Box 48 - Checklist of Good Practices: Cloud-based MIS 127
Box 49 - Cloud storage 128
Box 50 - Checklist of Good Practices: Biometric identification systems 133
Box 51 - What is meant when speaking about biometrics or biometric data? 135
Box 52 - Checklist of Good Practices: Automated decision-making 140
Box 53 - Potential risks of automated decision-making and profiling 141
Box 54 - The 'SyRI case' 143

Glossary of defined terms and abbreviations

ADB - Asian Development Bank

Aggregated Data - Such data refers to individual data combined to create high-level data, for instance, by statistical analysis. Aggregate data are used in research by analysts, policymakers or administrators.

AI - Artificial Intelligence is defined as the study of intelligent and rational agents that receive precepts from the environment and perform actions. For example, a rational agent can choose the best action to achieve a goal given the resources available. Machine learning is a type of artificial intelligence that refers to algorithms that can improve their model using training data. Machine learning algorithms can make various predictions and make decisions.

Algorithm - An algorithm refers to a clear instruction to solve a problem or a class of problems. Algorithms consist of a finite number of instructions.

Anonymised Data - Any data set consisting of data, which does not allow for the re-identification of individuals using processing, sharing, or publication is anonymous. Anonymised data is not considered personal data. Thus, for example, a beneficiary list with several data variables per person (name, age, gender, address, ID, benefit amount, income), from which all identifiers (namely, name, address, ID) have been irreversibly deleted, can be considered anonymised data. Data protection and privacy frameworks do not apply to anonymised data or other aggregate or statistical data which do not relate to individual persons. This Implementation Guide, however, applies also to non-personal data if it is assessed as sensitive (see below).

API - Application Programming Interface

Automated Decision-Making - Or also called algorithmic decision making or systems refers to automated or semi-automated systems using the analysis of large amounts of (personal) data to make decisions. These systems might be semi-automated and include human supervision or they might be fully automated, making decisions without human supervision or intervention.

Big Data or Data Analytics - Big Data describes very large datasets that entail information from various sources. These are too big to be dealt with traditional data-processing applications and provide bigger statistical power. Data analytics refers to the analysis of such large datasets, usually in the context of predictive analytics or the analysis of user behaviour.

Biometric data - Biometrics refer to unique human characteristics such as individual biological traits like the iris or fingerprints or behavioural characteristics like gait. An individual's biometric data is unique. Therefore, they create specific implications for personal data protection and privacy, and they are used as an identifier in passports, identity cards, among others.

BOMS - The Beneficiary Operations Management System provides inputs for the provision of benefits. During the beneficiary operations management stage, which is part of the delivery chain, inputs from the payroll are allocated to beneficiaries who are part of the programme, and their status is updated. The stages serve maintenance and continuous improvement in case of errors, grievances, inefficiency, lack of accountability or fraud during programmes. The inputs to beneficiary operations management include the beneficiary registry, information on benefits and services, and the related conditionalities. Outputs of the beneficiary operations management include revisions of benefits, services and the beneficiary registry. These are conducted for the implementation cycle of a programme.

CFM - Complaint and Feedback Mechanisms

CoE - Council of Europe

COMPAS - Correctional Offender Management Profiling for Alternative Sanctions

Consent - Consent generally applies if a natural person voluntarily agrees to a proposal. It is a crucial concept and legal basis for personal data processing. According to various data protection regulations and frameworks, such as the GDPR and the CoE Convention 108+, consent must be given freely, voluntarily, informed and unambiguously by data subjects for personal data processing to take place legally. The issue of consent is challenging if data subjects cannot give their consent or the enforceability of obtaining lawful consent is impaired.

Data controller - A natural or legal person (e.g., government, United Nations system organisation, development agency, private company), be it public or private, who

alone or jointly with others determines the means of and purposes for processing personal data. The controller is usually the main responsible towards data subjects for safeguarding their personal data and respecting their rights. In most international data protection and privacy frameworks, controllership is a factual determination, not an appointment. For example, if an employee of a social protection ministry, ultra vires, meaning beyond his/her competences, shares a data set with a private company for marketing purposes, then such employee—determining the purpose and means of such data processing—would become a controller and be responsible (and liable) towards the data subjects for any violation of the applicable data protection and privacy framework.

Data processing - Any operation or set of operations performed on personal data, whether or not by automated means, such as the collection, recording, storage, consultation, use, disclosure by transmission, dissemination, restriction, erasure or destruction.

Data processor - Any natural or legal person, who processes personal data on behalf of the 'data controller'. This concept is not reflected in all international data protection and privacy frameworks. The idea is that the data processor is not taking any decisions with respect to the data processing, but mainly implements the instructions of the controller. Implementing partners, financial or technological service providers and international organisations can be processors of a government implementing a social protection programme. The processor may be instructed by the data controller to assume specific data processing tasks, such as the collection of the data and information of the data subjects about the data processing, or the implementation of a complaint and feedback mechanism on behalf of the data controller.

Data Subject - Any individual whose personal data is being processed. In social protection programmes, data subjects include those participating in programmes as applicants, registrants, recipients or beneficiaries.

DG INTPA - European Commission Directorate-General for International Partnerships (DG DEVCO, Directorate-General for Cooperation and Development until 2021)

DIAL - The Digital Impact Alliance

DFAT/AusAID - Department of Foreign Affairs and Trade of Australia/Australian Aid

DPA - Data Protection Authority is an independent public authority established by the government to supervise compliance with data protection and privacy legislation. These authorities are generally responsible for providing guidance on national data protection legislation, responding to complaints by data subjects, enforcing data protection laws by investigating alleged privacy violations and imposing sanctions when the law is breached. The DPA is also largely charged with the application of the law through the issuing of regulations, offering of guidance and cooperation with other authorities, public and private, where the processing of personal data might be involved.

DPIA - A Data Protection Impact Assessment aims to evaluate, identify and communicate the risks of personal data processing in the context of a project, programme or initiative. The DPIA should ultimately inform the data subject of such risks and support mitigating and avoiding data protection and privacy risks. The DPIA should be active for the duration of a programme or initiative and monitor the rise of new threats and the changes throughout the process.

DPO - A Data Protection Office or Officer is a designated individual or team working independently in an organisation that ensures data protection regulations are upheld, and the rights of data subjects are respected.

ECG - Electrocardiogram, which measures the heartbeat

ECOWAS - Economic Community of West African States

EEG - Electroencephalogram, which measures brain activity.

EU - European Union

GDPR - General Data Protection Regulation of the European Union

GIZ - German Corporation for International Cooperation GmbH

ICT - Information and Communications Technology

ID - Identity Document

Information custodian - The role of information custodian or steward, also called a data custodian, is an individual responsible for maintaining and supporting the IT

infrastructure and the associated data following the organisation's requirements or programme.

ISSA - Information Systems Security Association

Information owner - An information owner has essential security responsibilities. Usually, the term refers to a lead administrator of a programme, data controller or initiative. Therefore, the role is often referred to as 'data owner' or simply 'owner'. Assigning an information owner is an essential step, e.g., for GDPR compliance, to ensure accountability, define policies accurately, create trusted data, for instance, by customers, and reduce redundant work.

ILO - International Labour Organisation

IO - International Organisation means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more states. Development and humanitarian agencies can be international inter-governmental organisations.

ISPA - Interagency Social Protection Assessment

IT - Information technology is the use of computers to create, process, store, and exchange all kinds of electronic data and information. I

MIS - A Management Information System supports the implementation of social protection programmes. The system is a specific information technology to integrate data and information management. That includes a database to store information about beneficiaries and application software to systematise information.

MSI-NET - Committee of Experts on Internet Intermediaries

NGO - Non-Governmental Organisation

OECD - Organisation for Economic Co-operation and Development

Personal data - Means any information or set(s) of information that, either by itself or together with other relevant data, can be used to identify an individual (known as the 'data subject'), directly or indirectly, via an identifier (such as an identification number) or via one or more factors specific to the person's physical, physiological,

genetic, mental, economic, cultural or social identity. It can be held in both electronic and physical form.

Profiling - In the context of personal data processing, profiling refers to the examination of data from a database by means of automated processing. That procedure often involves the evaluation of a data subject's personal information to predict his or her performance, health, personal preferences, interests or behaviour.

Pseudonymised data - Data that has been processed in such a way that they cannot lead to the re-identification of a data subject without additional information and technical or organisational measures. Such data may still be considered personal data.

Sensitive personal data - Some data protection and privacy frameworks include the additional category of sensitive data as a sub-category of personal data. For the purposes of this Implementation Guide, sensitive data shall mean any personal data, which, if disclosed, may result in discrimination against or the repression of an individual, by limiting or negating its rights. It typically includes information such as race, ethnicity, medical information, sexual orientation, political opinions, philosophical and other beliefs, membership of associations or trade unions, religious affiliation, genetic data, biometric data (when processed solely to identify a natural person), among others. Other types of information (personal and non-personal) can be sensitive for certain groups in particular circumstances, such as the status as refugee, migrant or asylum seeker, people living in humanitarian crisis zones. In some cases, even information that appears to be non-sensitive could be sensitive and may create risks to a person's safety, either alone or in combination with other data held or publicly available. Thus, the sensitivity of data needs to be considered on a case-by-case basis.

Social Registries - Also called Single Registries, are systems to determine the eligibility of social programmes and support their outreach, intake and registration. As an inclusion system, they allow individuals and families to be included in social programmes. As information systems, they support registration and determination of eligibility for social programmes. Furthermore, they hold all information about prospective and included participants of social programmes.

SPIAC-B - Social Protection Interagency Cooperation Board

`

SPIS - Social Protection Information Systems enable the flow and management of information within the social protection sector and other sectors (e.g., education, health or agriculture). They provide a resource to deliver, monitor and manage benefits in social protection programmes.

SyRI - System Risk Indication

UN - United Nations

WFP - World Food Program

Introduction

Why an Implementation Guide of good practices for ensuring data protection and privacy in social protection?

In low and middle-income countries, social protection practitioners may face specific challenges in complying with national and international data protection and privacy standards and, as applicable, national legal frameworks. In consequence, they need special attention and support.

In this context, the Social Protection Inter-Agency Cooperation Board (SPIAC-B) created a workstream on Data Protection under a dedicated working group on Digital Social Protection, led by GIZ Sector Initiative on Social Protection in partnership with the ILO, ISSA, the World Bank, DG INTPA, WFP, DFAT/AusAID, ADB, DIAL, and others.

To encourage and support partner governments in their efforts to ensure data protection and privacy in social protection systems, the working group has developed this Implementation Guide. It is a practical and sector-specific guide, specially adapted to the context of social protection systems in low and middle-income countries.

It seeks to serve as a tool that will offer guidance, increase awareness and support people on the ground in the decision-making process for designing delivery structures of social protection schemes and programmes, while dealing with the country-specific challenges involved in complying with data protection and privacy principles and legal requirements, particularly when digital technologies are employed.

The Implementation Guide is not an end-state, but guidance built in such a way that each social protection system or programme can adapt it to its specific context. It builds on existing national and international data protection and privacy guidelines, frameworks, laws and regulations. Besides, it is based on and further develops the SPIAC-B working group on Digital Social Protection discussion, initiated in the Issue Paper entitled "Data protection for social protection: key issues for low- and middle-income countries".[2]

[2] GIZ 2020.

`

Who is this Implementation Guide for?

It is aimed at practitioners involved in the design, implementation and expansion of social protection systems and programmes at the country level, especially regarding non-contributory schemes. These include national and local government partners, policymakers, social protection authorities and ministries, managers of social protection programmes, social workers and other professionals responsible for implementing programmes, civil society organisations, donors and the private sector.

It is equally intended for managers and programme staff of development and humanitarian agencies supporting local authorities in the implementation of their social protection systems and programmes, particularly those in charge of advising on and applying data protection and privacy standards.

Finally, it also provides useful information for any individual, household or family participating in social protection programmes as applicants, registrants or beneficiaries. In other words, for the 'data subjects'.[3]

Why is this Implementation Guide important for your work?

If you don't understand why the protection and privacy of personal data is essential for your work or you do have a notion but don't know where to start, this guide is for you.

This guide explains what is currently understood by personal data protection and privacy (Chapter 1).

It explains why the protection of personal data is necessary for any social protection programme (Chapter 2).

It presents international practices that could serve as a reference and inspiration for national data protection laws and as a framework for social protection programmes (Chapter 3).

Finally, it provides you with step-by-step guidance and practical measures that will help in implementing the data protection and privacy principles into social protection programmes and respect individuals' rights to data protection (Chapter 4).

---

[3] See 'Glossary of defined terms and abbreviations.'

1. Personal data protection and privacy

1.1. What is personal data protection and privacy?

Privacy of individuals' **personal data** is an essential element of the right to privacy. This element is called **data privacy** and is increasingly relevant to people's lives.

Since the invention of computers, our personal information is increasingly processed through digital means and moves in seconds through systems around the world, becoming sometimes more challenging to protect than our homes or our letter correspondence.[4] In this context, the concept of **personal data protection** has gained importance in realising the right to (data) privacy.

Data privacy and data protection are intrinsically linked. In this Implementation Guide the term **'personal data protection and privacy'** will be used to refer to the appropriate and permissioned use, governance, and protection of personal data.

Box 1- The right to privacy as a fundamental human right

Privacy is a fundamental human right that recognises the right of individuals to be free from arbitrary or unlawful interference with matters of personal nature (such as their body, family, home, correspondence, property, thoughts, feelings, personal information), or unlawful attacks on their honour and reputation. It is enshrined in several international human rights treaties and documents, widely ratified by states, contained in many conventions at the regional level, as well as national constitutions and bills-of-rights.

Privacy is essential to our autonomy and the protection of human dignity. It recognises that there is a need to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us and shielding ourselves from others who may wish to exercise control over us.

[4] UN General Assembly, Resolution 73/179, 2018, Resolution 42/15, 2019, and Resolution 75/176, 2020.

`

Through the below instruments, states are called upon to respect such rights, and create laws which protect the sphere of privacy.

International human rights instruments
- Universal Declaration of Human Rights (UDHR) – Article 12
- International Covenant on Civil and Political Rights (ICCPR) – Article 17
- Convention on the Rights of the Child – Article 16
- Convention on the Protection of All Migrant Workers and Members of their Families – Article 14

Regional human rights instruments
- African Charter on the Rights and Welfare of the Child – Article 10
- African Union Principles on Freedom of Expression – Principle IV
- American Convention on Human Rights – Article 11
- Association of Southeast Asian Nations (ASEAN) Human Rights Declaration - Principle 21
- Arab Charter on Human Rights – Article 21
- Charter of Fundamental Rights of the European Union – Article 7
- European Convention for the Protection of Human Rights and Fundamental Freedoms – Article 8

A full enjoyment of the right to (data) privacy requires that the personal data is actively protected, and the processing regulated. Data protection and privacy sets up clear obligations for those who control or process data to take measures to protect personal data and to mitigate interference with the right to privacy. And it holds them to account when they fail to comply with obligations. Through specific data-related rights granted to data subjects (so-called data subject rights)[5] individuals are enabled to better control the information relating to them.

However, the right to privacy is not absolute. The laws protecting privacy, including data privacy, thus need to strike a balance with other rights (such as the freedom of expression) and set out the necessity of the right to privacy in the interest, for example, of the prevention of crime, public safety, or the work of the judiciary. Significant interferences with the constitutionally recognised right to privacy need to be based on law and cannot be done without laws guaranteeing that the interference will be legitimate and proportional.

[5] See Section 3.3. – Data subject rights.

In sum, while 'privacy' is broader and covers many areas of the private life beyond personal information, 'personal data protection and privacy' covers the right to be free from unlawful interference with our own personal information. Personal data protection and privacy means the fair, transparent and lawful use of information about people, set up as a legal framework restricting the processing of personal data by authorities, companies and individuals, and grants rights to individuals empowering them to protect their data from abuse.

Box 2- A word on terminology

In this Implementation Guide the term **'data protection and privacy'** will be used.

Different legal systems and cultures use different terms to refer to the same or related concept. In some organisational or legal frameworks, for instance, the term 'data privacy' or 'data protection' may be used instead. Sometimes these two terms are used as interchangeable, and other times as different concepts.

Data protection and privacy frameworks are used in this Implementation Guide as the set of standards (whether as incorporated by laws, treaties, or non-binding principles or guidelines) which limit the processing of any personal data by any natural or legal person.

Data protection and privacy standards are the elements of data protection and privacy frameworks identified as good practices by this Implementation Guide.[6]

1.2. International and regional data protection and privacy instruments

The need for data protection and privacy laws was first recognised by a number of countries, mostly in Europe, in 1960. Trans-border flow of data soon required a harmonisation of those laws. As a result, regional and international bodies engaged in the formulation of common data protection and privacy standards, agreeable to the members of the respective bodies.

Until today, **there are no universally recognised data protection and privacy standards.** What is available on an international level are international treaties

[6] See Section 3.1. – Data protection and privacy standards.

between states (CoE Convention 108+, ECOWAS, and Malabo Convention), guidelines or principles issued by international organisations like the United Nations and the OECD, and regional bodies that have agreed upon frameworks, guidelines, or principles.

Box 3 - Most significant internationally agreed-upon data protection and privacy instruments [7]

Data protection guidelines and principles by international organisations (non-binding)

- 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
- United Nations (UN) General Assembly Resolution, Guidelines for the Regulation of Computerised Personal Data Files, 1990 – addresses member states of the UN and governmental international organisations
- UN Personal Data Protection and Privacy Principles, 2018 – issued by the High-Level Management Committee of the United Nations, following approval by United Nations systems organisations; addresses only UN systems organisations

International and regional data protection treaties between states (binding)

- 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 (CoE Convention 108+)
- Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection, 2010
- African Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014 – the Convention is not yet in force, as only eight out of minimum 15 states have ratified it
- European Union (EU), General Data Protection Regulation (GDPR), 2016/679 - which has direct legal effect in all EU member states, like a national law

Regional data protection guidelines (non-binding)

- Asia-Pacific Economic Cooperation (APEC) Privacy Framework, 2005, as amended in 2015
- Association of Southeast Asian Nations (ASEAN) Framework on Personal Data Protection, 2016

[7] For a more detailed overview, see Annex 1.

1.3. Key terms you should know[8]

Personal data: Means any information or set(s) of information that, either by itself or together with other relevant data, can be used to identify an individual (known as the 'data subject'), directly or indirectly, via an identifier (such as an identification number) or via one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. It can be held in both electronic and physical form.

Data subject: Any individual whose personal data is being processed. In social protection programmes, data subjects include those participating in programmes as applicants, registrants, recipients or beneficiaries.

Data processing: Any operation or set of operations performed on personal data, whether or not by automated means, such as the collection, recording, storage, consultation, use, disclosure by transmission, dissemination, restriction, erasure or destruction.

Data controller: A natural or legal person (e.g., government, United Nations system organisation, development agency, private company), be it public or private, who alone or jointly with others determines the means of and purposes for processing personal data. The controller is usually the main responsible towards data subjects for safeguarding their personal data and respecting their rights. In most international data protection and privacy frameworks, controllership is a factual determination, not an appointment. For example, if an employee of a social protection ministry, ultra vires, meaning beyond his/her competences, shares a data set with a private company for marketing purposes, then such employee – determining the purpose and means of such data processing – would become a controller and be responsible (and liable) towards the data subjects for any violation of the applicable data protection and privacy framework.

Data processor: Any natural or legal person, who processes personal data on behalf of the 'data controller'. This concept is not reflected in all international data protection and privacy frameworks. The idea is that the data processor is not taking

[8] For a broader definition of key terms, see 'Glossary of defined terms and abbreviations.'

any decisions with respect to the data processing, but mainly implements the instructions of the controller. Implementing partners, financial or technological service providers and international organisations can be processors of a government implementing a social protection programme. The processor may be instructed by the data controller to assume specific data processing tasks, such as the collection of the data and information of the data subjects about the data processing, or the implementation of a complaint and feedback mechanism on behalf of the data controller.

2. Why is personal data protection critical for social protection programmes?

2.1. Social protection and personal data

Social protection has slightly different meanings for different institutions. For example, the SPIAC-B defines social protection as:

> "Social protection encompasses the set of policies and programmes aimed at preventing or protecting all people against poverty, vulnerability and social exclusion, throughout the lifecycle, with a particular emphasis on vulnerable groups. Social protection includes social assistance, social insurance, and labour market interventions. It can be provided in cash or in-kind, through non-contributory and contributory schemes, and by building human capital, productive assets, and access to jobs."[9]

Furthermore, social protection is a human right,[10] and social protection programmes and policies support individuals and societies with risk management. Therefore, social protection programmes include instruments to improve resilience, equity and opportunity.[11] Social protection interventions include various types, such as categorical programs for child allowances or social pensions, conditional and unconditional cash transfers, unemployment and disability assistance and insurance, active labour market programs, employment services, training services, social and social work services.[12] These components vary from country to country, and programmes are often government-owned. Social protection programmes usually target poor, marginalised or vulnerable groups to increase the presence and effectiveness of safety nets.[13] However, depending on the programme, different population groups are intended, like children, the elderly, low-income families, the

[9] SPIAC-Bb, n.d.
[10] United Nations 2015 (Art. 23 and 25).
[11] Leite et al. 2017 (p. 96).
[12] Lindert et al. 2020 (p. 2).
[13] WFP 2017.

unemployed, persons with disabilities, and individuals facing social risks such as children or youth.[14]

Various social protection programmes are employed to support different individuals and groups.

Two major groups of social protection programmes can be distinguished according to financing mechanisms: Contributory and non-contributory schemes. These often coexist and provide different benefits to different individuals and groups of society. In **contributory schemes**, the beneficiaries need to contribute and thus determine the entitlement to benefits. For instance, social insurance schemes for employees grant health care and social services, including cash benefits for specific situations (e.g., maternity, unemployment, old age). However, in **non-contributory schemes**, beneficiaries do not need to contribute to receive benefits. Taxes and other state revenues often finance these schemes.[15]

In **low- and middle-income countries,** social protection programmes most often target vulnerable populations.[16] Therefore, the focus of programmes in these countries is on the so-called "social assistance", based on non-contributory schemes, namely the transfer of resources, either cash or in-kind, to vulnerable individuals or households with no other means of adequate support.

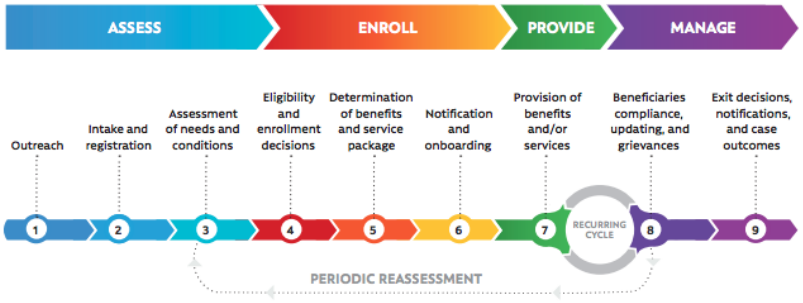
Accordingly, this Implementation Guide seeks to support social protection practitioners in low- and middle-income countries working principally in non-contributory schemes (but now exclusively) while facing some country-specific challenges to comply with national and international data protection and privacy standards and, as applicable, national legal frameworks.

Information management in social protection programmes

Social protection systems are complex and context-specific. However, social protection programmes worldwide go through similar implementation phases along the delivery chain (see Figure 1).

[14] Lindert et al. 2020 (p. 3).
[15] ILO 2018.
[16] WFP 2017.

Figure 1: Social protection delivery chain[17]



Many social protection programmes use **management information systems (MIS)[18]** to manage programme's datasets. The MIS of a programme supports the delivery of its implementation phases (Figure 1). MIS enables information flow and management for critical processes. It consists of application software, hardware, databases, telecommunications systems and staff.[19] It collects a lot of data, which is in the hands of governments and technology providers. Various core functions can be integrated across programmes on integrated digital platforms, the so-called **integrated management information system**.[20]

In addition, organisations use information and inclusion systems called **social registries** to determine the eligibility of individuals for social protection programmes and support outreach, intake and registration. These systems support potential beneficiaries and programme administrators alike. Also, multiple programmes can use a joint social registry, which is then called an **integrated social registry**.[21]

Furthermore, platforms for grievances and appeals, payments, and beneficiary management might be part of social protection programmes. Moreover, organisations might establish links to broader information systems and registries

[17] Lindert et al. 2020 (p. 11).

[18] The World Bank is moving towards calling these 'Beneficiary Operations Management Systems' (BOMS) (Barca and Chirchir, 2019, p. 12).

[19] Sepúlveda Carmona 2018 (p. 30).

[20] Barca and Chirchir 2019 (p.12).

[21] Leite et al. 2017 (p. iv-v)

such as national ID systems, civil registry systems or humanitarian and Disaster Risk Management systems. The latter collects data that might be useful for social protection programmes, for instance, beneficiary databases and vulnerability assessments. Interoperability between systems and efficient information flows are crucial for social protection programmes to be successful.

To enable the realisation of social protection programmes, a lot of **personal and sensitive data** of applicants, registrants, recipients or beneficiaries (name, age, gender, address, income, health status, biometrics such as fingerprints, and much more) is processed (collected,[22] stored, transferred, and shared). Data collection and processing of personal data happens at every step of programmes' implementation, throughout the delivery chain and the different platforms for information management.

Therefore, social protection authorities and managers, development partners and practitioners in general that process personal data, in their capacity as either data controllers or processors, should adhere to data protection and privacy principles and standards and be able to comply with specific national and international rules that protect privacy and govern how personal information is processed.[23]

Box 4 - International organisations, non-governmental organisations and applicable law

Development and humanitarian agencies can be international inter-governmental organisations (hereinafter referred to as **international organisations**) or international or national non-governmental organisations (NGOs). [24]

NGOs are subject to the country's jurisdiction where they operate and need to comply with the applicable laws. However, what rules apply to them depends on the respective laws and factual circumstances and is not dealt with by this Implementation Guide. Instead, this Implementation Guide describes good practices regarding personal data protection and privacy and suggests its application by NGOs without prejudice to national laws.

International organisations work in different ways:

[22] In social protection systems, information can be collected verbally (e.g., via interviews) or in writing (e.g., via filling out forms). In addition, it can be stored physically (e.g., paper files) or electronically (e.g., computers or external hard drives, cloud storage, USB device, computer networks).

[23] Barca and Chirchir 2019 (p.13).

[24] See 'Glossary of defined terms and abbreviations.'

- They implement **humanitarian aid** projects independent from host governments, target persons as they deem fit, and provide cash transfers received from donors (as sole controllers). The legal basis for the performance of these organisations is a basic agreement with the host government allowing them. International organisations enjoy privileges and immunities to ensure they have complete independence to perform the mandate attributed to them under international law. To that extent, they are not subject to the jurisdiction of the countries in which they work. "They can therefore process personal data according to their own rules, subject to the international monitoring and enforcement of their own compliance systems; in this regard, they constitute their own 'jurisdiction'."[25] This has specific implications for framing data protection and privacy principles and standards. This Implementation Guide will not deal with these specific implications. However, the personal data protection and privacy standards described here can be applied by international organisations without prejudice to their mandate under international law.
- However, international organisations also work closely with governments and **implement social protection systems** on their behalf or together (as processors or joint controllers). This type of performance would not be characterised as humanitarian aid but rather as technical assistance or development support. In this case, international organisations need to take requirements under national laws (as instructed by the controller or joint controller) because they are helping to implement national social protection programmes, subject to national laws under which the individuals may have specific rights. International organisations can apply the personal data protection and privacy standards described in this Implementation Guide in this case.[26]

2.2. Why is data protection needed in social protection?

Social protection programmes process personal data collected from individuals, families, and households to deliver its services and benefits regularly. And why is it so essential to protect this data?

[25] Kuner and Marelli 2017 (p. 34).

[26] See Section 3.5 - International data sharing and Box No. 30 - Legal basis and joint programmes of international organisations and social protection authorities.

Respecting data protection and privacy laws and frameworks is extremely important, and the benefits of doing so go beyond mere legal compliance and avoiding penalties. Ensuring personal data protection and privacy is a fundamental step for social protection programmes to reach their goals, such as quality of services, respect of human rights, and protection of minorities and vulnerable populations. Therefore, the protection of the personal data of the applicants, registrants, recipients or beneficiaries of social protection services improves the results of these programmes.

Moreover, many social protection programmes use MIS to automate business processes and manage data. In addition, new and emerging technologies are used, such as biometrics. These information management systems and digital technologies may increase the risks to data protection and privacy.[27] Therefore, social protection programmes need to establish strict security protocols, compliance with data protection and privacy rules, and data-sharing principles to protect data subjects' rights.[28]

The lack of consideration of data protection and privacy rights in the design and management of these programmes—for instance, the 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, or give rise to exclusion errors, undermining programme objectives.

Lastly, there is an even more serious concern in social protection systems than, for instance, in the private sector because these systems are set up to protect, principally, the most vulnerable population. This population relies on social protection schemes and programmes and does not have any alternative. Moreover, vulnerable people are less able to protect their rights and claim their entitlements compared to wealthier parts of the population. Therefore, protecting their data rights is vital to ensure a social protection rights-based approach and respect to individuals' fundamental and human rights.

---

[27] See Section 2.4. - Digital technologies increase the urgency of data protection.

[28] Sepúlveda Carmona 2018 (p. 30).

2.3. Main stakeholders and responsibilities

In the particular context of social protection practitioners involved in the design, implementation and expansion of social protection systems and programmes at the country level, when discussing data protection and privacy, the main stakeholder groups and their roles and responsibilities usually are:

- **Governments**: Includes national and local government's ministries, departments, secretaries and other public bodies. Their responsibility is to provide the conditions and resources for the development of a data protection and privacy regime, and the appropriate structure to enforce data protection legislation.
- **Policy and lawmakers:** They are the government and lawmakers at the country level. They are responsible for the design of the data protection and privacy laws, that can be either sectorial or comprehensive. They establish legislation that defines the obligations and rights of different stakeholders and sanctions to violations.
- **Data Protection Authorities (DPAs):** An independent public authority which has been appointed by the government to supervise compliance with data protection and privacy legislation continually. These authorities are generally responsible for providing guidance on national data protection legislation, enforcing data protection laws by investigating alleged privacy violations and imposing sanctions when the law is breached.
- **Data subjects:** They can be the social protection programme's applicants, registrants, recipients, beneficiaries or any other citizen whose personal data is being processed. Their responsibility is to become active stakeholders, taking control over their own personal data and privacy, by understanding the risks involved and exercising the rights related to personal data and privacy.
- **Data controllers and processors:** Any of the stakeholders that control and/or process personal data (e.g., social protection schemes and programmes, private sector companies, development agencies, governments, and ICT providers). They are responsible for safeguarding personal data and respecting the rights of data subjects, demonstrating compliance with data protection and privacy principles and legislation.
- **Development and humanitarian agencies and other development partners**: Any organisation dedicated to distributing aid and promoting

economic growth and development in the areas they serve. Externally, their role is to advise and support local governments to develop and/or improve their data protection and privacy framework and enforcement mechanisms. Internally, they are responsible for demonstrating compliance with the data protection and privacy principles and internal guidelines, as well as with the legislation to which they are subject.

- **Civil society:** Civil society organisations, activists, academics, employers' and workers' organisations or consumer protection organisations lobby governments, lawmakers or other stakeholders to ensure that data subjects have rights over their personal data, supervise that these rights are respected, report violations and raise public awareness about data protection and privacy.

2.4. Digital technologies increase the urgency of data protection

Digital technologies hold great potential for the developing world. For instance, they are enabling a major shift in how social protection systems are designed and implemented and benefits and services delivered in different aspects of the social protection delivery chain.[29] For example, they are used to develop ID systems, digital payments, MIS, social protection information systems (SPISs)—a critical milestone in developing a national social protection system—,[30] among other things.

While digital technologies may simplify and accelerate processes, reduce some costs, increase efficiency and effectiveness, and improve transparency and inclusiveness, they also bring inherent challenges and risks. These include high technological costs, complexity (requiring a different skillset from administrative staff, for instance), 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 protection.

The inherent risks and possible adverse side effects of digital technologies are enhanced by the lack of appropriate infrastructure and legacy systems in developing countries but long present in the developed ones. Any digital

[29] Lindert et al. 2020 (p. 422).

[30] Barca and Chirchir 2019 (p.11-15).

technology should only be adopted if it complies with personal data protection and privacy regulations in place, which should explicitly state the rights of the data subjects.

Therefore, the combination of the processing of personal data and the adoption of digital technologies, apart from bringing many advantages to these systems, may impose considerable challenges to personal data protection and privacy if not accompanied by a careful risk assessment and the implementation of the appropriate safeguards.

2.5. There is no contradiction between the right to (data) privacy and the right to social protection

According to the Vienna Declaration—a statement to reinforce the Universal Declaration of Human Rights—"all human rights are universal, indivisible and interdependent and interrelated."[31] This is the case with privacy and social protection, both human rights. It is not possible to enjoy the protection of one without the other. Privacy and social protection are both a precondition for a democratic society.[32]

There is no contradiction between protecting personal data and privacy and providing effective social protection programmes and benefits.

However, sometimes, the most vulnerable members of society are faced with a trade-off: invasions of (data) privacy in exchange of access to social protection benefits.[33] For instance, when applying for social assistance benefits, access is often conditional upon increased surveillance, control and data exploitation. Moreover, in some cases, individuals are required to provide biometric data (e.g., fingerprinting and retina scanning)—without the appropriate safeguards—as a condition for access.

It is important to remember that individuals and families do not waive their rights to data protection and privacy when they provide their personal information to

[31] United Nations 1993 (Art. 5).
[32] Privacy International 2019.
[33] Privacy International 2019.

become applicants, registrants, recipients or beneficiaries of social protection programmes.[34]

Box 5 - Why should social protection practitioners care about data protection and privacy?

- Social protection systems process (collect, use, store, disclosure) personal data of applicants and beneficiaries of their programmes. This data needs protection.
- Why? If personal data is not adequately protected, the right to privacy may be violated, and individuals may suffer material, physical or symbolic harm.
- Digital technologies (automated decision-making, digital payments, biometrics) can bring benefits and facilities to social protection systems. Still, they also come with some inherent risks for the protection of personal data and privacy that need special attention and actions to avoid harm to beneficiaries of social protection programmes.
- Personal data protection is a fundamental step to achieve social protection systems goals such as quality of services, respect of human rights, and protection of minorities and vulnerable populations.
- Data protection is essential to create trust among social protection authorities, practitioners and applicants and beneficiaries. The lack of trust may restrain vulnerable populations' access to social protection services and benefits, fearing that sharing their personal information will lead to harm, discrimination, stigmatisation, surveillance, among other risks.
- Compliance with organisational and legal data protection and privacy frameworks is important to avoid penalties for social protection practitioners.
- Social protection and privacy are both human rights and, therefore, interdependent, indivisible, and interrelated.[35] This means that one needs the other to be fulfilled. Both are equally important.
- No effective social protection system is possible without personal data protection and privacy.
- Data protection, privacy and social protection are all a precondition for a democratic society.

[34] Sepúlveda Carmona 2018 (p. 12).

[35] United Nations 1993 (Art. 5).

3. Good international practice of data protection and privacy

3.1. Data protection and privacy standards

Several international and regional data protection instruments share a set of core data protection and privacy standards.[36] While they can have different names,[37] and can deviate in scope and content, personal data protection and privacy frameworks typically consist of the following groups of standards.

a) **Basic principles governing the processing of personal data** (hereafter '*data protection and privacy principles*')
   (1) Purpose specification
   (2) Data minimisation
   (3) Lawfulness, fairness and transparency
   (4) Accuracy
   (5) Retention limitation
   (6) Security
   (7) Accountability

b) **Data subject rights**
   (1) Right to information about the personal data processing
   (2) Right to access the personal data that is processed
   (3) Right to data rectification
   (4) Right to data erasure

[36] To the knowledge of the authors, no detailed study of the minimum common data protection and privacy elements in international and regional data protection and privacy treaties and frameworks, as well as regional and national laws, exists which could serve as a reliable basis for defining good international practice of personal data protection and privacy. This Implementation Guide does not claim to define good international practice of personal data protection and privacy. The principles and elements presented in this guide are based on the review of the frameworks set out in Box 3. Their interpretation draws mostly from the definitions contained in the OECD Guidelines, the GDPR and the CoE Convention 108+, as deemed appropriate in the opinion of the authors, given detailed guiding notes, recitals and opinions.

[37] The terms used in this Implementation Guide are a mix drawn from the relevant data protection and privacy frameworks, as deemed most comprehensive. For a more detailed overview, see Annex 1.

(5) Right to object to processing or to withdraw consent
(6) Rights relating to automated decision making
(7) Right to complaint to an independent body
(8) Right to an effective remedy (administrative or judicial redress)

c) **Accountability, oversight and enforcement**
(1) Legal responsibilities with respect to (a) and (b) *(accountability)*
(2) Independent authority monitoring compliance with (a) and (b) *(oversight)*
(3) Legal redress for data subjects *(enforceability)*

d) **Transborder data flow/international data sharing**

e) **Sensitive personal data**

These data protection and privacy standards need to be considered when data is qualified as personal data, when there is only a remote possibility of identifying an individual in an otherwise anonymised data set, and when data of groups are considered sensitive.

3.2. Data processing principles

Good international practices indicate that the core principles restricting the processing of personal data include the following. These need to be applied to all phases of data processing and regularly reassessed.

Figure 2. Data processing phases[38]

[38] Original figure for this publication.

3.2.1. Purpose specification

Personal data should be processed only for one or more specified, explicit and legitimate purpose(s), stated to the data subjects at the point of collection.

Why is it important? This principle recognises that personal data belongs to the individual's private sphere. Like any other personal item, such as mail or personal belongings, personal data can only be accessed by third parties for specific purposes. Given that the purposes for which data is used are too manifold, they cannot be specified by the law itself. However, specifying and informing the data subject about the purposes for processing personal data is a way to self-impose on the data controller an obligation that certain data collected for one purpose will not be used for a different purpose.

The legitimate purpose needs to be determined for each data processing activity. For example, the purpose of a data collection could be the creation of a list of beneficiaries to receive cash transfers. Another situation could be calling beneficiaries (using their data) and interviewing them with the purpose of monitoring a social protection programme.

Some data protection and privacy frameworks allow for the further processing of personal data for other purposes than those stated to data subjects at the time of data collection, if such other purposes are compatible with the initial purpose

specified at the time of data collection.[39] As a guideline, the purpose will not be compatible if data subjects might consider the further processing unexpected, inappropriate, or otherwise objectionable.[40]

The purpose of data processing goes hand in hand with the lawfulness. If the purpose of the further processing is not compatible with the initial purpose communicated to the data subjects at the time of data collection, then such data processing should only be permitted, if (i) also the new purpose is specified, explicit and legitimate and (ii) the controller has a new legal basis, such as consent or a legal obligation.[41] The law might state exceptions to this rule. For example, the GDPR and CoE Convention 108+ provide that processing for other purposes such as archiving in the public interest, scientific, historical or statistical purposes, subject to safeguards such as pseudonymisation and even anonymisation in the case of statistical purposes, shall not be considered incompatible with the initial purpose (even though, de facto, it is a different purpose).[42] Data, thus, can be processed for that further purpose without a new legal basis (such as the beneficiary's consent).

3.2.2. Data minimisation

Personal data should be adequate, relevant and limited (i.e., minimal) to what is necessary in relation to the purposes for which it is being processed.

Why is it important? The intrusion into the individual's privacy sphere through data processing needs to be minimal, in terms of the number of data variables processed, the sensitivity of the data, and the extent of the processing.

The data minimisation relates to the purpose specification principle. Personal data is adequate if it is of sufficient quality and quantity to meet the specified purposes. It is relevant if it is closely connected to the specified purpose.

The data minimisation principle is satisfied if the purpose cannot be reached with less or no personal data, or less sensitive personal data. This relates not only to the data collection but also to the further data processing. Thus, data needs to be

[39] GDPR 2016/679, Art. 5 (1) and CoE Convention 108+ 2018, Art. 5 (48).
[40] CoE Convention 108+ 2018, Explanatory Report (Sec. 49).
[41] See Section 3.2.3 - Lawfulness, fairness and transparency.
[42] GDPR 2016/679, Art 5. (1) and CoE Convention 108+ 2018, Art. 5 (50).

deleted if the specified purpose has been achieved or it is not necessary anymore because the purpose has changed.[43]

Thus, limiting the collection of personal data is essential, especially regarding sensitive personal data.

3.2.3. Lawfulness, fairness and transparency

Personal data should be processed in a lawful, fair and transparent manner.

Why is it important? The interference with the individual's constitutionally guaranteed right to privacy needs to be permitted by law in order to allow for legitimate, appropriate and proportionate interferences.

Processing personal data in a **lawful** way means that the controller has a legal basis (or legal grounds) for processing this kind of information for a legitimate, specific and explicit purpose and that it will be done in a way that respects the rule of law. The law may provide for several legal bases for processing personal data.

Data controllers need to identify one of the legal bases for each data processing activity in the data protection and privacy framework that they are subject to. Different types of controllers, such as governments, humanitarian organisations and companies, will typically rely on different legal bases for varied activities. For example, governments will be authorised to process personal data for official activities on public interest and/or a legal obligation. Still, for the personal data of their staff, the processing will be based on a contract with the individual. Companies providing services to individuals, such as mobile phone providers or banks, will process the contractual data based on the contract with the individual. Any additional data will be based on the individuals' consent and, in specific cases, on legitimate interests. International organisations are not subject to national laws but to their own rules. They will process data based on the legal basis identified by their rules. These may be specific to the activities they typically implement.

What legal basis is suggested to be used in the area of social protection will be discussed in further in this Implementation Guide.[44]

---

[43] See Section 3.2.5 - Retention limitation.

[44] See Section 4.3 - How to apply the data protection and privacy standards to social protection programmes.

Box 6 - Legal bases for processing personal data

According to the international and regional data protection and privacy frameworks, the legal bases for processing personal data may include the following.[45] The processing shall be lawful only if and to the extent that at least one of them applies:

1) Public interest: Public interest is the appropriate legal basis when the processing of personal data is necessary to exercise official authority or a task in the public interest and the task has a basis in law. Public interest grounds could be the administration of justice, public health and social security, the prevention, investigation, detection and prosecution of criminal offences, and the execution of criminal penalties, the enforcement of civil law claims, among others. For international organisations, the legal basis of public interest applies when the activity in question is part of a humanitarian mandate established under national or international law or is otherwise an activity in the public interest laid down by law.[46]

2) Vital interests: The processing is necessary to protect the vital interests of a data subject or another person (i.e., protect someone's life, integrity, health, dignity, or security). In the case of vital interest, it is necessary that this legal basis is accompanied by sufficient elements to consider that, in the absence of the personal data processing, the individual could be at risk of physical or moral harm.

3) Legal obligation: The processing is necessary for compliance with a legal obligation to which the controller is subject (not including contractual obligations). It is not necessary that this legal basis expressly permits specific data processing activities, such as data collection. For example, a social protection law may oblige a specific domestic authority to provide assistance to applicants which provide evidence of being under a poverty level. In this case, the authority is required to collect the data to assess those conditions and to ensure delivery of the benefits to the targeted persons, to comply with its legal obligation.

4) Informed consent: Consent indicates the data subjects' agreement to the processing of personal data relating to them for a specific purpose. Where the processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data. If the data subject does not provide consent, the data cannot be processed on this legal basis. Consent won't always be the most appropriate legal basis.

[45] See, for instance, GDPR 2016/679 (Art. 6, 7, 8, 9), CoE Convention 108+ 2018 (Art. 5, 17), for a legal basis of consent and personal data processing. Other bases are provided by ECOWAS 2010 or the OECD Privacy Framework 2013.

[46] Kuner and Marelli 2017 (p. 67).

5) Contract with the data subject: The processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract with the data subject.

6) Legitimate interest: Data controllers can process personal data without consent or another legal basis, if they need to do so for a genuine and legitimate reason, unless the individual's rights and interests override this. Legitimate interest is the most flexible lawful basis for processing and, as such, is open to abuse. When relying on legitimate interests, data controllers should take on extra responsibility for considering and protecting people's rights and interests. The processing must be necessary to achieve the stated purpose. If the same result can be reasonably accomplished in another less intrusive way, legitimate interests will not apply. Examples of potential legitimate interests are IT security and fraud prevention.

Transparency means that personal data is not used in ways that data subjects would not expect, were not informed of and are not otherwise aware of. In addition, data subjects need to be informed on what legal basis their data is being processed.

Fairness is related to the manner by which the information is obtained. It implies that nobody is coerced into giving personal information or has no choice to giving their personal data due to their situation (e.g., in desperate need of aid). Also, no unfair practices shall be used, such as the use of hidden data registration devices (e.g., voice recorders) or deceiving data subjects into supplying information.

3.2.4. Accuracy

Personal data that is processed should be accurate, complete and, where necessary, up to date. The opposite would be inaccurate (incorrect or misleading), incomplete or outdated personal data.

Why is it important? Personal data is used to contact individuals and verify their identity, for example, to allow them to exercise rights or obtain benefits. If the data is not accurate, such purposes of data processing may not be achievable. In addition, inaccurate data may cause poor decision-making and be detrimental to an individual, such as excluding a person from a social protection programme based on wrong socio-economic data.

Mechanisms should be put in place to ensure that the data is systematically and regularly reviewed and updated, corrected or deleted.

3.2.5. Retention limitation

The retention limitation principle means that personal data should only be retained, in a form which permits identification of data subjects, for the period of time that is necessary for the purposes for which it was processed. The right to privacy requires that no personal data will be kept by data controllers if the use purposes have been fulfilled or are no longer pursued.

Why is it important? To comply with the purpose specification, data minimisation, and accuracy principle. Ensuring the erasure or anonymisation of personal data when it is no longer needed reduces the risk that it will be used for different purposes than the original, or that it becomes irrelevant, excessive, inaccurate or out of date.

Holding personal data for longer than necessary may lead to unnecessary costs associated with storage and security. Control over data may be lost when data are no longer of interest, and the storage of such data increases security risks (e.g., theft or unauthorised copying). Finally, erasure of unused data helps to reduce the burden of the data controller to respond to data subject access requests for any personal data held by it.

Under some frameworks, personal data may be stored for longer periods if it will be processed for some specific purposes such as for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[47] In these cases, appropriate technical and organisational measures should be put in place to safeguard the rights and freedoms of the data subjects, such as protection against unauthorised access, abuse or disclosure.

3.2.6. Security

Personal data–during storage, transmission and use–as well as the infrastructure relied upon for processing, have to be secure. Systems need to be available. Therefore, appropriate **physical, technological and organisational measures** must be taken to ensure the security of data and systems and to protect personal

[47] GDPR 2016/679 (Art. 5) and OECD Privacy Framework 2013 (p. 14).

data from unauthorised or unlawful processing, and against accidental or deliberate loss, destruction, modification, disclosure, or unauthorised access.

Why is it important? Inadequate or insufficient information security puts systems and programmes at risk and might create harm and distress to people. In extreme cases, lives may be at risk. Security incidents may also cause reputational issues for data controllers and processors. Finally, information security is essential to develop a trusty relationship with data subjects.

Harm generated by the loss or abuse of personal data includes, for instance:

- persecution
- identity fraud
- witnesses put at risk of physical harm or intimidation
- credit card fraud
- exposure to embarrassment or inconvenience
- fake applications for services or benefits

These risks may be grouped into three categories as following:

- Confidentiality: only authorised people or parties (acting within the scope of authority given to them) can access, disclose, alter or delete the data – Risk: illegitimate access to data, unauthorised use or modifications.
- Integrity: tracking of who is modifying data – Risk: changes of the data are not tracked, cannot be validated/verified.
- Availability: access to and availability of personal data is restored in a timely manner in case of any incident – Risk: accidental loss or destruction.

In order to maintain security, the data controller needs to assess the specific risks inherent in the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security and will vary depending, among other things:

- type of operation
- level of assessed dated protection risks
- nature and sensitivity of the personal data to be protected
- format (paper or electronic) or form of storage (paper file cardboard, server, cloud)

- use of data (hardware such as servers, laptops, hard drives, cell phones; software such as operating system, MIS)
- transfer of data (e-mail/internet, API)
- environment/location of the specific personal data
- prevailing security and logistical conditions[48]

Box 7 - Security measures

Personal data security measures should relate to physical security of the premises where the personal data is stored, technological and organisational security, and may include the following:[49]

1) Physical security measures

- the quality of doors and locks, and the protection of premises by such means as alarms, security lighting or closed-circuit television
- access control to premises and how visitors are supervised
- disposal of any paper and electronic waste
- how to keep IT equipment (computers, laptops, mobile devices) secure
- hot to keep paper files secure (lock on cupboards)

2) Technological security measures

- system security: the security of network and information systems, particularly those which process personal data
- data security: the security of the data held within systems, e.g., ensuring appropriate access controls are in place, and that data is stored securely
- online security: e.g., the security of the website, online services or applications
- device security: e.g., tablets used for data collection

3) Organisational security measures

- issue an information security policy to cover the above and to establish procedures for staff to follow
- identify a person/team with day-to-day responsibility for personal data in the information security division within the organisation
- make sure this person/team have the appropriate resources and authority to do their job effectively
- build a culture of security awareness within the organisation, particularly relating to personal data
- training staff on information security, with an emphasis on personal data

[48] Kuner and Marelli 2017 (p. 44).

[49] ICOb n.d.

- checking whether security measures are actually being adhered to
- establishing standard procedures to deal with security incidents, and
- regular testing and review of the adequacy of the above security measures (do they remain appropriate and up to date?) and update, if necessary

In the IT context, technological security measures might be referred to as 'cybersecurity'. However, cybersecurity relates to the protection of networks and information systems from attack. Thus, information security (e.g., security of personal data) is broader than cybersecurity, as it also covers physical and organisational security measures.

3.2.7. Accountability

Those that process personal data should be accountable for demonstrating compliance with the data protection and privacy principles, their obligations, and facilitating the exercise of the data subject rights.[50]

3.3. Data subject rights

The rights of the data subjects or individual rights are the second key pillar of the international and regional data protection and privacy frameworks.[51] They recognise that data subjects should be fully informed about and, thus, enabled to better control the processing of their personal information.

Good international practices indicate that the rights of data subjects in a data protection and privacy framework should include:

- Right to information
- Right to access
- Right to rectification

[50] Why this principle is important, and some implementation aspects will be discussed in detail in Section 3.4.1 - Accountability: Legal obligations of data controllers and processors.

[51] In a number of international and regional data protection and privacy instruments–such as the OECD, UN (1990) and APEC–the rights of the data subjects are integrated into different principles. In other instruments such as the Malabo Convention, ECOWAS and the GDPR, the rights of the data subject are presented in a specific section, separated from the data protection and privacy principles. Regardless of how the rights of the data subjects are presented in different international and regional frameworks, all of them recognise such rights. For a more detailed overview, see Annex 1.

- Right to erasure
- Right to withhold consent or the right to object
- Rights relating to automated decision making and profiling
- Right to complain to an independent body (administrative remedy)
- Right to a judicial remedy, including financial compensation

Data subject rights are not absolute but may have to be reconciled with other rights and legitimate interests. Limitations need to be provided for by law and must constitute a necessary and proportionate measure.[52]

3.3.1. Right to information

The controller should, at the time when personal data are obtained from data subjects themselves or within a reasonable time if obtained from third parties, fairly and transparently inform the data subjects in detail on how their personal data will be processed.

Box 8 - Checklist of Good Practices: What information should be provided to data subjects?

Good international practices recommend that individuals be provided with the following information:[53]

- ☐ the identity and the contact details of the controller
- ☐ the purposes of the processing
- ☐ the legal basis for the processing
- ☐ the categories of data involved
- ☐ with which entities the personal data is shared and for what purposes
- ☐ whether the controller intends to transfer personal data to a third country or international organisation and the appropriate safeguards provided
- ☐ the period for which the personal data will be stored
- ☐ the rights that the data subjects have over their data against the controller and processor, and how they can exercise them

[52] CoE Convention 108+ 2018 (Art. 9).
[53] See GDPR 2016/679 (Art. 13, 14), OECD Privacy Framework 2013 (p. 15), CoE Convention 108+ 2018 (Art. 8), Malabo Convention 2014 (Art. 16), and APEC 2005 (Art. 21-23).

- ☐ the rights data subjects have, if any, if the controller or processor fail to comply (remedies), namely, the right to submit a complaint to an independent body (administrative remedy) and/or right to a judicial remedy
- ☐ the existence of automated decision-making, including profiling, and meaningful information about the logic involved, the significance and the envisaged consequence of such processing for the data subject
- ☐ the source of the personal data (if not obtained from the data subject)
- ☐ whether providing the data is mandatory or voluntary, and the possible consequences of failure to provide such data

3.3.2. Right to access

The data subject should have the right to obtain from the data controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case, at reasonable intervals and without excessive delay or expense, access to the personal data and detailed information about the processing of such data, including the purpose of processing.

Being able to access their personal data enables individuals to examine if it is being processed with a lawful basis, in accordance with the information provided to them at data collection, and whether it is accurate. This knowledge enables them to decide whether they want to take further action, such as exercising their right to rectify, erase or, as applicable, withdraw their consent (if the legal basis was consent) or object to the processing. It also allows them to report alleged violations of their rights and might prevent data controllers from this kind of practices.

Box 9 - Checklist of Good Practices: Exercising the right to access

Good international practice recommends that data subjects should be able to easily request and be given information about the processing of their personal data from the controller. [54] Access should be:

- ☐ freely given or, if any charge, it should be not excessive (e.g., a reasonable fee based on administrative costs)
- ☐ within a reasonable and stated time

[54] See GDPR 2016/679 (Art. 15), OECD Privacy Framework 2013 (p. 15), CoE Convention 108+ 2018 (Art. 9), Malabo Convention 2014 (Art. 17) and APEC 2005 (Art. 29-30).

- ☐ in a form that is readily intelligible to data subjects and does not require any particular expertise or knowledge to comprehend the information

If the request to access is denied, the data subject should be given reasons why, and to be able to challenge such denial.

3.3.3. Right to rectification

Data subjects should have the right to request and obtain from the data controller, without undue delay, the rectification (to correct, update, or modify) of personal data regarding them to ensure the data is accurate, complete and up-to-date.

Depending on the content of the requests and without placing an unreasonable burden of proof on them, data controllers may need to require data subjects to provide proof of the alleged inaccuracy and assess the credibility of the assertion.[55]

When the accuracy of an individual's personal data is contested, and while exercising the right to rectify personal information, such data should not be used to make decisions about the data subject.

3.3.4. Right to erasure

Certain data protection frameworks such as from Nigeria, South Africa, the GDPR and the CoE Convention No. 108+, include the right to erasure. It allows 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.

Box 10 - Checklist of Good Practices: When to exercise the right to erasure?

Good international practices recommend that data subjects should have the right to have their personal data erased from the controller's database where:[56]

- ☐ the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed

[55] Kuner and Marelli 2017 (p. 55).

[56] See GDPR 2016/679 (Art. 17), CoE Convention 108+ 2018 (Art. 9), Malabo Convention (Art. 19), APEC 2005 (Art. 29-30).

- ☐ the data subject has withdrawn consent, and there is no other legal ground for the processing
- ☐ in case the data has been obtained based on a public task or legitimate interests, the data subject objects to the processing, and there are no compelling legitimate overriding the rights and freedoms of the data subject
- ☐ the processing does not comply with the applicable data protection and privacy framework, and/or
- ☐ the personal data have to be erased for compliance with a legal obligation to which the controller is subject.

However, the GDPR (the so-called 'right to be forgotten') and the CoE Convention 108+ recognise limitations of this right. It shall not apply if processing is necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest to which the controller is subject, or in the exercise of official authority vested in the controller. In this case, it is assumed that the controller needs to keep the data to comply with its legal obligations or public tasks. In the case of public interest, the controller may however have to stop the processing (but may keep the data).[57]

Any erasure requests should be brought to the attention of any processors who are processing the data on behalf of the controller and joint controllers unless that results impossible or involves unreasonable effort.[58]

One major challenge is how to reconcile the right to erase personal data 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. Therefore, it is essential that such a right clearly provides safeguards to ensure that it is not open to abuse.

3.3.5. Right to withdraw consent and to object to data processing

[57] CoE Convention 108+ 2018 (Explanatory Report, Sec. 73), GDPR 2016/679 (Art. 17).
[58] GDPR 2016/679 (Art. 19).

If the controller chooses consent as legal basis for processing, it needs to inform data subjects about their right to *withhold or withdraw* their consent at any time,[59] but also about the implications of withholding the consent.[60]

If personal data is being processed based on a legal obligation of the controller or based on grounds of public interest or in its official authority, data subjects have a right to *object* to the processing, at any time, unless the controller has a legitimate ground for data processing which overrides the interests or rights and freedoms of the data subject, such as taxes or public health.[61] The controller needs to provide evidence of these overriding legitimate grounds to the individuals. If it does not have those grounds, it needs to stop the processing and needs to delete the data (public interest) or may keep the data (legal obligation).

The right to object might be absolute in some cases, for instance, where personal data are processed for direct marketing purposes.

3.3.6. Rights related to automated decision making and profiling

Some international and regional data protection and privacy frameworks—e.g., CoE Convention 108+ and the GDPR—establish data subject rights relating to automated decision making.[62] According to these frameworks, data subjects should have the right not to be subject to a decision based purely on automated processing of personal data (without human intervention), if such decisions produce legal effects (refusal of a legal right or effect on legal status) or similarly significantly affect the data subjects. In exceptional cases where this processing technique is used, an individual should have the right to obtain human intervention (in a simple way), to express his or her point of view, and to challenge a decision.

The GDPR extends this right to include automated decision making based on 'profiling' (see Box No.11 below for detailed explanation).

---

[59] CoE Convention 108+ 2018 (Explanatory Report, Sec. 45), GDPR 2016/679 (Art. 7).

[60] See more information about the implication of withholding data or withdrawing consent in Section 3.3.5 - Right to withdraw consent and to object to data processing.

[61] CoE Convention 108+ 2018 (Art. 9; Explanatory Report, Sec. 78), GDPR 2016/679 (Art. 21).

[62] CoE Convention 108+ 2018 (Art. 9), GDPR 2016/679 (Art. 22).

This 'right' works slightly different than the other data subject rights, as controllers and processors do not have to act only upon a request of a data subject. Instead, this prohibition applies independently of whether the data subject takes action regarding the processing of their personal data.[63]

Box 11 - What is automated decision-making and profiling?

Automated decision-making means the process of making decisions by technological and automated means without any human involvement. For instance, a decision of an algorithm integrated into a software to reject an online credit application based on certain information provided by the data subject or additional data obtained from other resources.

A process may still be considered solely automated if a human inputs the data to be processed, and then the decision-making is carried out by an automated system.

Automated decision-making can be based on so-called 'profiles' of individuals created through profiling. But it can also be based on data provided by the data subjects or other sources.

Profiling means any form of automated processing of personal data consisting of the use of such data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[64]

Profiles are created based on personal data of the data subject, obtained directly or indirectly. It is important to take into consideration that personal data can be revealed from other data: it can be derived, inferred and predicted. The information is analysed to classify people into different groups or sectors, using artificial intelligence, including machine-learning,[65] in order to evaluate (score, rank, assess) and predict certain things about an individual (behaviours, interests, performances) based on the information contained in the profile.

Profiling may happen in a variety of contexts and for different purposes: from targeted advertising and healthcare screenings to predictive policing. For example, calculating a score—through profiling—that predicts the likelihood of an individual

[63] Article 29 Working Party 2018 (p. 19).

[64] GDPR 2016/679 (Art. 4).

[65] For more information about artificial intelligence, including machine learning, see 'Glossary of defined terms and abbreviations'.

committing a future crime based on the individual's belonging to such a profiled group.[66]

These profiles can be used to inform decisions about individuals that may or may not be automated. To the extent they inform automated decisions, the respective data subject rights need to be respected.

The rationale behind this right "is driven by a concern for algorithmic bias; a worry of incorrect or unsubstantiated solely automated decisions based on inaccurate or incomplete data; and the need for individuals to have redress and the ability to context a decision if an algorithm is incorrect or unfair".[67]

As a consequence, the GDPR and the CoE Convention 108+ require that any individual who may be subject to a purely automated decision has the right to challenge such a decision by substantiating the possible inaccuracy of the personal data in question before the decision is made, the irrelevance of a profile to be applied to his or her particular situation, or where individuals are stigmatised by application of algorithmic reasoning resulting in limitation of a right or refusal of a social benefit or where they see their credit capacity evaluated by a software only.[68]

Automated decision making, including profiling, may only be permitted, if it is authorised by a law which lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.[69]

Box 12 - Checklist of Good Practices: Rights related to automated decision making and profiling

Good international practice advises that:[70]

- ☐ Both automated individual decision-making and profiling are covered in a data protection framework. However, they don't need to be dealt with together, since they are two different processing techniques that can be or not used together.
- ☐ Individuals have the right to not be subject to purely automated decision making (involving or not profiling), with legal or similarly significant effects to their lives (e.g., an automated decision regarding a refusal of a social protection benefit).

[66] Privacy International 2018 (p. 57).

[67] Kuner and Marelli 2017 (p. 453).

[68] CoE Convention 108+ 2018 (Explanatory Report, Sec. 75).

[69] CoE Convention 108+ 2018 (Explanatory Report, Sec. 75) and GDPR 2016/679 (Art. 22).

[70] GDPR 2016/679 (Art. 22).

☐ If, in exceptional cases (regulated by law), the data controller is carrying out solely automated decision-making that has legal or similarly significant effects on data subjects, additional measures to protect individuals should apply. These should include, at least:

• the right to request, in a simple way, and obtain human intervention on the part of the controller

• to express his or her point of view

• to obtain an explanation of the decision reached after such assessment ('right to explanation')

• to challenge the decision

3.3.7. Right to complain to an independent body (administrative remedy)

Data subjects should be entitled to lodge an inquiry or complaint relating to the alleged violation of their rights with a body that is independent from the controller, in order to obtain an independent review of the data processing activity in question.[71]

In states with comprehensive data protection and privacy laws, this independent body would be a data protection authority (DPA) established by law that is tasked with monitoring the data protection and privacy law enforcement. Here, the importance of supervisory authorities having the power to receive complaints, investigate them and impose effective sanctions (or refer the case to a court, if the framework in question includes this alternative) is highlighted.

In countries that do not have data protection and privacy laws, or such laws do not provide for establishing an independent DPA, data subjects should nevertheless enjoy this right, to the extent possible. In this case, controllers, such as public authorities or companies, may establish internal offices responsible for the handling of data subject requests, such as a data protection office (DPO).[72] Some frameworks foresee the necessity of providing appropriate administrative remedies in situations where privacy protections are violated.[73] After submitting a complaint to a

[71] CoE Convention 108+ 2018 (Art. 77).

[72] See Section 4.3.3 - How to be an accountable social protection controller.

[73] APEC 2005 (Art. 20, 53), CoE Convention 108+ 2018 (Art. 9, 12), GDPR 2016/679 (Art. 78, 79).

supervisory authority or internal offices (such as DPA or DPO), the authority/office should inform the individuals on the progress and the outcome of the complaint, including the possibility of a judicial remedy, if existent.

3.3.8. Right to an effective judicial remedy

Individuals should have the right to an effective judicial remedy against data controllers or processors, 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.

After the internal administrative processes have been exhausted, some frameworks envision the right to appeal to the regular judicial system. CoE Convention 108+ obliges states to grant data subjects appropriate judicial remedies for violations of the respective framework.[74] The GDPR, being binding on legal subjects in EU member states territory, directly grants them the right to a judicial remedy.

The GDPR, in addition, provides for an express right to receive compensation from the controller or processor for the damage suffered as a consequence of a violation of the regulation.[75]

To facilitate data subject rights' access to an effective remedy (administrative or judicial), individuals should be able to be represented—before a supervisory authority or a court—by non-profit organisations active in the field of data protection or human rights, at no cost.

3.4. Accountability, oversight and enforcement

International and regional data protection standards further contain provisions aimed at implementing the aforementioned principles and data subject's rights. Thus, those who process personal data must be accountable for demonstrating compliance with their data protection and privacy obligations, including facilitating

[74] CoE Convention 108+ 2018 (Art. 9, 12), GDPR 2016/679 (Art. 78, 79).
[75] GDPR 2016/679 (Art. 82).

the exercise of the data subject rights. They are also responsible for demonstrating their compliance to the DPA (if existent) upon request.

These provisions aim to strengthen the data subject's position by increasing their ability to check compliance from controllers.

For a comprehensive data protection and privacy regime, accountability of controllers needs to be paired with oversight of the compliance of controllers and the enforceability of the rights and obligations. Therefore, comprehensive data protection and privacy frameworks commonly contain:

- **Legal obligations:** A clear regime of responsibilities of those that process personal data, namely data controllers and processors
- **Independent oversight:** The independent monitoring of the application of the data protection and privacy framework, including compliance of data controllers and data processors with their obligations, through a DPA
- **Administrative and legal redress:** The data subjects' right to a complaint to the independent DPA and to an effective judicial remedy, where they consider that their personal data was not processed in compliance with the law, and also in case its complaint to the DPA has not been successful

3.4.1. Accountability: Legal obligations of data controllers and processors

Most data protection and privacy frameworks allocate the responsibilities to comply with the framework to data controllers and data processors. The **data controller** is the individual or the legal entity that, alone or jointly with others, determines the purpose and means of the personal data processing. That means that the data controller de facto takes decisions, whether or not it has such authority, concerning data processing. The **data processor** is the individual or legal entity that processes data on behalf of a data controller.

Data protection and privacy frameworks typically see the data controller as the main responsible for complying with the data processing principles and the data subject rights. The processor instead acts on behalf of and upon the controller's instructions. Its duties are limited to the agreement with the controller and, if applicable, specific processor obligations in the data protection and privacy law.

The data protection and privacy standards should result in the following obligations of data controllers and data processors (see Table 1 below for detailed explanation), in addition to other obligations under applicable laws. These obligations should be reflected by the respective data protection law.

Table 1 - Obligations of data controllers and data processors[76]

Data protection and privacy principles	Obligations of controllers	Obligations of processors
Purpose specification	Determine the legitimate purpose for each data processing activity	Process data only for the purpose as determined by the data controller, established in the legal agreement with the controller
Data minimisation	Ensure that only minimum data necessary for the fulfilment of the purpose is processed	Ensure that only minimum data necessary for the fulfilment of such purpose is processed, to be provided for in the legal agreement
Lawfulness, fairness and transparency	Identify the legal basis for each data processing activity related to a specific purpose. Ensure fairness and transparency of each data processing activity	N/A – processor processes the data based on the legal agreement. Only the controller requires a legal basis
Accuracy	Ensure that data is accurate and up-to-date	In case processor is instructed in the legal agreement to collect or update data, ensure that data is accurate and up-to-date
Retention limitation	Ensure that data is deleted once the purpose has been fulfilled	Ensure that data is deleted once the purpose has been fulfilled, to be provided in the legal agreement
Security	Ensure that data is secure during each data processing activity, including transfer and storage, and adequate technical and organisational measures are put in place for that purpose	Ensure that data is secure during each data processing activity in accordance with law and particular requirements provided in the legal agreement
Data subject rights	- Ensure that data subjects are enabled to exercise their rights, such as access, rectification, erasure and if applicable, right to object, and rights related to automated decision making - Comply with such rights - If applicable, inform and support data subjects about their right to submit complaints to an	N/A, unless the data controller delegates some of its responsibilities to the data processor, for example to provide data subjects certain information about the data processing or to set-up and operate a hotline through which data subjects can exercise their data subject rights

[76] Original table for this publication.

`

	independent body such as a DPA, or to obtain judicial redress (including financial compensation)	
International Data Transfers	- Only share personal data with entities in other countries or international organisations if the recipient of the data provides a level of protection of personal data that is equivalent to the level established in the data protection and privacy framework of the sender - Conclude and implement data-sharing agreements with data recipients/data senders in a third country or international organisation	Not share personal data with any third party, unless expressly instructed/authorised by data controller to do so, for example with approved sub-processors
General obligations to ensure and demonstrate compliance with the above principles	- Appoint an internal data protection office or officer	- Appoint an internal data protection office or officer
	- Implement data protection impact assessments (DPIA), where applicable	- Implement DPIA on their technologies for provision to the controller
	- Maintain records of processing activities	- Maintain records of processing activities
	- Select only processors which have sufficient guarantees to implement appropriate measures to comply with its obligations under the data protection and privacy framework and sign legal agreement with processor to determine the scope of the data processing to be assumed by it and to oblige it to comply with the applicable data protection and privacy framework	- Sign legal agreements with controller to obtain precise instructions about the data processing activity and limit its liabilities
	- Sign legal agreements determining the allocation of responsibilities when two entities act as joint data controllers	- N/A
	- Notification of data breach to data subjects and, if existent, to data protection authority	- Notification of data breach to the controller
	- Be liable and compensate data subjects for any damages incurred due to violations of the data protection and privacy framework	- Be liable and compensate data subjects for any damages incurred due to violations of obligations of data protection and privacy framework directed to processors or has acted

		outside/against instructions of controller
	- Put in place an organisational data protection policy covering all of the above	- Put in place an organisational data protection policy covering all of the above

3.4.2. Independent oversight

A key element of any accountability mechanism is oversight. All international and regional data protection and privacy frameworks recognise the necessity of an independent supervisory body that monitors and enforces the application of the data protection and privacy framework.

Box 13 - Independent supervisory authority/ data protection authority (DPA)

What is it? A public body, as determined by each jurisdiction, that is responsible for enforcing personal data protection and privacy laws, and that is tasked to monitor and enforce the application of such laws, such as through approval requirements, investigations, and administrative fines, to handle complaints and to promote awareness of rights and obligations thereunder.

The law should establish the DPA's structure, powers and mandate.[77] Good international practice recommends that DPAs should follow these guidelines:

Structure

- Appoint members through a transparent procedure
- Have sufficient resources (financial, technical and human)
- Members should be free from external influence and refrain from actions incompatible with their duties

Tasks

- Monitor and enforce the application of the data protection and privacy laws
- Conduct investigations on the application of such laws
- Handle complaints of data subjects with respect to violations of such laws
- Provide advice to relevant public bodies
- Provide information to data subjects with regards to the exercise of their rights under the law
- Promote public awareness
- Issue recommendations and guidelines

[77] Privacy International 2018 (p. 86-88).

Powers

- Impose sanctions
- Suspend data flows
- Issue reprimands to data controllers with respect to violations of the laws
- Order the controller to comply with data subject requests
- Carry out data protection audits
- In some cases, a data protection law can give the DPA powers to regulate certain aspects of the law, for example, to update definitions or security requirements[78]
- Approve safeguards for trans-border data flows

Such a national DPA is established by law. However, in the absence of respective laws, public authorities may have the power to establish a sectorial DPA. Whether and how this can be accomplished depends on the national laws of the given country.

3.4.3. Enforcement: Administrative and judicial redress

Many international and regional data protection and privacy frameworks recognise the need for a judicial remedy for data subjects, in addition to the data subjects' administrative right to complain to a data protection authority and receive an administrative remedy.[79] For example, judicial redress would be relevant in the case that data subjects do not agree with the DPA's decision, controllers/processors do not comply with the DPA's decision, or data subjects wish to obtain compensation for any damages suffered.

Data subjects will only be able to assert these rights in court or in front of an alternative dispute resolution body if such rights are recognised by law.

3.5. International data sharing

[78] Privacy International 2018 (p. 87).

[79] CoE Convention 108+ 2018 (Art. 9, 124), GDPR 2016/679 (Art. 78-82).

International and regional data protection and privacy frameworks also recognise the importance of protecting personal data not only when processed within a given jurisdiction but also when it "travels across borders".[80]

This may occur, for example, when governments share personal data of migrants that crossed the border from one country to another or when controllers use processors located in other jurisdiction(s), such as cloud providers or other service providers.[81] International data sharing occurs when a government shares personal data with an international organisation and—vice versa—, given that any data processing by international organisations is subject to their own data protection and privacy frameworks, not the national laws.[82]

The scenarios can be grouped as follows:

- **Data sharing between data controllers:** the receiving entity (with a place of incorporation in a different country or being an international organisation) is a new data controller, as it determines the purposes and the means of the data processing. For example, a government shares citizens' personal data in a region hit by a natural disaster with an international organisation that rolls out assistance programs to vulnerable persons targeted by itself.
- **Data sharing between data controllers and their processors:** the receiving entity (located in a different country or being an international organisation) processes the data on behalf of the controller. For example, a government shares personal data of social protection beneficiaries with a service provider incorporated outside of the country of the social protection programme.

In both scenarios, once personal data are shared, they risk losing the protection they enjoyed when processed by the original controller. It is, therefore, important that any data protection and privacy framework provide that where the recipient is subject to another jurisdiction or is an international organisation, the transfer of personal data may only take place where an appropriate level of protection (based

[80] OECD Privacy Framework 2013 (Art. 16-18), GDPR 2016/679 (Art. 44-50), CoE Convention 108+ 2018 (Art 14).

[81] See Section 4.4.2 - Data protection and privacy challenges of specific technologies.

[82] See Box 4 - International organisations, non-governmental organisations and applicable law.

on the data protection and privacy framework of the transferring entity) is secured.[83] An appropriate level of protection of the data recipient can be ensured through:

- the law of the state or international organisation, including applicable international treaties or agreements, receiving the data (this requires a review of those laws), or
- legally binding instruments adopted and implemented by the persons involved in the transfer and further processing

At the same time, data may be shared with a controller subject to a data protection privacy regime providing more robust protections. For instance, data is shared by a government without data protection and privacy laws with the International Committee of the Red Cross, which has very strong data protection policies in place or with a service provider subject to the GDPR. In this case, a data-sharing agreement may still be required, but the concern that the data leaves the jurisdiction of the transferring entity is of minor concern.

3.6. Sensitive personal data

International and regional data protection and privacy frameworks suggest that any data protection and privacy laws or policies should recognise the particular need to protect sensitive personal data. Also known as 'special category' of (personal) data,[84] it is a particular sub-category of personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms. Therefore, they merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.

It typically includes information revealing personal characteristics (including physical appearance), as well as information such as:

- the racial or ethnic origin of the individual
- medical information

[83] CoE Convention 108+ 2018 (Art. 14).

[84] GDPR 2016/679 (Art. 9), CoE Convention 108+ 2018 (Art. 6, 55-61).

- sexual orientation
- political opinions
- philosophical and other beliefs
- membership of associations or trade unions
- religious affiliation
- genetic data or biometric data (when processed solely to identify a data subject)[85]
- data relating to children

For example, biometric data allows the irreversible re-identification of individuals, as such information cannot be modified as an address or name. This increases the risks for an individual if his/her biometric data falls into the wrong hands (identity theft, persecution). In addition, this kind of data is at risk of being used for political purposes or giving rise to unlawful or arbitrary discrimination, limiting or negating the rights of data subjects in general. For instance, religious or racial information being used as a base for denying a social protection benefit.

The GDPR, the Malabo Convention and CoE Convention 108+ generally forbid the processing of such personal data and provide for specific situations in which sensitive personal data may be processed under special safeguards provided therein.[86]

For example, in the area of social protection, the GDPR provides that sensitive data may be processed, without the individual's consent, if

> "processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject".[87]

[85] See 'Glossary of defined terms and abbreviations.'

[86] GDPR 2016/679 (Art. 9), CoE Convention 108+ 2018 (Art. 6, 55-61), Malabo Convention 2014 (Art. 14).

[87] GDPR 2016/679 (Art. 9).

Other appropriate safeguards to prevent adverse effects for the data subject where sensitive personal data is implicated, maybe for instance:

- the data subject's explicit consent needs to be obtained
- laws should be promulgated covering the intended purpose and means of processing, indicating the exceptional cases where the processing of sensitive personal data would be permitted
- laws or competent bodies that require health professionals to maintaining professional secrecy with respect to the sensitive personal data
- measures put in place following a specific risk assessment
- specific and qualified organisational or technical security measures
- individuals' ability to apply for the suppression of their data

These safeguards should not be used alone but ideally in a cumulative manner.

In addition, regarding automated decision-making, when the decision making is based on sensitive personal data, good international practice recommends that the processing should only be carried out if:

- individual's explicit consent has been provided or
- the processing is necessary for reasons of substantial public interest.

4. How to implement data protection and privacy into social protection programmes?

4.1. How to promote and adopt standards for data protection and privacy?

Data protection and privacy standards applicable to social protection programmes in a given country can be created at different levels:

a) Adoption or improvement of a national data protection law
b) Issuance of an organisational policy for the organisation or public authority which implements social protection programmes
c) Development of data management protocols for each social protection programme

4.1.1. National data protection and privacy law

A first fundamental but a relatively high-level and long-term step for implementing data protection and privacy standards into any social protection programme would be the adoption of a national data protection and privacy law. Or, in case this already exists, its improvement and supplementation. In this sense, from the social protection side, authorities could encourage lawmakers to introduce or update data protection and privacy legislation.

Lawmakers in countries envisaging to adopt a national data protection law could take the good practices for data protection and privacy as reference and inspiration.[88] Furthermore, any international or regional data protection and privacy frameworks that apply to the given country need to be taken into consideration. In addition, 'hidden' data protection standards in sector-specific laws such as information or cyber security, electronic communications, financial services, and others need to be considered.

[88] See Chapter 3 – Good international practice of data protection and privacy.

Thus, to suggest a sound draft of a data protection law, lawmakers should first review the social protection and data protection and privacy laws and frameworks in a given country. Then, hold them against the standards presented in this Implementation Guide, namely, the data processing principles, data subject rights, as appropriate, accountability requirements, oversight and enforceability, and transborder data flow/international data sharing. Lastly, map out in a spreadsheet the different requirements under the applicable instruments, including similarities and deviations, as well as all elements that are missing or need to be amended, reinforced or further specified in the existing national law.

Upon the national data protection and privacy law issuance, social protection laws, regulations, and policies may need to be amended to reflect mandatory data protection requirements and enable applying the country's data protection and privacy standards to all social protection programmes in their different phases.

4.1.2. Organisational data protection and privacy policy

In the absence of a national data protection and privacy law, personal data protection and privacy principles and certain essential procedures and provisions should be integrated into an **organisational data protection and privacy policy** applicable to the respective data controller. For example, such a policy would be required from a social protection ministry or department and larger international NGOs implementing social protection programmes as controllers.

By issuing a data protection and privacy policy, the respective organisation or authority would self-impose a data protection and privacy framework governing all social protection programmes implemented by it, thus facilitating the implementation of consistent data protection and privacy standards throughout its social protection programmes.

Such a data protection and privacy policy would contain the data processing principles, data subject rights and accountability mechanisms presented in Chapter 3. However, it could not establish external oversight or enforceability of data subject's rights. The policy would also have to be in line with any international or regional data protection and privacy frameworks to which the organisation or authority is subject.

`

The controller would have to determine the scope of the policy. The data protection and privacy policy could be established for all social protection programmes, thus limited to the personal data of the applicants, registrants, recipients or beneficiaries. However, it could also cover all personal data processed by the controller, including employees, job applicants, vendors, in the case of international organisations, individual donors, and others.

Even when countries have data protection and privacy laws in place, it is suggested to draw up an organisational data protection and privacy policy as it would help demonstrate compliance with the data protection and privacy laws in place.[89] Demonstrate compliance includes, among other things, showing that:

- a policy is in place
- staff is aware of it and have been trained appropriately
- a person who is responsible for compliance has been appointed
- audits are undertaken
- a system for handling complaints has been set up
- being transparent about the use and transfer of data

The data protection and privacy policy needs to be integrated into and adapted to the governance structure of the respective organisation. Its content (for example, security principle, confidentiality) and the bodies and procedures to be established by it (e.g., oversight through a data protection officer, legal redress for data subjects) may overlap with other organisational policies, such as information security, risk management, records retention and the management of confidential or internal intellectual property. Its issuance, thus, requires a detailed review of existing organisational policies.

Box 14 - Data protection and privacy policy

What is it? It is an internal policy that outlines the organisational or authority approach to personal data protection and privacy. It is a set of the data protection and privacy principles, including certain procedures, rules, measures and guidelines that inform how the organisation or authority will ensure the implementation of personal data protection and privacy standards. It also contains the data subject rights and accountability mechanisms.

[89] Sepúlveda Carmona 2018 (p. 54).

It should be:

- in line with any applicable national laws or international and regional frameworks
- possible to implement
- integrated into the organisation's governance structure
- tailored to the structure, scale, volume and sensitivity of the data controller's operations
- easy for staff to understand and follow
- updated according to monitoring and periodic assessment

Why is it important? Having a data protection and privacy policy in place helps to ensure compliance with national data protection and privacy laws and to demonstrate how the organisation is taking measures to ensure compliance.[90] It is particularly important for organisations or authorities which wish to implement good standards of personal data protection and privacy into their operations, if national laws do not contain such standards.

Box 15 - Implementing an organisational data protection and privacy policy

What to include in your policy? The policy should include, as a minimum, the personal data processing principles, data subject's rights and accountability mechanisms, as deemed appropriate by the respective entity. Suggestions on how to structure a policy are as following:

1) Introduction and purpose
2) Scope
3) Definition of key terms
4) Data protection principles:
- Which ones do you commit to?
- Set out appropriate guidance on how to uphold each principle
5) Data subject rights
6) Accountability mechanisms:
a) The establishment of a data protection officer to monitor the implementation of the policy;
b) Regulate roles and responsibilities of specific departments, such as the department owning the personal data internally ('information owner'), the department using such data ('information custodian or steward'), the IT security department, the legal department, the compliance department, the controller/audit department, and others.

[90] GDPR 2016/679 (Art. 24) suggests controllers to implement data protection policies, "where appropriate in relation to processing activities."

7) Treatment of sensitive data: the use of sensitive data of beneficiaries should be specifically regulated, in terms of permitted use purposes, legal basis, data minimisation, strict security measures and short retention periods, among others
8) International data-sharing (if applicable)
9) Other general obligations of the controller as set out in Table 2, such as data breach notification procedures and record-keeping
10) Good practice and practical steps for staff to follow

This list is neither a complete nor an exhaustive one. Each organisation/authority should include what makes sense in its context.

How to implement it?

- Guidelines: Any data protection and privacy policy should be accompanied by guidelines on its the implementation containing guidance on points which are particularly relevant for implementing a social protection programme, such as what legal basis to choose, when and how to use biometrics (if at all), how to allow individuals to exercise data subject rights, how to assess and select third party service providers or processors, etc.
- Cultural change: Creating internal awareness regarding data protection and privacy by communication and training staff is key for implementing the data protection and privacy policy.
- Data management protocols: Establish data management protocols reflecting how the data protection and privacy policy and guidelines will be implemented with respect to each specific social protection programme.[91]

In the absence of national data protection and privacy laws that establish independent oversight and enforceability of data subject rights, the social protection authority could consider (if and to the extent permitted by the applicable laws) alternative mechanisms in order to gap the time until a data protection law is in place:

- With respect to **independent oversight**, a social protection ministry or authority may consider establishing its own external body, which oversees and enforces the data protection and privacy policy and reviews complaints by data subjects concerning alleged violations of their rights by the controller.

[91] See Section 4.1.3 - Data management protocol for each social protection programme.

- With respect to **enforceable data subject's rights**, the ministry could consider establishing alternative dispute resolution mechanisms for data subjects to enforce their rights against the controller, such as arbitration or mediation. The dispute resolution body should have the power to issue decisions that bind the controller.

4.1.3. Data management protocol for each social protection programme

In order to translate data protection and privacy standards (from applicable laws, the organisational policy or, in their absence, from good international practice) to each social protection programme, it's necessary to apply the provisions of the data protection and privacy policy (or in its absence, the data protection and privacy principles). While this does not replace laws nor an organisational policy with binding effect, it at least allows for the implementation of personal data protection and privacy standards.

How the standards will be implemented should be reflected in a **data management protocol** (also called 'standard operating procedures' or 'operational guidelines'). This document ensures that staff and partners act in accordance with the data protection and privacy principles established by law, the organisational policy or, in the absence of any other applicable data protection and privacy framework, only the protocol, as appropriate. Such data management protocol could be part of the programme description.

Social protection programmes around the world go through similar implementation phases along the delivery chain.[92] Therefore, it is important that the **data management protocol** covers at least the following points:

- The data flow in each stage of the delivery chain, for example:
  a. Is personal data needed in the assessment stage or can assessments be done based on aggregate data? E.g., from international organisations or the government?
  b. How will data be collected from individuals? E.g., census-type data collection vs. data collection upon demand/application?

[92] See Figure 1 - Social protection delivery chain.

c. Storage of the data in a MIS operated by an international corporation: Where will the data be stored (in country)? What are the security measures? Who has access to the data?

- All stakeholders and risks
- How each principle is applied in each phase. E.g., for which purpose each data variable is collected or shared with each partner (specified purpose), how data will be kept up to date (retention limitation)
- How data subjects can exercise their rights. E.g., which rights can be granted, and which cannot, how data subject will be informed about their rights
- All accountability measures, to the extent not covered by the data protection policy or laws. E.g., who would be the data protection officer for the respective programme
- All mitigation measures from the data protection impact assessment (DPIA)
- Resources and capacity to train staff on the data management protocol

These points will be discussed in more detail in the following sections. The DPIA will provide much of the information that is relevant for the data management protocol.

4.2. How to conduct a data protection impact assessment (DPIA) and ensure privacy by design?

The processing of personal data can create or increase risks for individuals, groups and organisations. Therefore, social protection programmes should ensure that **impact assessments** are undertaken *prior to* collecting and processing personal data. The purpose of a so-called data protection impact assessment (DPIA) is to identify, evaluate and address the risks to personal data–and, ultimately, to the data subject–arising from a project. A DPIA should ultimately lead to a project design that avoids or minimises any data protection and privacy risks (privacy by design).[93]

Box 16 - Privacy-by-design

Systems should secure privacy-by-design, meaning that data protection and privacy is a default design objective. In other words, systems by *standard* should implement

[93] Kuner and Marelli 2017 (p. 84)

data protection and privacy principles and safeguard individual rights. This should happen *before* designing new social protection programmes or introducing digital technologies.

According to the OECD Privacy Guidelines, the 'privacy-by-design' approach is interpreted broader, meaning that technologies, processes, and practices to protect privacy should be built into the system architecture and not added on later as an afterthought.[94] Privacy should become part of institutional or organisational priorities, programmes objectives, design processes, and planning operations.

Thus, the DPIA needs to be implemented prior to any data processing activity in order to design the data processing in such a manner as to prevent or minimise the risk of interference with the data subjects' rights and fundamental freedoms.[95]

Box 17 - Data Protection Impact Assessment (DPIA)

What is it? It is an assessment of the impact of the envisaged processing operations on personal data. It is the process that helps to systematically identify and minimise the data protection risks of a programme or project, to anticipate and mitigate risks to data subjects and data controllers.

When is it necessary? It is prudent and advisable always to carry out a DPIA prior to processing any personal data. However, it is particularly vital where a type of processing is likely to result in a high risk to the rights and freedoms of individuals.

Exemplary situations where a DPIA is required or strongly advised by some international and regional data protection and privacy frameworks:[96]

- Where processing involves sensitive personal data
- When data processing is used to make automated decisions about people that could have legal (or similarly significant) effects
- When processing children's data
- When processing could result in physical harm to the data subjects if it is leaked
- While systematically monitoring a publicly accessible place on a large scale

Box 18 - Implementing a DPIA

[94] OECD Privacy Framework 2013 (p. 104).

[95] CoE Convention 108+ 2018 (Art. 10).

[96] GDPR 2016/679 (Art. 35) and CoE Convention 108+ 2018 (Art. 10, Explanatory Report Art. 88). Other frameworks advise to carry a privacy risk assessment but do not give further details, such as the OECD Privacy Framework 2013 (p. 16) and APEC 2005 (Art. 44).

How to implement? There are different approaches to conducting DPIAs. The following guidance draws on good international practices from a range of sources.[97] Based on it, follow these steps:

Step 1: Identify the need for a DPIA: Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Setting up a team: Identify the most appropriate DPIA team. The team undertaking the DPIA should be familiar with data protection and privacy applicable frameworks and standards, as well as organisational policies.

Step 2: Describe the processing of personal data:

a) Mapping the information flows: This section should detail (at a minimum):
- the type of data to be collected;
- whether sensitive information will be collected;
- how the data will be collected;
- for what purposes the data will be used;
- how and where the data will be stored and/or backed up;
- who will have access to the personal data;
- whether personal data will be disclosed;
- whether sensitive Personal Data will be disclosed; and
- whether any data will be transferred to other organisations or countries.

b) You might find it useful to refer to a flow diagram or other way of describing data flows.

c) What types of processing identified as likely high risk are involved?

Step 3: Consultation process: Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views–or justify why it's not appropriate to do so.

- Who else do you need to involve within your organisation?
- Do you need to ask your processors to assist?
- Do you plan to consult information security experts or any other experts?

Step 4: Assess necessity and proportionality: Describe compliance and proportionality measures, in particular:

- What is the lawful basis for processing?
- Does the processing actually achieve the purpose?
- Is there another way to achieve the same outcome?
- How will you prevent function creep?

[97] ICOe (n.d.) and Kuner and Marelli 2017 (p. 65-67, 299-305).

- How will you ensure data accuracy and data minimisation?
- What information will you give individuals?
- How will you help to support their rights?
- What measures do you take to ensure processors comply?
- How do you safeguard any international transfers?
- How will you ensure data deletion also by partners?

Step 5: Identify and assess risks:

- Describe the source of risk and the nature of the potential impact on individuals. Include associated compliance and corporate risks as necessary.
- Likelihood of harm: remote, possible or probable
- Severity of harm: minimal, significant or severe
- Overall risk: low, medium or high

Step 6: Identify measures to reduce risk: Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

- Risk: describe it
- Options to reduce or eliminate risk
- Effect on risk: eliminated/reduced/accepted
- Residual risk: low/medium/high
- Measure approved: yes/no

If the DPIA identifies risks, which cannot be mitigated in a sufficient manner, a project may have to be abandoned or set up in a completely different way.

Commented [2]: Is there an example from the social protection area?

How do the DPIA and the data management protocol relate to each other?

The DPIA will collect all relevant facts, identify risks and suggest solutions for risk minimisation with respect to the data processing activities in the context of a new social protection programme.

The data management protocol instead will, based on the information and solutions in the DPIA, describe how the data processing activities will be implemented.

For example, the DPIA would assess the risk to distribute social protection benefits through the services of a mobile money provider, which is subject to laws that require the provider to collect biometric data from the mobile money account holders and share that data with the central bank. Based on this risk, the controller

may decide to distribute the benefits through a bank, which is not subject to the aforementioned laws.

Therefore, the data management protocol would have a specific section dedicated to that bank. It would set out what data will be shared with the bank, for what purpose, who may have access to it, how the data will be securely transferred, and what are the controller's minimum security measures to ensure secure storage by the bank (list applicable technical and organisational measures), when the bank has to delete the data, how to prove that, among other things. This section from the data management protocol will also be relevant to ensure that the bank (processor) will be obliged to comply with the social protection controller's data protection and privacy requirements through the legal agreement.[98]

4.3. How to apply the data protection and privacy standards to social protection programmes?

This Section provides concrete recommendations on how to apply the data protection and privacy standards to social protection programmes. They should be reflected in a data management protocol.[99]

4.3.1. How to limit processing in line with the data processing principles?

(i) For what legitimate purposes do social protection programmes need to collect data?

Box 19 - Checklist of Good Practices: Purpose specification principle

☐ Ensure purpose specification of data: personal data should only be collected for a determined, explicit and legitimate purpose, stated to data subjects at the time of data collection, with subsequent processing also compatible with these

[98] See Section 3.4.1 - Accountability: Legal obligations of data controllers and processors.

[99] See Section 4.1.3 - Data management protocol for each social protection programme.

purposes. Any exceptions or deviations should not generally be allowed unless permitted by law.

Before collecting data, the social protection controller should determine and state the specific purpose(s) for which personal data will be processed in the context of a social protection programme. The purpose(s) should be as specific as possible, explicit and legitimate.

What personal data is needed for a given social protection programme depends on the type of social protection programme and how it is implemented. For instance, the purpose 'provision of social assistance' will not satisfy the requirement that the purpose needs to be specific. The purpose instead needs to be determined with respect to each personal data variable collected and should cover all processing activities throughout the lifecycle of the.

Typically, the delivery of a social protection programme will require different types of data for a range of sub-purposes, namely for:

- **Assessment** of needs and conditions of the affected population
- **Enrolment** of beneficiaries in social protection programme (purpose of identification/verification)
- **Delivery** of social protection programme (authentication)
- **Reconciliation** of social protection programme
- **Monitoring** of social protection programme
- **Complaint and feedback**

Such purposes of the processing need to be clarified and communicated to individuals at the time of collection. In addition, social protection programmes need to be aware of the purposes of processing at the outset of the project, as they will need to identify a legal basis for each of the purposes for which data is processed and communicate those to the individuals as well.[100]

It may happen that during the delivery of the social protection programme, events occur which require the use of personal data for other purposes than those which were stated at the time of collection. For example, a bank is not able to provide

[100] See Section 3.4.1 - Accountability: Legal obligations of data controllers and processors.

liquidity at ATMs in a conflict-affected zone. In this case, the social protection programme would have to choose another delivery mechanism. In order to establish whether this processing is compatible with the purpose for which the data were initially collected,[101] the controller should take into account, among other things:

- Any link between those purposes and the purposes of the intended further processing
- The context in which the personal data has been collected, in particular, the reasonable expectations of data subjects based on their relationship with the controller as to its further use
- The nature of the personal data
- The consequences of the intended further processing for data subjects and
- The existence of appropriate safeguards in both the original and intended further processing

Box 20 - Purpose specification and integration of programme databases

Personal data of recipients or beneficiaries enrolled in a social protection programme are usually stored in a programme specific database (so-called programme or beneficiary database).

The information in programme databases is accessed and managed through software applications called **'management information systems' (MIS).** Sometimes, MIS are also referred to as the programme database and the related management application together.

Through integrated MIS, related programme databases (e.g., a poverty assistance database and a newly established health emergency assistance database) can be, relatively easy, integrated in order to allow them to talk to each other (e.g., use the same identifier and data formatting), so that beneficiaries can be uniquely identified across these databases (so-called integrated programme or beneficiary database) for the purposes of developing an overview who receives what, coordinate interventions, facilitate planning and more generally combine monitoring and evaluation across programmes.[102] Still, the different databases will contain different data of each individual, depending on the respective programmatic purposes.

Commented [3]: Programmatic colleagues to suggest the technical terms used in SP programming.

[101] About further processing for compatible purposes, see Section 3.2. - Data processing principles.

[102] Barca and Chirchir 2014 (p. 24).

`

Whether the new emergency database may **obtain access** to the data of the poverty database, **without obtaining a new legal basis**, such as consent or public interest, depends on:

(i) whether the integration pursues a **legitimate purpose**, such as assurance that all persons in the poverty database will be covered by the emergency programme (purpose: nobody falls through the cracks; quicker access to the data allows for quicker response) or, to the contrary, that persons enrolled in the poverty programme shall not double dip in the emergency programme (fraud prevention), and

(ii) whether this **purpose is compatible with the purpose** stated to the beneficiaries (at the time of data collection) in the poverty database. This depends on the facts and should be assessed as advised above this box.

If the new purpose is not compatible (which would be the norm, for example, in the case of integration with tax payment, electoral, civil or law enforcement registries), the integration of databases should only occur, if provided for by law, the purpose is legitimate, meaning strictly necessary and proportional to the interference with individuals' rights.[103] Data sharing protocols between ministries regulating the integration of the database are not sufficient.[104]

Moreover, according to the transparency principle, social protection programme applicants and beneficiaries should be informed, at the time of data collection and before the databases are integrated, whether data will be shared with other government agencies.

Provided that data is collected and used for compatible purposes or permitted by law and proportional to the interference with data subject rights, many databases could be integrated and managed in this way. One example would be Kenya's

[103] "Determining whether a privacy and data protection rights interference is reasonable and not arbitrary requires balancing each case's circumstances precisely. For example, linking information about social protection beneficiaries to a tax payment database might be justified by an objective of improved targeting and fraud elimination. Similarly, foundational registry (identify registry) integration with functional registries (social protection systems, electoral authorities, etc.) may be permissible when legally allowed and proportional to the specified purposes (e.g., improving various systems' efficiencies). However, integrating social protection databases with law enforcement registries (e.g., local, national, regional and international policing agencies)—even when legally authorised 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 2018, p. 28).

[104] See Section 4.3.4 - How to share data?

integrated beneficiary management system, integrating five programme databases (confusingly called "Single Registry").[105]

Box 21 - Purpose specification and social registries

Recent trends, mainly driven by the World Bank, encourage a different approach going beyond mere integration of programme databases.[106] It suggests collecting information on a large swathe of the population without including them in any social protection programmes, but with the intention to use the information for future consolidated targeting processes designed to serve multiple programmes (so-called '**social registries**' or '**single registries**').[107]

The purpose specification requires that data will be collected and used for a specific, explicit and legitimate purpose. The programmatic purpose behind the social registry (which is only a system not a programme) is to target a large part of or the entire population in a consolidated manner through targeting algorithms processing the available data based on proxy means-test based methodologies. This approach will result in a list of eligible households, or a list of all households ranked on their levels of poverty and vulnerability at a central level. The list will be shared with individual programme implementers who use the list as a basis and often adapt it to their purposes.[108] It may be that detailed and sensitive data about households (often over 100 data variables) will be stored in a social registry without that household ever being enrolled in a social protection programme.

Commented [4]: Social protection specialists to confirm.

Thus, it may be asked how the collection of a large data set (to be stored in a so-called 'social registry') in order to enable consolidated targeting without a specific programmatic context will be compatible with the specific legitimate purpose principle.[109]

According to international good practices, personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[110] Generally speaking, assessments and targeting do not require personal data, they

[105] Barca and Chirchir 2014 (p. 25).

[106] Leite et al. 2017 (p. 66-80).

[107] Barca and Chirchir 2014 (p. 25).

[108] Barca and Chirchir 2014 (p. 38).

[109] If the legitimate purpose of the social registry is to collect detailed data about the lives of individuals for potential targeting in the future, then the data minimisation principle cannot lead to the limitation of those data items. The data minimisation principle can only lead to the minimisation of data items which are NOT needed for the social registry. This is why the amount of data collection for the social registry is a question of whether it pursues a legitimate and specific purpose.

[110] GDPR 2016/679, Recital 39.

can also be conducted based on aggregate or pseudonymised data.[111] Further, it is questionable whether the consolidated targeting is not an undefined, imprecise or vague purpose and, thus, whether it is not, illegitimately, unexpected and objectionable[112] for an individual to disclose a wide range of sensitive information about its life and, eventually, not to obtain any assistance.

Whether the data collection for a social registry can be seen as done for a specific and legitimate purpose, depends on a comprehensive balancing of the pros and cons of the goals to be reached through such a social registry, considering all circumstances in each instance, including:

- the existing social protection programmes and policies in the given country
- the benefits of such a social registry for the government as compared to other less intrusive approaches, as the integration of existing programme/beneficiary databases
- the size of the affected population that would be part of such a registry (to be larger in middle- and low-income countries that have less resources and capacity for its management)
- operational aspects such as the management of data collection, its transformation into information, time-consuming data updates, capacity to implement strong security safeguards
- available resources for assistance, registry update, central management
- likelihood of the vast majority of the individuals to be registered in the social registry to be enrolled on a continuous (poverty based) or repeated (emergency/shock) basis into social protection programmes; if such likelihood does not exist, or only in the foreseeable future when data is already outdated, the number of the data subjects should be reduced/adapted
- staff availability and capacity for managing a big registry on top of existing programme databases
- sensitivity of the data to be collected in the specific country context
- and, last but not least, the rights, freedoms and interests of the individuals, particularly the right not to accept intrusions into their privacy sphere unless for specific purposes under adequate safeguards

Following an assessment, the consolidated targeting envisaged by the social registry could be a legitimate and specific purpose (even though no assistance is guaranteed), if there are strong arguments justifying the consolidated targeting, such as for example […], outweighing the disadvantages and the interference with the individuals' right to data protection and privacy.

Commented [LDG5]: Social protection experts to provide examples.

[111] See Box 25 - Assessments and pseudonymised data.

[112] CoE Convention 108+ (Explanatory Report, Sec. 48).

A data protection and privacy advisor should be consulted when considering engaging in comprehensive data collection for a social registry.

Further, **commercial service providers** may use the beneficiary data obtained from the social protection programme (e.g., beneficiary payment lists) for their own purposes. For example, financial service providers may need to cross-check beneficiary lists against mandatory sanctions lists, retain metadata for law enforcement purposes or profile beneficiaries for creditworthiness.[113]

Box 22 - Collection of metadata by commercial service providers

In addition to the minimum data that the controller of the social protection programme needs to collect in order to deliver it and the data that it will collect in the course of the implementation of the social protection programme (transactional data, data obtained through monitoring and complaints), technologies have developed in a way that they collect a lot of additional data during the implementation, such as:

- metadata on the use of bank accounts collected by financial service providers or the technologies used by them (and operated by a technology provider)
- geolocation and movements of individuals tracked by mobile phone operators
- purchasing behaviour of individuals, and potentially their location tracked by retail voucher redemption application provider

Such data is not needed for the typical purposes set out above to deliver a social protection programme. Social protection programmes need to be aware of these additional data collections at the outset of the project and verify the following points, in the context of a DPIA, to identify risks to individuals:

- Will the social protection programme obtain such data as part of the service, or will the service/technology provider collect and use it for its own purposes?
- If the social protection programme will obtain the data, for which purposes?

  - Such data can be used to understand beneficiaries better (data analytics), to profile them, but also just to feed technologies for machine learning purposes.[114] Are these separate legitimate purposes, not listed above, about which the individuals were informed?

  - Or are the purposes for which the data shall be used compatible purposes which do not have to be communicated to the data subjects? This seems

Commented [LDG6]: Social protection experts to provide examples.

[113] Kuner and Marelli 2017 (p. 153).

[114] See Section 4.3.2 - How to ensure that data subjects can exercise their rights.

improbable, given that the purposes are not strictly linked to the delivery of the social protection programme.

- If the technology provider collects the data for its own purposes, does it act as a processor of the social protection programme or not rather as a new controller?
- If the commercial provider acts as a new controller, the social protection programme should clarify the purposes for which the data are collected, the legal basis, such as a legal obligation or legitimate interests, and whether it is acceptable that the provider keeps that data and uses it as a controller or whether it is preferable to work with another company?
- If the new controller has no legal basis for such data processing, the social protection programme should determine whether such data use is acceptable.

Contractual clauses in the processing agreement should restrict the use of the data (shared with the processor for the implementation of the social programme) for other purposes and the collection and use of additional data by the commercial service provider for its purposes as much as possible. Furthermore, the social protection controller should take measures to ensure compliance by the commercial service providers with the agreement.[115]

Any personal data that is not collected for specific and legitimate purposes nor purposes compatible in addition to that may not be processed since the purpose specification principle would not be fulfilled. A pertinent example is India's national biometric identification database, Aadhaar, which bypasses this data protection principle.[116] In 2009, it was established to standardise government databases. However, it is being used for various other purposes (different and incompatible with the original purpose), from school admissions to obtaining death certificates. The violation of this data processing principle should not be 'healed' by the individual providing their consent to the processing.[117] The OECD Guidelines, however, recognised such an exception, which has been often abused and misused.[118]

[115] See Section 4.3.2 - How to ensure that data subjects can exercise their rights.

[116] Privacy International 2018 (p. 40).

[117] CoE Convention 108+ 2018 (Art. 5), GDPR 2016/679 (Art. 5).

[118] OECD Privacy Framework 2013 (p. 14).

(ii) What data to process for each purpose and how to minimise data?

Box 23 - Checklist of Good Practices: Data minimisation principle

- ☐ Ensure data minimisation: only collect the personal data adequate, relevant and not excessive to accomplish the purposes established at the time of collection.
- ☐ While requesting personal data to stakeholders, enforce the data minimisation and 'only-once' principle to interoperability interfaces between systems. Where possible, avoid requirements for full access to or transfer of databases, and enhance coordination between stakeholders to prevent repeated requests for personal data to data subjects.

Data minimisation works in synchronicity with the purpose specification principle. Information collected in social protection programmes, across and regardless of the stage, should be the minimum necessary to meet the established purposes. For instance, the information collected for the purposes of a cash or in-kind assistance operation needs to be proportionate to these purposes and the minimum necessary.

Commented [LDG7]: Social protection experts to provide examples.

Unnecessary data collection cannot be justified and may increase costs and pose risks for data subjects' rights in both well-known and unpredictable ways. For instance, 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.

Data minimisation is important not only from an individual's rights perspective but also from the information security side. The larger amount of data, the costlier and more complex to guarantee its security. Thus, limiting the collection of personal data is essential, especially regarding **sensitive personal data**.

Box 24 - Data categories to fulfil data minimisation and purpose specification principles

The below list is a rule of thumb for data categories that can be seen as necessary to fulfil the specific and legitimate purposes for implementing a social assistance programme.

- **Assessment** of needs and conditions:

- Detailed socio-economic data (e.g., income, expenditure, household size)
- Food security
- Vulnerability data (e.g., age, gender, location, sensitive data such as health, diseases, disability, status as a refugee, asylum seeker, or citizen)

- **Enrolment** in social protection programme:
  - Data that allows for the *identification* of the individual, such as a legal or functional identity card, and potentially information that allows for the *verification*[119] that the individual is the person it claims to be
  - Benefit amount or items (this is personal data as it relates to an identifiable individual)
- **Delivery** of social protection programme:
  - Data for *authentication* purposes. Sometimes biometric data (e.g., fingerprint, iris scan) are collected for the purpose of authentication and avoidance of double-dipping/fraud[120]
  - Depending on the delivery mechanism (cash in envelope, bank account, prepaid cards, mobile money or other), specific data will be needed/created, such as bank account details, phone numbers (equalling mobile money accounts). In addition, laws applicable to the service provider may require the collection of additional data by the service provider (e.g., biometric data for the distribution of SIM cards)
  - Phone number to *communicate* to beneficiaries completed cash transfers, distribution locations or other important information regarding the cash delivery
  - In the case smartphone applications are used to communicate with beneficiaries, allowing beneficiaries to manage their credits or the comparison of retail shop prices, identification and authentication data will be required
- **Reconciliation** of social protection programme:

[119] Identification is the process where someone claims to be a particular person by showing a document including his/her picture and personal information. Verification is conducted only once. It is the process of ensuring whether that person is indeed the person that he/she claims to be (e.g., by checking that the ID is valid, that the person showing the ID looks like the picture on the ID). Once the identity of the person is verified, it needs to be authenticated each time he/she tries to get access to resources (iDenfy 2020).

[120] In middle- and higher-income countries, double registration in several government services is more common (Chirchir and Barca 2020, p. 36). With respect to biometrics, the need to authenticate beneficiaries and the principle of data minimisation, see Section 4.4.2. - Data protection and privacy challenges of specific technologies.

- Transactional data reported by the service provider (e.g., cash-out of benefits, unredeemed benefits)
- In the case of voucher programmes, where beneficiaries can redeem vouchers issued in contracted retail shops for food or other items, data about the voucher redemption and the items purchased

- **Monitoring** of social protection programme:
  - Phone number or other details to contact and interview beneficiary
  - In some cases, data to authenticate beneficiary may be necessary but, usually, no reason to assume that non-beneficiary would participate in the interview
  - Information requested from the beneficiary by the monitors may contain personal data (e.g., personal opinions)
- **Complaint and feedback**:
  - In the case of beneficiaries, data to authenticate caller (e.g., voice biometrics)
  - With respect to general questions of the affected population, no ID is necessary
  - Reported information can be personal data when it relates to an individual; can be sensitive data, such as complaints about harassment

However, at the design stage of every social protection programme, it needs to be asked, with respect to each data variable processed throughout the delivery chain, whether the respective purpose cannot be reached without such data variables or with less intrusive data.

Box 25 - Assessments and pseudonymised data

Governments, international organisations, and NGOs may assess, target and assist overlapping populations. When assessing needs and conditions before setting up a social protection programme, it may be more effective to request socio-economic and other vulnerability data from different stakeholders than to conduct time and cost consuming assessments of the affected population.

In this case, applying the data minimisation principle means that the sharing entity will provide a pseudonymised list containing all the information relevant for the assessments but not any identifying data. Instead of names, ID, address, phone

number and other identifying data, the list will contain a pseudonym or number representing each individual.[121]

Once the data recipient has conducted the assessments based on the pseudonymised list, targeted a sub-group thereof, and intends to implement assistance, it will need to contact the targeted beneficiaries for the purpose of benefit delivery. At this stage, personal data is necessary to identify and assist the targeted persons. The data recipient may thus request the personal data of the targeted persons by listing their pseudonyms.

To follow through with this data sharing between two controllers, three requirements need to be fulfilled:

- the purpose pursued by the new controller needs to be compatible with the purpose stated to the beneficiaries at the time of the data collection
- the sharing controller has a legal basis for sharing that data with the receiving controller who envisages another social protection programme (e.g., consent or legitimate interests)
- the parties enter into a data-sharing agreement

Data minimisation at the data collection stage can be reached through on-demand registration compared to census like registrations. This will depend on the awareness and trust of individuals that a registration will indeed result in enrolment in social protection programmes.

Commented [LDG8]: Social protection experts to provide examples.

Box 26 - Assurance to donors and data minimisation

Donors requesting assurance that their funds have reached targeted beneficiaries may request counter-signed beneficiary lists or reports of financial service providers as evidence, which contain personal data. While the purpose (assurance) is legitimate, the request for personal data violates the data minimisation principle.

The personal data of all beneficiaries are not necessary, therefore excessive, for donors, given that they neither intend nor will be able to reach out to all these beneficiaries to confirm the receipt of assistance.

Instead, assurance can be reached by providing anonymised payment lists or reports (deleting identifiers, signatures, thumbprints) and a confirmation by the

[121] Unfortunately, sophisticated techniques that allow datasets to be de-anonymised (see Box No. 37 - Erase or anonymise personal data?) exist. Good international practice for sharing public data and ensuring that the data from individuals and individual households remains confidential is to use 'differential privacy' (NCSL 2021).

responsible social protection officer or manager that benefits have been delivered to all individuals on those lists. Also, if required, detailed information about the benefit delivery process and existing monitoring processes, can be provided.

(iii) Which legal basis to choose for the social protection programme?

Box 27 - Checklist of Good Practices: Lawfulness, fairness, and transparency principle

- ☐ Determine the legal basis for each processing activity relating to a specific purpose
- ☐ Obtain and process personal data with a lawful basis, fairly and in a transparent manner
- ☐ Ensure transparent and fair information and communication with data subjects by clearly informing them, at the time of data collection, on how, why and when their personal data is being processed, both where they have provided this directly to a controller and where the controller has obtained it from another source
- ☐ Inform data subjects about their data rights
- ☐ Guarantee that any information and communication relating to the processing of personal data is easily accessible, legible, understandable, and adapted to the relevant data subjects.
- ☐ Ensure that the data subjects' consent is informed, freely given and specific. In the case of processing sensitive personal data, consent should also be explicit. It should be possible to withdraw consent at any time. Any exceptions where obtaining consent is not possible should be very limited, requiring heightened levels of transparency, only applied on an individual case-by-case basis, and another legal and legitimate basis for personal data processing is required.
- ☐ Offer data subjects alternatives that will allow them to continue receiving assistance should they not provide or object to the programme's processing of their personal data, especially in the case of sensitive personal data.

Commented [9]: Maybe it is worth discussing with the SPIAC-B 'consent' in the context of social protection programmes. Is it a legal basis for processing?

Beneficiaries of social protection programmes 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 of all processors), and how long it will be held.

Legal basis

Under the principle of the lawfulness of data processing, a legitimate legal basis is required in order for the personal data processing operations to take place. The social protection controller, namely the social protection ministry/authority,[122] needs to determine the legal basis/es on which it intends to process the data for the respective purposes of the social assistance programme, prior to the collection/processing of the data.

Which legal bases are available depends on the domestic data protection and privacy laws. **If the national data protection and privacy laws provide for the range of legal bases** (namely consent, contract with the data subject, legal obligation, public interest, vital interest, legitimate interests),[123] which legal basis should a public authority choose for the implementation of a social protection programme?

- **Processing necessary for compliance with a legal obligation:** a legal obligation could be a suitable legal basis if the government is obliged by a social protection law to provide social assistance to individuals. This would be the case in contributory social protection schemes, where, by law, the contributions made by beneficiaries (and their employers) determine their entitlement to benefits paid by the state. In each case, it should be reviewed whether the national social protection laws provide for an obligation of the social protection authorities to provide social assistance and under what conditions. Conditions to be fulfilled by the applicant would still amount to a legal obligation. Conditionality (availability of funds) or leeway on the side of the public authority may result in the law not representing a legal obligation. It may even be that beneficiaries are legally obliged to provide their data.
- **Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority:** The national laws of low- and middle-income countries may not provide for an explicit obligation of the

Commented [10]: Social protection experts to confirm.

[122] For a detailed discussion of how international organisations should select the legal basis for humanitarian cash and in-kind assistance programmes, see Kuner and Marelli 2017 (p. 59-73). For the selection of the legal basis for projects where international organisations support national social protection programmes as joint controllers or processors, see Box 30 - Legal basis and joint programmes of international organisations and social protection authorities.

[123] See Section 3.2.3. - Lawfulness, fairness and transparency.

social protection authorities to provide social assistance, but still foresee that the social protection authorities shall implement certain social protection activities, such as the provision of emergency assistance to affected populations in the case of natural or man-made disasters, or […]. Also, it could be that social protection laws provide for certain activities to be carried in the exercise of official authority vested in the controller. Data processing necessary for the performance of these tasks provided for by law would fall under this legal basis.[124] This would cover the respective assessments, enrolment, delivery, reconciliation and monitoring.

- **Processing necessary in order to protect vital interests**: Data processing may serve both a ground of public interest and be necessary to protect the vital interests of the data subjects, as, for instance, in the case of data processed for the purpose of monitoring a life-threatening epidemic and its spread or in humanitarian emergencies.[125]
- **Processing necessary for legitimate interests not overriding data subject rights and freedoms**: Public authorities may not rely on the legal basis of legitimate interests.[126] This mirrors the requirement that authorities may only act on the basis of laws and may not determine to process personal data for activities outside of their public tasks or obligations as laid down by law. This is particularly important in the context of the use of new and complex technologies, for example, biometric technology. Public authorities may not use such technologies for the processing of personal data unless laws provide for it and the respective safeguards.
- **Processing necessary for the performance of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract:** Social protection authorities would likely not be able to use this legal basis for the processing personal data of beneficiaries or applicants, as they typically do not enter into contracts with beneficiaries or applicants in the context of the implementation of social protection programmes.
- **The data subject has given consent to the processing of data**: Consent of data subject is the most 'popular' legal basis for the processing of personal data. However, in the context of social protection programmes implemented

Commented [11]: Social protection expert to please insert some examples of what social protection laws in low- and middle-income countries usually provide in terms of social assistance activities to be implemented by the respective ministries.

Commented [12]: Social protection expert to please review this statement.

[124] CoE Convention 108+ (Explanatory Report Sec. 47), GDPR 2016/679 (Recital 45).
[125] CoE Convention 108+ 2018, (Explanatory Report Sec. 47).
[126] GDPR 2016/679 (Art. 6).

by public authorities which act on the basis of laws, there is no room for individuals to provide their consent to the processing if to the extent that processing is required in order to implement public tasks. In other words, if a law says that a social protection authority has the task to identify vulnerable people and enrol them, then the social protection authority has a legal basis for processing the data it needs. It does not need another legal basis, such as consent.

When and when not to reply in consent of the data subject?

Now, consent could be seen as being more inclusive or more empowering legal basis. However, in most cases, this will not be the case. First, even if individuals were asked for their consent, such consent may not be valid given that individuals have no real choice to refuse to consent due to a situation of need and vulnerability. Particularly when the social protection programme does not offer any alternative assistance that does not require personal data processing.[127] In this case, it may be little worthy to ask for consent. Second, processing data based on public interest does not mean that individuals cannot dispute the processing. While they cannot 'withdraw their consent' (which has not been given), they can still not provide their data in the first place and, at a later stage, object to the processing at any time. However, the right to object does not apply when the public authorities are legally obliged to process the information, for example, in the case of law enforcement or fraud investigations, or when public authorities can demonstrate a compelling interest to continue the processing.[128]

Commented [13]: We should add a few words about social protection programmes where providing personal data is mandatory, if any. Advice from social protection experts to be obtained. Examples are welcomed

In all cases, the term 'necessary' is to be strictly construed. The data processing needs to be truly necessary, and not only convenient to fulfil a legal obligation, a public interest task or an activity carried out in the exercise of official authority, all laid down by law.

Finally, it is important to note that relying on a legal basis other than consent does not discharge the controller from its obligation to **provide comprehensive**

[127] See Box 29 - Consent: Some specific conditions to be considered valid.

[128] See Section 3.3.5 - Right to withdraw consent and to object to data processing.

information to the data subject about the data processing (transparency) and process the data fairly (fairness).

If national data protection laws only provide for consent, it would have to be assessed what the reason for this restriction was, whether public authorities are subject to the law or whether the law can be interpreted in a way that other legal bases such as public interest task or legal obligation can be relied upon in addition to consent. Domestic legal advice should be obtained.

However, there may be **other specific processing activities of the social protection programme for which it could be advisable to rely on consent.** Therefore, it should be assessed in detail concerning each data processing activity by which legal basis it will be covered. For example, it may be that the sharing of personal data with a financial service provider will be covered by a public interest task (delivery of cash to beneficiaries). Still, the management of data subject's complaints and feedback collected by a private call centre may not be covered by the public authority's legal obligation or public interest task. In this case, it may be appropriate that the call centre collects individuals' consent, as the processor, on behalf of the social protection authority (the data controller). Monitoring instead should always be based on public interest or legal obligation, if applicable.

Box 28 - Lawful processing of sensitive data

Under which conditions sensitive data like biometrics, health or disability data can be lawfully used for the implementation of a social protection programme, depends also on the manner the national laws regulate the use of sensitive data. If it is generally prohibited as suggested by the GDPR and CoE Convention 108+. No legal basis would be required for such processing, but rather a law would have to specifically authorise the use of specific types of sensitive data for specific reasons by specific public authorities or private entities, as for the case of social protection laws.[129]

In the absence of such a regulation by national law, it is strongly suggested to use sensitive data only if appropriate safeguards are put in place. The consent of the data subject alone cannot suffice.

[129] See Section 3.6. - Sensitive personal data.

If consent is used as a legal basis for any processing activity in the context of the social protection programme, the following should be taken into account.

Box 29 - Consent: some specific conditions to be considered valid

In some international and regional data protection and privacy frameworks,[130] consent needs to fulfil some specific conditions to be considered valid. It needs to be:

- **Unambiguous:** It should be evident that the data subject has consented and to what. This requires more than just proof that they have read the terms and conditions. There should be a clear sign that they agree.
- **Timing:** Consent should be obtained at the time of personal data collection or as soon as it is reasonably practical thereafter.
- **Freely given**: Consent should be regarded as freely given if the data subject has genuine or free choice to consent or is able to refuse or withdraw consent without prejudice.
- **Vulnerability**: When weighing the validity of consent, the data subject's vulnerability should be considered. Vulnerability varies depending on the circumstances. The following factors should be taken into account:[131]
  - the characteristics of the data subject, such as illiteracy, disability, age
  - health status, gender and sexual orientation
  - the location of the data subject, such as a detention facility, resettlement camp, remote area
  - environmental and other factors, such as unfamiliar surroundings, incomprehensible language and concepts
  - the data subject's position concerning others, such as belonging to a minority group or ethnicity
  - social, cultural and religious norms of families, communities, or other groups to which data subjects belong
  - the complexity of the envisaged processing operation, particularly if complex new technologies are employed
- **Informed and meaningful:** To be accepted as the legal basis for processing consent should be informed. Consent should not be a "check-the-box" exercise. Meaningful consent occurs when the data subject makes an informed decision. Informed consent requires that information and communication related to the processing of personal data be accessible and easy to understand. Data subjects should understand all implications related to the processing of the information they provide.

[130] GDPR (2016/679), CoE Convention 108+ 2018.

[131] Kuner and Marelli 2017 (p. 46).

- **Documented:** Where the processing is based on the data subject's consent, it is essential to keep a record of it to be able to prove that the data subject has consented to the processing. Additionally, it is important to record any limitations/conditions for the use of the consent and the specific purpose for which it is obtained.
- **Specific:** The data subject is aware of the fact that and the extent to which consent is given tied to a specific context. Consent should be dissociated from other terms and conditions (including giving separate consent options for different types of processing or types of data, e.g., consent to the processing of location data but not health data).
- **Refusable and revocable:** The data subject should have the right to refuse to consent or to withdraw consent easily and at any time. Consent should be as easy to withdraw as it is to provide. If data subjects expressly refuse to consent, they should be advised about the implications, including the possible effects this may have on assistance that might or might not be provided by social protection programmes. However, if assistance cannot be provided in the absence of consent, then consent cannot be considered a legal basis for the processing.

Commented [14]: Social protection experts, would you agree with this?

Consent should be given by:

- a **clear affirmative action**: it should require an active process by the individual, rather than a passive opt-out process. Mere silence, inactivity or pre-validated forms or boxes should not, therefore, constitute consent.
- or by a **statement**: oral or written (including by electronic means). This constitutes **explicit consent**, which must be expressly confirmed in words. Data subjects do not have to write the consent statement in their own words, but they should clearly indicate their agreement to the statement (e.g., by signing their name or ticking a box next to it). Implied consent should be avoided since it does not meet international data protection standards and good practices.

An expression of valid consent, which is only one of several legal bases and thus may fulfil the lawfulness principle, does not waive the need to respect the other basic principles for the protection of personal data and privacy set out in the applicable data protection regime that the controller is subject to.

The operationalisation of consent requirements should be context-specific and discussed and adapted for each particular social protection programme.

Consent should not be used, if:

- the data subject is not in a position to give consent
- the public authority is not able to obtain consent due to prevailing security or logistical conditions in the area of operations or the scale of the operation and data is obtained from a third party, like an international organisation

- the consent cannot be valid because the individual is being particularly vulnerable or having no real choice to refuse consent
- digital technologies are involved, and its risks are difficult to be fully appreciated by data subjects[132]

If national laws do not provide for data protection principles (including legal bases) and no regional data protection frameworks are applicable, it is nevertheless suggested to apply the good standards for the legal bases presented in this Implementation Guide, to the extent applicable social protection laws provide for legal obligations and/or public interest tasks of social protection authorities to process the law.

Box 30 - Legal basis and joint programmes of international organisations and social protection authorities

International organisations implement humanitarian programmes in accordance with their own internal rules and obligations, including on data protection and privacy (acting as controller).

Often, international organisations cooperate with public authorities to implement social protection schemes on behalf of those authorities (acting as a processor) or jointly together with those authorities (potentially acting as joint controllers). In these cases, national data protection and privacy laws and the international organisations' data protection and privacy framework applicable to its activities may overlap and contain deviating requirements.

In the context of national social protection programmes (differently from humanitarian aid programmes), beneficiaries need to be treated in accordance with domestic laws. For example, their data need to be collected based on the legal basis which the law provides. Public authorities and international organisations need to cooperate closely so that this is reflected in the design of the social protection programme. This may relate to other domestic legal requirements as well.

If the national laws do not provide for any personal data protection and privacy or contain gaps, international organisations and the public authorities should cooperate to reflect the good international practices and standards of data protection and privacy as presented in this Implementation Guide and as contained in the international organisations data protection and privacy framework in the project design, the data management protocol and the legal agreement governing their cooperation.

[132] Kuner and Marelli 2017 (p. 58).

Transparency

Transparency means that personal data is not used in ways that data subjects would not expect and are not aware of. No personal information should be secretly processed.

Transparency requires that information and communication related to the processing of personal data be accessible and easy to understand. Data subjects should understand all implications related to the information they provide.

Transparency can be challenging, especially given the vulnerability of some beneficiaries, particularly those of non-contributory social protection programmes. Thus, 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).

Box 31 - Providing information to enable transparency

Good international practice recommends that the below information is provided:

- The identity of the data controller
- What types of personal data need to be collected and processed
- Why such personal data are requested (specific and legitimate purpose)
- What legal basis the data will be processed
- The identity of all processors with whom the data is expected to be shared and for which specific purposes (enrolment, data storage, authentication, delivery of cash or food, monitoring)
- How to exercise the data subject rights (access, update, correct or delete data or to complain about the data processing, and the right to object and the right to withdraw consent[133]
- Beneficiary's right to hold back the data and the implications, particularly any alternatives to obtain benefits without providing the personal data

Particularly for public entities, transparency means not only informing the data subjects. It also means, and especially in the context of engagements that are difficult to understand for data subjects (such as the use of complex technologies like artificial intelligence, profiling and automated decision making), to be transparent to the public, the media and civil society organisations about the details

[133] See Section 4.3.2 - How to ensure that data subjects can exercise their rights.

of the data processing that such technologies engage in. Accountability would also require publishing the contracts entered into with the technology providers (excluding confidential information like price).

Fairness

Fairness is related to the form or 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). It also means that no unfair practices will be used, such as the use of hidden data registration devices (e.g., voice recorders) or deceiving data subjects into supplying information.

Box 32 - What if individuals do not want to provide their personal data or object to the processing?

Beneficiaries have the right to withhold their data or, at a later stage during the project implementation, may object to the processing of their data.

Controllers should try to find out what the specific reason for the objection to the processing is. The concern could relate to a specific partner about which the data subject was informed or the provision of specific data variables.

Depending on the concerns, if known, the controller should determine how to offer data subjects alternatives that will allow them to continue receiving assistance without providing their personal data or specific data variables.

The answer to these questions is not ready, and there is no step by step to follow. What is important to highlight is that social protection programmes should take this issue seriously and take on a genuine commitment to respect the rights of individuals. They should intensely seek technical and organisational solutions to make these rights effective without interrupting or denying, as far as possible, the delivery of services and benefits.

If it is not possible to offer a genuine alternative to individuals receiving assistance, beneficiaries need to be informed about the implications for withholding the data.

Commented [15]: Could stakeholders please provide an example for this case? The rest of the text should then be adjusted appropriately.

(iv) How and when to ensure the accuracy of personal data?

Box 33 - Checklist of Good Practices: Accuracy principle

- ☐ Ensure—in all data processing phases (collection, registration, storage, use, and sharing) and throughout the social protection delivery chain—that personal data is accurate, kept as complete as possible and, where necessary, kept up to date.
- ☐ Put in place protocols to update, correct or erase inaccurate personal data without delay, including complaint and feedback mechanisms to allow data subjects to request such updates.
- ☐ Define who is responsible for updating the personal data, for implementing the procedures for that to happen.
- ☐ Conduct regular spot checks on the accuracy and relevance of the personal data recorded.

In different data processing phases (collection, registration, storage, use and sharing) of the social protection delivery chain, personal data should be accurate, complete and, where necessary, up to date. If such data is inaccurate, incomplete or outdated, it could lead to poor decision-making, and may have unwanted or severe implications (e.g., wrongly denying access to a social protection service or benefit, benefit fraud).

Box 34 - How to implement the data accuracy principle?

In practice, this means that social protection programmes should:

1. Plan data accuracy. Before you collect or receive personal information:
- determine what the minimum data fields are which you need for the specified purposes (the fewer data, the easier to be kept up to date)
- if you receive data from third parties, obtain dataset description (metadata) and assurance that the data is accurate, complete and up-to-date, and, if applicable, information on data inaccuracies
- determine how often up-dates are needed
- determine mechanisms on how to keep data accurate and up to date. For example, through regular census, integrating databases (e.g., linking data to civil registries, where deaths, births, marriages, etc. are registered, however considering the privacy implications thereof),[134] through smartphone applications for data subjects
- determine the sufficiency of funds for this exercise, carefully consider and address other challenges to the accuracy of information, and adjust data collection exercise, if required
2. Ensure any information collected is correct and corresponds to reality.

[134] See Section 4.3.1 - How to limit processing in line with the data processing principles.

- correctly record the information provided
- correctly record the source of the information
- ensure that the status (valid/not valid) of personal data is clear
- validate the data through additional information, e.g., ask proof of residence address or income/payslip to prove that the ID presented belongs to the person having presented it

3. Assess data accuracy

- where does the data come from (who collected it) and how often it is updated?
- is the information consistent across all systems?

4. Implement and monitor data accuracy

- put in place protocols to update, correct or erase inaccurate personal data without delay, including grievance and redress mechanisms to allow data subjects to request such updates (comply with the individual's right to rectification)
- define who is responsible for updating the personal data, the procedures and protocols for that to happen
- periodically ask individuals to update their details, especially if the information could have serious implications for them
- ensure that not only positive data will be recorded – e.g.,
- inform individuals that intentional delivery of false information may amount to fraud and have implications for the assistance
- keep a historical record of changes (updates, rectifications, erasures) on data
- conduct regular spot checks on the accuracy and relevance of the personal data recorded

Commented [16]: Any examples here?

Commented [17]: Question to programmatic colleagues, what happens if beneficiaries provenly provide wrong information to obtain more benefits? Will they be excluded from programmes? Or their assistance adapted?

Is it necessary to always have personal data up to date?

It will depend on the purpose for which the social protection programme uses the specific personal information. For instance, in the case of a benefit or service that depends on the level of income of the individual or the household, the income information should be kept up to date. However, the address information may not need to be regularly updated. Also, "data variables associated with income and occupation have a higher dynamism and ought to be updated every 1 to 1.5 years, while variables associated with housing and ownership of goods have a lower dynamism, so that updating every 3-3.5 years is recommended."[135]

The effort to ensure data accuracy should increase according to the importance of having personal data accurate. Suppose the personal data is being used to make

[135] Irrazaval 2004, cit. in Barca and Chirchir 2014 (p.39).

decisions that may significantly affect the individual concerned, his/her family or household. In that case, social protection programmes need to put more effort into ensuring accuracy.

(v) When to delete data?

Box 35 - Checklist of Good Practices: Retention limitation principle

- ☐ Ensure retention limitation principle: personal data should be retained, in a form which permits identification of data subjects, for no longer than what is required for the purposes for which such data was originally processed. The period of time for which the personal data are stored should be limited to a strict minimum. Any exceptions to this should be strictly limited and clearly defined by law, or, in the absence of laws, by the organisational policy or the data management protocol.
- ☐ Establish a retention policy and schedules specifying the retention periods for all the personal data that is held, determining how it will be subsequently securely deleted from databases or anonymised, both by the data controller and any third parties that have had access to the data.

Social protection authorities, as well as their processors, should retain specific categories of personal data for defined periods of time. And they should be able to demonstrate at any time, to supervisory authorities (as well as upon requests of data subjects), why and for how long they hold personal data in a form that permits identification of individuals. This is the case, either because:

- the original purpose or a compatible purpose applies
- a new specific and legitimate purpose for the processing of data has arisen, for which the controller has a new legal basis (public interest, legal obligation) and about which the controller has informed the data subjects in question (including about the new data retention period)[136]
- the data needs to be retained for legal or regulatory requirements such as for income tax and audit purposes, or litigation

Individuals must be informed at data collection about how long their data will be retained.

[136] See Box 20 - Purpose specification and integration of programme databases.

Box 36 - How to implement the retention limitation principle?

Social protection authorities should establish an organisational retention policy (in addition to or contained in the data protection and privacy policy),[137] specifically for personal data, that includes the following:

1. A list of the types of record or information held
2. The purpose the personal data is used for
3. Specific and standard time limits (retention period) for different categories of personal data. E.g., for biometric data (specific) the standard retention time limit would be five years.
4. A system for ensuring that the predetermined retention periods are respected in practice (assigning responsibilities, and defining procedures) and for reviewing, at appropriate intervals, if personal information held is still needed
5. Ensure that staff across the organisation knows what information they should be keeping and where
6. How personal data will be subsequently securely deleted from databases or anonymised by the data controller
7. Ensure that any processors that have had access to the data to delete the data following the fulfilment of the purposes for which they have obtained it, through their contractual obligation (including evidence/confirmation of the deletion; audits of controllers to ensure deletion).

If no such retention policy exists, the social protection programme manager should determine, in the data management protocol,[138] the retention period for all data types processed for the purposes of the social protection programme.

Other controllers who have received the data should not necessarily delete the data. Beneficiaries should be asked whether they wish to have their data also deleted from the systems of other controllers. For example, from systems of international organisations, who have received the data from the social protection authority and use it now for humanitarian assistance.

[137] See Section 4.1.2 - Organisational data protection and privacy policy.

[138] See Section 4.1.3 - Data management protocol for each social protection programme.

Box 37 - Erase or anonymise personal data?

Social protection practitioners have two options to comply with the retention limitation principle: erase (delete) the data or anonymise it. Archiving instead does not delete data.

Erasure

Data being held in physical form (e.g., paper documents) should be irreversibly destroyed. Electronic data should be deleted, including any copies or back-up on the system or devices.

However, it is not always possible to erase all traces of electronic data. A key issue is to ensure that the data controller puts the data 'beyond use', meaning:[139]

- there is no intention to use or access this again or to share it with any other organisation
- ensuring appropriate technical and organisational security measures
- commitment to permanent deletion of the information if, or when, this becomes possible.

Anonymisation

Alternatively, personal data can be anonymised in such a way that it is no longer in a form that enables the identification of data subjects. For example, the data can be presented at a general level (aggregated) or turned into statistics in such a manner that individuals can no longer be identified.

However, full anonymisation is often challenging to achieve. In addition, data that has been anonymised may not stay that way over time. There are sophisticated techniques that allow datasets to be **de-anonymised**: meaning the reverse process in which previous anonymous data is cross-referenced with other data sources to re-

[139] ICOd, n.d.

identify the individuals whose personal data was contained in the data set rendered anonymous. Thus, data subjects are no longer anonymous.[140]

Social protection programmes should test the anonymised data set according to its level of acceptable risk. This process should be documented, for instance, as part of the DPIA.

If following erasure or anonymisation, the data still allows for the identification of individuals, and, thus, represents personal data, the data protection and privacy standards presented in this guide will continue to apply.

(vi) How to ensure the security of data processed by social protection programmes?

Box 38 - Checklist of Good Practices: Data security principle

- ☐ Protect personal data, as well as the infrastructure relied upon for processing, with security safeguards—during storage, transmission and use—against risks such as unlawful or unauthorised access, use and disclosure, as well as accidental or deliberate loss, destruction, modification or damage of data, by implementing appropriate technical and organisational measures to keep the database secure.
- ☐ Ensure that any data processor, processing data on behalf of a data processor, also implements appropriate technical and organisational measures through assessments, contracts and compliance monitoring.
- ☐ Set up security protocols and systems governing the access to the programme's social information systems, which includes establishing and regularly updating an information security policy and a clear distribution of data-processing responsibilities and access control permissions.
- ☐ Regularly undertake information risk assessments of the security requirements, implement appropriate measures to mitigate those risks and monitoring mechanisms to ensure security safeguards are in place.
- ☐ Ensure personal data is stored securely, whether in an electronic database or using a paper filing system. Ensure that the use of techniques such as cloud storage complies with national laws, including the data protection and privacy regime as well as any data localisation laws, and careful consideration of security controls offered by using cloud technologies.
- ☐ Ensure higher security levels when processing sensitive personal data, such as biometric or health data, which requires a specific risk assessment, and should be

[140] Good international practice for sharing public data and ensuring that the data from individuals and individual households remains confidential is to use 'differential privacy' (NCSL 2021).

authorised and limited by data protection and privacy laws, regulations, frameworks or internal guidelines, and needs appropriate safeguards.[141]

To ensure that social protection programmes are implemented with appropriate security safeguards to secure personal data, the social protection authority should first ensure that its policies and their level of implementation are sufficient to ensure the protection of personal data. This will require:

- **Review of existing policies:** In particular, policies relating to information security and confidentiality of business information, to ensure that personal data is covered therein and that the physical, technological and organisational measures for the protection of personal data are reflected.[142] Otherwise, update policies. IT policies require information owners to classify information as strictly confidential, confidential, official use, public and then develop standard security measures related to these classifications. Personal data of beneficiaries should generally be classified as strictly or highly confidential data and enjoy respective protection.
- **Resources:** Data controllers must assign sufficient resources to develop and implement the information security policy framework, as well as the security framework for each specific social protection programme.
- **Organisational measures:** Implementation of the organisational measures,[143] in particular training on staff against the most common data security breaches, namely:
  a. To keep equipment and paper records secure and inaccessible for unauthorised individuals (in cupboards, lock equipment with passwords whenever leaving the computer, etc.)
  b. Not send personal data files by unsecured emails
  c. Keep passwords secure
- **Guidelines:** Development of specific guidelines for social protection programme managers on what security aspects to consider when setting up a social protection programme. Such guidelines would normally be part of the

[141] See Section 4.4.2. - Data protection and privacy challenges of specific technologies
[142] See Section 4.1. - How to promote and adopt standards for data protection and privacy
[143] See Section 4.1.2. - Organisational data protection and privacy policy.

guidelines on how to implement the organisational data protection and privacy policy principles in social protection programmes.[144]

The next step would be the security safeguards of the concrete envisaged social protection programme. The social protection manager should ensure:

- To involve information security specialists in the DPIA to assess, in line with the technological and physical security measures:
  a. the security of servers where personal data is stored
  b. the security of the network
  c. the security of software processing personal data
     i. the programme database
     ii. the software application MIS to manage the programme database and automate core business processes
     iii. the integration of programme databases through integrated MIS – access to both databases should be limited to authorised staff only
  d. the security of hardware processing personal data, such as:
     i. tablets for data collection
     ii. functional identity cards with pictures or even biometrics
     iii. electronic voucher cards
     iv. fingerprint readers, in case they store biometrics and other personal data
     v. smartphones used by beneficiaries to access benefits or exercise their privacy rights, to the extent possible
  e. the security of data transfer technology (encrypted email, API, clouds with access of data sender and recipient)
  f. with respect to any software or hardware provided by third party, assess the provider's organisation, technological and physical security measures, including:
     i. location of server where database is stored, including in the case clouds of service providers are used
     ii. the provider's internal personal data processing systems

[144] See Section 4.3. - How to apply the data protection and privacy standards to social protection programmes.

iii. any platform for the exchange of beneficiary lists, reports, and other personal data
iv. any applications for use by data subjects to access their benefits, for example in the case of mobile banking or mobile money

- to implement any particular security requirements identified in the DPIA, such as the treatment of biometrics or any other sensitive data or to abstain from a particular software or other service provider due to unsolvable security flaws
- to regularly undertake risk assessment of the security measures to ensure they are up-to-date; to be reflected in the data management protocol
- to reflect any security requirements relating to service providers identified in the DPIA in the contracts with such providers[145]
- to carry out regular IT audits of the third parties to monitor and ensure compliance with security measures—to be reflected in the data management protocol

What concrete hardware or software security standards should be applied to the processing of different categories of personal data, or how the security of systems will be tested goes beyond the scope of this Implementation Guide. It will be managed by the information technology division, ideally comprising a cross-functional team with legal and personal data protection and privacy experts, under the supervision of the social protection programme manager.

Who should be authorised to access personal data?

The information collected for social protection purposes should only be accessed–on a need-to-know basis–by authorised staff of the social protection authorities or other authorised users of third parties (service providers, partners).

Still, the biggest threats to the security and integrity of an information system come from such authorised users and not from external actors such as hackers.[146] Persons, who have been trusted with access, may disclose data intentionally or

[145] See Section 4.2 - How to conduct a data protection impact assessment (DPIA) and ensure privacy by design.
[146] ISPA (2016).

unintentionally (human error). In addition, cultural factors may cause the disclosure of data not deemed as confidential. This reinforces the importance of setting appropriate operating procedures and training staff on the confidentiality of personal information and individuals' rights to privacy.

Sharing personal data sets with third parties should follow specific procedures.[147] Sharing personal data with other ministries for the purpose of integrating databases is neither a question of data security (as the data will be shared securely and accessed by, formally, authorised persons), nor of data sharing (given that ministries are typically part of the same legal entity of the state), but foremost a question of whether there is a **legitimate purpose** which justifies combining different and unrelated personal data sets by a ministry, causing a greater interference with persons privacy rights.[148]

Personal data security breaches

An important element of any data protection and privacy framework is the handling of data security incidents. A personal data security 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, limitation of their rights, discrimination, identity theft or fraud, financial loss, reputational damage, and other economic or social disadvantages. Most breaches occur through human error.

Usually, organisations and authorities have non-personal data specific security incident management plans in place which cover generally the handling of security incidents with respect to confidential business information of an organisation. Any such existing data breach management plan should be updated to cover the specific requirements of personal data and the respective technical and organisational measures. Such a plan should basically set out, among other things:

- what constitutes a personal data security breach
- who determines that a data security breach has occurred and thus initiates the implementation of the data security incident plan

[147] See Section 4.3.4 - How to share data.

[148] See Section 4.3.1 - How to limit processing in line with the data processing principles.

- specific responsibilities of the respective organisational departments, such as data protection officer, information owner, department where the incident occurred, IT department, communication department, legal department, etc.
- immediate response to the security incident (first two days), such as investigation how the breach occurred exactly, scope of the data breach, what data is at risk, immediate mitigation measures, notification obligations to data protection authority
- long-term response to the security incident, if existent, public communications, i.e., to the press, review of legal rights of the controller against processors and/or potential rights of data subjects against the controller, notification to data subjects

Box 39 - Breach notification to data protection authority and/or data subjects

The breach notification should include as a minimum:

- the type of incident/ nature of the breach
- the date of the incident
- the cause
- those who were affected
- the type of personal data compromised
- the number of people whose data was compromised
- the likely consequences
- the measures taken to address the breach and mitigate adverse effects

In addition, the affected individuals should be given the necessary tools to minimise the harm caused by the breach. For example, in the case of an online application where data subjects can update or correct their personal data, the notification should suggest or even enforce a password reset.

4.3.2. How to ensure that data subjects can exercise their rights?

Box 40 - Checklist of Good Practices: Rights of data subjects

☐ Respect, promote and facilitate the exercise of the rights of the data subjects.

☐ Widely disseminate awareness of the rights of data subjects among organisational and social protection programme staff, with concrete guidelines, and offer support through continuous formal training.

☐ Ensure the right to information: provide individuals, at the time when personal data are obtained, detailed information about why, how and until when their data will be processed. It is important to secure the information necessary for

individuals to make an informed decision about whether to share or not their personal data.

- ☐ Ensure the right to access and challenge: data subjects are able to easily obtain (request and be given) confirmation of whether a controller processes personal data concerning them and, where that is the case, access to such data and information about its processing (collection, storage or use). If the request for information has been refused, the data subject should have the right to be given the reasons why, and to challenge such denial.
- ☐ Ensure the rights to rectify and erase: data subjects are allowed to rectify (correct, update or modify) personal data processed about themselves to ensure such data is accurate, complete and kept up to date. Data subjects should, in certain circumstances, have the right to request that the data controller erase their personal data.
- ☐ Ensure the right to object: if data has been collected based on public interest or legitimate interests, data subjects can object, at any time, to the processing of their personal data. If they object, the onus should be on the data controller to demonstrate legitimate grounds for the processing which override the individual's interests, rights and freedoms or for the establishment, exercise or defence of legal claims.
- ☐ Ensure rights related to automated decision making: data subjects are not subject to purely automated decision making, including profiling, which produces legal or other significant effects to them. Where exemptions allow for solely automated decision making, they should be subject to very strict limitations, and data subjects should have at least the right to request (in a simple way) and obtain human intervention, to express his or her point of view, and to challenge the decision.
- ☐ Ensure the right to submit a complaint and to an effective remedy: data subjects are able to submit a complaint to an independent supervisory authority and to request an effective judicial remedy via the courts, 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.

Each social protection programme needs to respect the applicable data subject rights. When designing and implementing social protection programmes, social protection authorities, development and humanitarian agencies, and social protection practitioners, in general, should take the following steps with respect to data subject rights:

(i) Map data subject rights under applicable frameworks

Map which are the rights of the data subjects recognised in:

- applicable data protection and privacy laws
- the applicable regional or international frameworks and/or
- organisational data protection and privacy policy

to which the data controller is subject.

(ii) Determine data subject rights for the social protection programme

In the absence of such frameworks, determine the data subject rights, as per the good practices and standards presented in this Implementation Guide, which shall be granted to the data subjects and reflect those in the data management protocol.[149]

The rights of data subjects with respect to a social protection programme implemented by a public authority (controller) comprise two different types of rights:

a) The rights exercisable against the controller should include the following:[150]
   - Right to information
   - Right to access
   - Rights to rectify
   - Right to erase, if applicable
   - Right to object or, if applicable, to withdraw consent
   - Rights related to automated decision making (including profiling), if applicable

These again can be divided into the rights which are granted at data collection (see (iii) below) and those which can be asserted throughout the implementation of the social protection programme (see (iv) below).

In the absence of laws or a policy, the controller needs to determine:

---

[149] See Section 4.3.1 - How to limit processing in line with the data processing principles.

[150] OECD Privacy Framework 2013 (p. 15), CoE Convention 108+, GDPR 2016/679 (Art. 9) and Privacy International 2018.

- Which processing activities are based on a legal obligation, public interest and/or consent
- In case of the processing necessary for a **legal obligation**, whether it wants to allow:
    - for the right to object to processing (e.g., GDPR does not) and
    - for the right to erase the data (e.g., GDPR does not)
- In case of processing necessary for a **public interest**, whether it wants to allow:
    - for the right to object to the processing (e.g., GDPR allows it, unless the controller has compelling legitimate grounds overriding the interests, rights and freedoms of the data subject, or for the exercise of legal claims) and
    - for the right to erase the data (e.g., GDPR allows it, if the data subject has successfully objected to the processing).

b) In addition, there are the rights for redress, in case the controller did not comply with the above rights, or violated other provisions of the applicable data protection and privacy framework, leading to causing harm to the data subjects:
- Right to submit a complaint to an independent body
- Right to an effective judicial remedy, including financial compensation

Neither the right to submit a complaint to a data protection authority nor the right to an effective judicial remedy can be implemented by the social protection authority. Such rights can only be provided for in national laws. However, the social protection authority should inform data subjects about them, if they are applicable.

(iii) At data collection: inform about the processing and data subject rights

Data subjects need to be provided with all information necessary for them to make an informed decision about whether to share their personal data when applying for a service or benefit. The data management protocol shall provide, that the data subject shall be informed about:

- the processing in the context of the social protection programme

- the data subject rights that he/she has against the controller and how to exercise them
- if applicable, his/her rights to submit complaints to an independent body or to obtain a legal redress (in court), and how to avail of these rights and
- how such information shall be provided

If the data is collected from the data subject, such information shall be provided at the time of data collection. How the information will be given, depends on how the data will be collected.

- At a census data collection, individuals may be informed orally, through videos, or through brochures/in writing
- If the data is collected through an individual application for a social protection programme, the information shall be provided in the context of this process
- If individuals provide their data through online applications, they should receive an easy-to-understand privacy statement describing the processing

If the data is obtained from a third party, the individuals need to be informed as soon as reasonably possible after receipt by the new controller. Also, this information may be provided, depending on the circumstances, through diverse means, for example, in a sensitisation session to which data subjects will be invited through text messages.

(iv) During social protection programme: allow to exercise the requests to access, rectify, erase, object and, to intervene in automated decision making

Social protection programmes usually have the so-called complaint and feedback mechanisms (CFM) or complaint and appeal mechanisms in place to allow individuals to ask questions and communicate concerns. These can be used to also address data subjects' requests to the controller for access, rectification, erasure, to object to a specific processing activity and to intervene in automated decision making. They can take several forms (hotlines, help desks, boxes to provide written complaints or other) and be operated by the controller itself or outsourced to a private company or an NGO (processor).

CMFs can be set-up per social protection programme or covering several programmes in a country, even of various controllers. CMFs are not to be confused with organisation-internal mechanisms to address complaints by a data subject about the processing by a controller.[151] Such complaints should not be accepted by the complaints and feedback mechanism, but beneficiaries asked to directly contact the respective internal office which is competent to receive such complaints.

In each case, a DPIA should be conducted prior to the establishment of these communication channels given the sensitivity of the information they process. For example, where individuals communicate the reasons for which they wish to withdraw their data. A DPIA should be mandatory, when:

- a third-party implements the complaint and feedback mechanism
- a third-party technology is used to collect, manage, and store the information of data subjects for their identification and their complaint/requests, and
- personal data will be shared with other international organisations or NGOs, particularly in the case of multi-agency hotlines

The DPIA will assess two broad areas of data protection, namely:

- whether the design of personal data processing activities/flows to be conducted by the CFM comply with the data processing principles (first pillar of data protection and privacy standards).[152] The DPIA will serve as a guideline to design the CFM in a data protection compliant way[153]
- Whether the CFM appropriately allows data subjects to exercise their rights (the second pillar of data protection and privacy standards)[154]

Box 41 - CFM call centre: Compliance with data protection principles

The call centre, whether operated by the controller or a third party (processor), needs to establish detailed operating procedures, which will, among other things, determine the following personal data protection and privacy issues:

[151] See Section 4.4.1 - Steps for ensuring privacy compliance by technology providers.

[152] See Section 4.2. - How to conduct a data protection impact assessment (DPIA) and ensure privacy by design.

[153] See Box 17 - Data Protection Impact Assessment (DPIA).

[154] See Section 3.3 - Data subject rights.

`

- how to provide information, for example, on an answering machine, on the details of the data processing, including the legal basis (typically consent), and collect of consent

- which data needs to be collected for which purposes, for example, name, phone number and electronic voucher card number, if the card does not work and beneficiary requires a new one, social protection programme is to check the issue and call beneficiary back; name, phone number and detailed information in case a protection case is reported

- in which cases no personal data has to be collected, namely, if the caller does not require feedback, for example if he/she reports that in a given location sacks of rice are rotten or one out of several ATMs does not work

- how to minimise the access of the call centre operator to information, and avoid abuse of data for different purposes, for example, use a technology which irrevocably closes the window where personal data has to be recorded, only thereafter the claim can be reported in a new window, which ensures that individuals speak each time to a different operator; clean desk policy: operators cannot take smartphones, USB sticks, paper or pens inside the phone booth nor can they print, take screenshots nor download data

- in which cases data shall be shared with other agencies, for example a caller requests to be included in a social protection programme of a different controller (e.g., different international organisation)

- when the data will be deleted, for example data with respect to technical issues having been resolved may be deleted within short time frames, data with respect to protection cases or litigation potential need to be retained at least until the resolution of the matter, or within established retention periods.

Such operating procedures will result in even more detailed talking scripts for the call centre operators.

Following the conduction of the DPIA, detailed CFM operating procedures (to be reflected in the data management protocol for the social protection programme) should be established in order to ensure that data subjects can exercise their rights. The data subject rights should be simple to exercise.[155]

The operating procedures should contain detailed guidance at least on the following points:

[155] OECD Privacy Framework 2013.

- a clear allocation of responsibilities: if there is a data protection office, all data subject requests hereafter, should be channelled to, and assessed, by that office. If there is no data protection office, the suggested responses to requests by operators should be approved by programme manager in order to ensure consistent responses; the programme manager should also decide about potential fraudulent access requests, requests for deletion or objection to processing
- processes to inform data subject about the acceptance or rejection of a request, within a given timeline (set by laws or the organisational policy, if not by the data management protocol) and a sound reason
- guidance how to how and where to record the data subject requests and their fulfilment/rejection
- for all rights: how the caller can be verified as beneficiary of the social protection programme or as legal representative of the beneficiary with authorisation to access the data (power of attorney): what documentation is acceptable (for example, ID number, birth data and address, power of attorney, in case of the representative) and what isn't, in order to avoid fraudulent access requests.[156]
- right to access:
    - how to produce effectively and within a legal or self-given timeline a complete and understandable copy of the individual's data held by the controller and its processors
    - how to make available such a copy: determine easily accessible but still secure ways for individuals to obtain access and/or a copy
    - an efficient organisational data management system and privacy technologies may support the implementation of this right
- the right to rectification
    - how to obtain proof of the inaccuracy or incompleteness: depending on country circumstances require public records of births, marriages, death; what to do in cases that no proof can be provided (change of address for example)
    - how to set up processes, ideally automated, to ensure that processors and joint controllers will be informed about the rectification
- the right to erasure

[156] Manavis 2019.

- if the social protection authority recognises the right to erasure, how to seek reasons for that request and inform about the implications on the enrolment in the social protection programme[157]
- how to ensure that data is erased within the established retention periods
- ideally automated, to ensure that processors and joint controllers will be informed about the rectification

- the right to object to the processing
  - how to determine whether processing needs to continue despite the right to object, namely in which cases there would legitimate grounds for the processing that override their interests, rights and fundamental freedoms[158]

(v) Right to submit a complaint to a DPA and right to a judicial remedy

If these rights are recognised by national laws, social protection authorities should inform data subjects about them and provide guidance on how to exercise these rights.

Good practices with respect to complaints to a data protection authority would be:

- To have a complaint form available (in paper and online) for data subjects
- To have the contact information regarding the data protection and privacy authority easily accessible to data subjects
- State should provide for the data subjects to take action against a supervisory authority where it has failed to deal with their complaint
- Individuals should be empowered to act themselves, as well as instructing others (including NGOs) to take action on their behalf
- Provide the means for individuals to have access to an effective judicial remedy via the courts (e.g., offer public defender free of charge for people without resources to pay for a private layer)

[157] See Box No. 32 - What if individuals do not want to provide their personal data or object to the processing?
[158] See GDPR 2016/679 (Art. 21).

With respect to legal redress, if the law provides for data subjects to be represented by NGOs before a court, controllers should explain this and provide accessible contact details of NGOs active in this field.

If no national or sector-specific data protection authority exists, but the public authority has a data protection and privacy office(r) or the social protection programme has established a data protection and privacy office(r), then the data subject should be informed how to address complaints to those respective bodies or persons. These complaints should not be accepted by the CFM.

Table 2 - Obligations of entities and data subject rights

Data subject rights	Entity obliged to respect obligations, including data subject rights	Where to exercise the rights
Access, rectification, erasure, objection	Controller	CFM / DPO
Submit complaint about controller/processor or other violations	Controller, processor	DPA, if provided by law If no DPA: DPO
Obtain judicial remedy	Controller, processor, DPA	Court, if provided by law

4.3.3. How to be an accountable social protection controller?

Box 42 - Checklist of Good Practices: Accountability principle

☐ Have in place an organisational data protection and privacy policy that is integrated into the governance structure and that establishes internal oversight mechanisms and bodies (e.g., data protection and privacy committees and officers), ensuring personal data protection and the right to privacy are covered,

`

and the compliance with the organisational and/or domestically applicable data protection regime.

- ☐ Ensure the undertaking of a DPIA before processing personal data (i.e., before data collection), and define what safeguarding measures will be applied, especially when the processing is likely to result in a high risk to the rights and freedoms of natural persons.
- ☐ Establish clear lines of accountability, where data controllers and data processors take all appropriate measures to comply with the obligations established in the applicable data protection regime. The fulfilment of data protection and privacy obligations also need to be monitored and ensured when outsourcing or subcontracting services.
- ☐ Set up mechanisms to detect and investigate personal data breaches, develop a contingency plan for responding to an actual personal data breach and equivalent sanctions for infringement. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, inform the relevant supervisory authority (if existent) and the affected data subjects about the loss or unauthorised acquisition of their personal data (breach notification) in an appropriate and timely manner.
- ☐ Establish effective complaint and feedback mechanisms which data subjects are aware of and which they can access to file request access, rectification, erasure or object/complain about the processing.
- ☐ Ensure that it includes an independent supervisory authority that has the power to receive complaints, investigate (administrative remedy) them and apply sanctions or refer the case to a court (judicial remedy), if applicable.

The main elements of a data protection and privacy framework for a social protection authority are:[159]

- a clear framework of obligations of controllers and processors
- independent oversight by a DPA
- administrative and judicial remedies for data subjects

Such a framework—with binding obligations for controllers and processors, enforcement powers of the data protection authorities, and enforceable rights for individuals—can only be established by law.

[159] See Section 3.4. - Accountability, oversight and enforcement.

In the absence of such laws (but also in their presence), social protection data controllers (public and private, such as larger NGOs) are encouraged to implement **organisational data protection and privacy policies** which reflect the data protection and privacy standards.[160] In this case, they will have in terms of accountability:

- a clear internal framework of data protection and privacy rights and obligations of data subjects and controllers (which is, however, not legally binding on processors but can be forced against them through contractual means)
- if established as suggested in this Implementation Guide[161] and permitted under national laws, an external and independent ad-hoc oversight body to which data subjects can submit complaints, otherwise the data protection office will assume this task
- no possibility of individuals to obtain efficient legal redress in front of courts

However, the organisational policy does not replace data protection and privacy laws. Many data processing activities should not be carried out without laws determining appropriate safeguards to protect the data subject rights and freedoms. This would be the case, for instance, if the processing of sensitive data, the integration of databases, or the use of technologies using automated decision making or other complex technologies require a lot of data of vulnerable individuals.

The public authority should establish a data protection office or appoint a data protection officer who acts as the first point of contact for all data protection and privacy concerns in the organisation. In addition, among other things, it may provide guidance on the conduction of DPIAs and how to implement the data subject rights, approve international data sharing and the handling of sensitive data, lead the response to data security breaches, and may even support the adoption of the data protection and privacy policy.

Suppose there is no external DPA. In that case, the data protection office can assume the task to monitor compliance with the data protection and privacy policy, if applicable, and assess and decide over complaints by data subjects. In that case, its

[160] See Section 3.1. - Data protection and privacy standards and Section 3.4. - Accountability, oversight and enforcement.
[161] See Section 4.3.3. - How to be an accountable social protection controller.

office should be as independent as possible regarding instructions from within the organisation and funding. Data subjects should be informed to direct their complaints directly to the DPO (email, phone, name) and not through the CFM.

Box 43 - Data protection office or officer (DPO)

A data protection officer needs to ensure that an organisation complies with existing data protection and privacy regulations when processing the personal data of any data subjects concerned, such as staff, customers or beneficiaries. Any DPO must have adequate expertise concerning data protection and privacy, and knowledge about the way the organisation works.

Even though the DPO forms part of the organisation, they must perform their function independently. Therefore, organisations should avoid conflicts of interest, and their staff should not instruct the DPO about their duties. The DPO should manage their budget, not report to any direct supervisor, not be an employee in a contract, or not be a data processing controller.

The appointment of a DPO is specified, for instance in the GDPR,[162]which clarifies the requirement of instating a DPO whenever data processing is carried out by a public authority, regular and systematic monitoring of individuals on a large scale is necessary during processing and the data processed is of a particular category (including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, genetic data, health data or sexual orientation).[163] The CoE Convention 108+ specifies the instalment of a DPO as an obligation of a data controller to ensure personal data protection and privacy.[164]

Equally, social protection programmes or development and humanitarian organisations require the appointment of a DPO to ensure the accountability of data controllers in alignment with data protection and privacy regulations and data security.[165] Furthermore, any humanitarian organisation should pursue an audit of the DPIA, for instance, by a DPO.[166]

Without data protection and privacy laws and organisational policies, there is no accountability, no oversight, no enforceability. Data management protocols will allow demonstrating that a controller envisages to comply with data protection and

[162] GDPR 2016/679 (Art.37).
[163] GDPR 2016/679 (Art.9).
[164] CoE Convention 108+ 2018 (p. 25).
[165] Kuner and Morelli 2017 (p. 46).
[166] Kuner and Morelli (p. 89).

privacy standards set therein. They are, however, not binding to the controller itself (unless obligations are assumed in contracts, for example, with joint controllers), will not be examined by any external oversight body, and are not enforceable by data subjects.

4.3.4. How to share data?

Box 44 - Checklist of Good Practices: Data-sharing

- ☐ Regulate personal data-sharing between government agencies. Information between different databases may only be integrated if unambiguously authorised by law, established preceding the event, and the data subject is informed about it at the time of data collection.
- ☐ Regulate third party access to personal data by establishing a data-sharing agreement that clearly establishes who controls the information and who holds responsibility as custodian of the databases. Strict rules should apply when sharing or disclosing personal data, with measures that prevent data breaches, establish minimum safeguards against hackers and sanctions and redress measures to address successful cyberattacks.

Data sharing is a broadly used term, typically covering the following scenarios:

a) The transfer of personal data from one controller to another or both ways
b) The joint processing of personal data by one or more controllers
c) The processing of personal data by a processor on behalf of a controller which may require the exchange of personal data one or both ways

The most frequent scenario, under c) "the processing of personal data by a processor on behalf of a controller", has been extensively described in this Implementation Guide.[167] It requires a **data processing agreement**.

The exchange of data between controllers, under a), could occur, when a social protection ministry exchanges data with a large NGO acting as controller of social protection data sets and registered in the same jurisdiction, each using the data set for their own purposes.

Commented [18]: Any instances come to your mind where social protection ministries exchange data with private companies which act as controllers as well?

[167] See Section 3.2. - Data processing principles.

`

This type of data sharing is likely less risky, particularly in cases where the national data protection and privacy legislation, to which both controllers are subject, is strong. Probably for this reason, the EU GDPR does not even require data sharing agreements for this scenario. **International data sharing** instead may cause a deterioration (or improvement) of the safeguards that the data becomes subject to, when it crosses borders, for example, for the use of a social protection ministry of a neighbouring state or by an international organisation.[168]

Joint controllers, under b), determine the purpose and means of data processing jointly. For example, two international organisations implement cash transfer jointly: One agency assumes the assessments, targeting and monitoring, the other implements the cash transfers. The EU GDPR expressly requires a data sharing agreement for this type of activity.[169]

For accountability purposes, it is good practice to establish data-sharing agreements between separate and joint controllers, and data-sharing protocols between government agencies.

Box 45 - Data-sharing agreement between controllers

What is it? It is a written agreement between two or more parties establishing the terms and conditions for the sharing and receiving of personal data.

Why is it important? To comply with the accountability principle and also because it:

- clearly defines the purpose of the data sharing
- allows the different stakeholders involved to have a better view and understanding of their particular roles and responsibilities
- outlines what will occur with personal data in each step of the process
- establishes rules and procedures

Box 46 - Implementing data-sharing agreement between controllers

How to implement it? A data-sharing agreement needs to reflect appropriate safeguards depending on the volume and sensitivity of the data that will be shared.

Some suggestions on what to include on the agreement would be:[170]

[168] See Section 3.5. - International data sharing.

[169] GDPR 2016/679 (Art. 26).

[170] ICOa, n.d.

`

1. **What is the specific and legitimate purpose of the data-sharing initiative?**
- why the data-sharing initiative is necessary
- its specific aims
- the benefits it is expected to bring to individuals or society more widely

2. **Which other organisations will be involved in data sharing?**
- contact details of other organisations' Data Protection Officer (DPO) and other key members of staff
- procedures for including additional organisations in the data-sharing arrangement
- procedures for dealing with cases where an organisation needs to be excluded from the sharing agreement

3. **What data items are going to be shared?**
- Explain in detail the types of data the organisation is intending to share with other organisations
- In some cases, it may be appropriate to attach "permissions" to certain data items, so that only particular members of staff are allowed to access them, for example, ones who have received appropriate training.

4. **What are the responsibilities of the controllers?**
- Both controllers will be subject to the same laws. If the laws are not in line with best data protection standards, the agreement should list compliance by the new controller with all data protection and privacy standards, including data protection principles, data subject rights and minimum accountability measures (data protection officer)

5. **Has the data been collected lawfully, for legitimate purposes and is accurate and up-to-date?**
- The controller who will share the data shall warrant that it processes the data in compliance with applicable data protection laws, in particular that it has collected the data lawfully, for legitimate purposes, only the necessary data and that the data is accurate and up-to-date, otherwise information about inaccuracies.

6. **What is the lawful basis for sharing?**
- If the sharing entity is a public sector organisation, it should also set out the legal power under which it is allowed to share the information
- If consent is being used as a lawful basis for the disclosure, the controller can only share the data of persons who have provided consent. The agreement should also address issues surrounding the withholding or retraction of consent.

7. **Is there any sensitive personal data?**
- The relevant conditions for processing should be documented.

8. **What about access and individual rights?**
- In the case of data sharing between two controllers, the new controller will become responsible vis-à-vis the data subjects, and the old controller will be responsible to respect the data subject rights (such as the right of access to information, right to object, and requests for rectification and erasure). The

agreement could contain obligations to inform each other about requests or ask data subjects when requesting data deletion from one controller, whether its data also held by the other controller should be deleted and inform the other controller thereof.
- In the case of joint controllers, the agreement should state which controller is responsible for responding to individuals who exercise their data subject rights. However, individuals may choose to contact any controller.

9. **What happens in case of a data breach happened to one controller?**
- Liability and indemnity clauses for the case that the individual claims compensation from the controller who has not suffered a data breach
- Information of the respective other controller?

Box 47 - Exchange of data between ministries and integration of databases

Typically, all ministries are legally part of the same legal entity, the state. The state, thus, is the controller of all data processed by its ministries.[171] As a consequence, the exchange of personal data between bodies which are part of one legal entity–i.e., controller–(for example, two ministries of the same state), does not qualify as a data sharing as described above. These bodies have no separate legal personalities and cannot enter into a legal agreement with each other. Public authorities instead may have a separate legal personality than the state.[172]

Nevertheless, any data processing activity, including the sharing of data between ministries or departments, needs to be compliant with the applicable laws or good international practices of personal data protection and privacy presented in this Implementation Guide.

While no legal agreement may be needed, for accountability purposes, it is suggested that a **data sharing protocol** will be agreed upon with basically the same information as relevant for the data sharing agreement, with the following particularities:

- the new purpose for which the personal data shall be used by the controller (the state, represented by the requesting ministry) needs to be specific, explicit and legitimate and
- the controller (the government, represented by the requesting ministry) needs to identify a legal basis for the new purpose, unless such a purpose is compatible with the purpose which was stated to individuals at the time of data collection.

[171] This needs to be reviewed and confirmed in each country's case by lawyers admitted to the respective jurisdiction.
[172] Also, this needs to be reviewed and confirmed by lawyers admitted to the respective jurisdiction.

4.4. How to work with providers of digital technologies?

Technology providers can improve and assume more and more processes in the delivery of social protection programmes that previously were carried out by the social protection controller itself. Nowadays, a lot of data is stored with and managed through systems provided and operated by technology providers on behalf of social protection programmes.

For instance, currently, data is typically not stored anymore on local servers but on the cloud. Management information systems (software applications) allow for easy targeting based on algorithms, creation of beneficiary lists, and analysis of beneficiaries' preferences and behaviour. Beneficiaries receive their benefits over smartphones and, in the absence of government-issued IDs, can (or must) identify and authenticate themselves through their fingerprints, iris or other biometrics.

The cooperation with providers of digital and data-driven technologies, such as cloud-based technologies, technologies allowing for automated decision making, using big data for data analytics and artificial intelligence, requires a **comprehensive risk assessment** before any engagement. In addition, it requires precise and enforceable contracts and close compliance monitoring with respect to best data protection and privacy standards and—very importantly—concerning the observance of other human rights.[173] The latter is, however, not covered by this Implementation Guide. [174]

It is also critical to avoid vendor lock-in problems concerning external technology providers. This means not becoming dependent on a single provider, while not being able to switch to a different vendor without substantial costs, legal constraints, or technical incompatibilities. Prioritise systems and technologies that can be used independently afterwards. Above all, seek agreements where local staff can be trained in the use (and, where applicable, the development) of technologies and systems.

[173] Alston 2019 (p. 15).

[174] For further information, see Alston 2019 and 2020.

This section provides concrete recommendations for ensuring compliance with data protection and privacy standards when working with digital technology providers. Further, it highlights a few data-driven technologies to describe their specific data protection and privacy challenges.

4.4.1. Steps for ensuring privacy compliance by technology providers

Controllers can publicly procure technologies or in-kind contributions in the form of services. In whatever way an engagement is envisaged, it is recommended to take the following steps to ensure that digital technology providers comply with the data protection and privacy laws applicable to or the standards determined by the social protection controller.

(i) In the due diligence phase

The following information should be gathered from the vendor:

- Data protection and privacy laws applicable to the vendor and, in case of cross-border data flows, or any international or regional data protection frameworks binding the state where the vendor is incorporated
- Legal assessment whether the laws contain the main elements of data protection and privacy standards presented by this Implementation Guide. If they do not, make suggestions:
  - how the processor achieves accountability and provide evidence, for example, organisational data protection and privacy policy (including security incident plans, data retention policy), binding commitments to adhere to code of conducts approved by supervisory authorities
  - how independent oversight can be obtained, for example through membership in professional associations which conduct audits
- Data protection and IT security certifications
- Details of competent supervisory authority
- DPIA on the technology that is being offered, assessing its compliance with the data protection and privacy standards presented in this Implementation Guide, highlighting:
  - all data flows

- the processing and the access of the provider to which data, including metadata
- the purpose of each data processing activity by the provider (as processor, and, if applicable, as controller)
- how data collection and use is minimised
- if the processor acts also as a controller, for which data, for which purposes and on what legal basis. Example, a financial service provider processes beneficiaries' data for the implementation of cash transfers, as a processor. Under law, it also needs to do know-your-customer checks and, thus, use the data as a controller
- whether how and for what purposes personal data of social protection beneficiaries will be combined with data obtained from other sources (e.g., social media, big data held by the provider) and for what purposes (e.g., profiling, automated decision making)
- security:
    - where the data is stored and through which jurisdictions it will travel
    - how the data is secured against data security breaches
    - in case of sensitive data on clouds, how the data could be secured against access by the provider without compromising the service (e.g., encryption applied by the controller)
- data retention and how personal data will be deleted from all systems. Describe risks of identification of data subjects following deletion
- More specific questions with respect to biometrics, cloud-based services, and AI

- If technology interfaces with data subjects, detailed information about:
    - how end-users can participate in the design of technologies and evaluate them in a participatory manner
    - the accompanying programmes designed to promote and teach the needed digital skills to data subjects[175]
- Provide audit and/or investigation reports by data protection authorities in the last ten years (including reason, outcome, fines, implemented measures, including adjustments of services/technologies)

[175] Alston 2019 (p. 16).

- Detailed information with respect to data security breaches in the last ten years (including cause of breach, scope, impact on data subjects, financial compensation or fines, short term and long-term measures)
- Detailed information with respect to data protection and privacy related lawsuits (cause, outcome, penalty)

(ii) Have in place a specific process, which allows to come to an informed decision weighing all privacy and other risks

- Assess all information provided through a cross-functional team representing the data protection officer or data protection specialist, procurement, the unit requesting the service and the internal owner of the personal data of social protection beneficiaries and applicants, IT, the legal unit, and potentially the ethics officer
- Have in place a risk evaluation system
- Develop red lines

(iii) Award contract

The award contract should include:

- Controller's data protection and privacy terms and conditions, including:
  - strong audit rights (among other things: once a year, and at any time in the case of data breach; full access to systems and documentation on the premises for minimum five days)
  - information obligation regarding data breaches, investigations, audits by supervisory authorities, security updates
  - information obligation about any changes of the technology (ideally, no changes are technically possible without the prior approval of the controller)
- Controller's IT security requirements specific for the envisaged technology

(iv) Monitor compliance

- Regular audits
- Security tests

4.4.2. Data protection and privacy challenges of specific technologies

(i) Cloud-based management information systems (MIS)

Box 48 - Checklist of Good Practices: Cloud-based MIS

- ☐ The data controller should ensure that the use of cloud services complies with applicable data protection and privacy laws and regulations to which the data controller is subject and, also, with its internal policies.
- ☐ Conduct a specific risk assessment (a DPIA) prior to the use of cloud services or any international data sharing.
- ☐ Selection of a cloud service provider that complies with data protection and privacy standards and applicable legislation.
- ☐ Carefully review the contract with the cloud service provider before signature and ensure that it contains adequate data protection and privacy standards, accountability mechanisms, data security (technical, physical and organisational) measures, confidentiality clause, and mechanisms that facilitate the exercise of data subject rights.
- ☐ Ensure that the cloud service provider complies with international data sharing legal requirements.
- ☐ Conduct regular audits of the personal data processing performed by the cloud provider (or the sub-contractors) and cloud-based storage system security measures.

Creating a digital and integrated information system is a crucial step in developing a national social protection system.[176] In some cases, these MIS rely on cloud computing and cloud-based solutions.

There are many benefits of using these solutions, such as flexibility regarding the location and flow of data and access to extensive quantities of computing power in

[176] Barca and Chirchir 2019 (p.5).

the short term. Yet, cloud services may also bring additional challenges for data protection and privacy. Among them, the lack of transparency about the processing operation and the absence of control over the data.[177]

For social protection programmes, the most relevant risks are:

- the use of services from unprotected locations
- the interception of sensitive information
- weak authentication
- data can be stolen from the cloud service provider (e.g., by hackers)

Box 49 - Cloud storage

Cloud storage is a cloud computing model that stores data on remote servers accessed from the Internet (or "cloud"). It is done through a cloud computing provider who manages and operates data storage as a service.

Social protection programmes in low and middle-income countries often lack professional local hardware infrastructure and rely on cloud storage (usually in servers outside the country where the data was collected).

If this is the case, it is essential to ensure that the use of such storage services complies with national laws, including the data protection and privacy regime, as well as any data localisation laws, and careful consideration of security controls offered by using cloud technologies.

Before making decisions to rely on private cloud storage, the data controller would be expected to carry out a specific risk assessment. Furthermore, it would be responsible for selecting a cloud provider that complies with data protection and privacy principles and legislation and conducts regular audits and system security measures on cloud-based storage.

Before personal data are stored in a cloud, social protection programs should:[178]

- initiate a DPIA on the intended storage in the cloud, prior to the use of cloud services
- conduct due diligence on the cloud service provider to ensure that it takes data protection and privacy into serious consideration

[177] Kuner and Marelli 2017 (p. 162).

[178] Kuner and Marelli 2017 (p. 169-173).

- discuss data protection and privacy openly with the cloud service provider and evaluate whether it is capable of fulfilling its data protection obligations
- carefully review the contract with the cloud service provider before signature and ensure that it contains adequate data protection and privacy standards

The **data protection and privacy standards** apply to cloud services.[179] Following, relevant standards and issues will be discussed in greater detail:[180]

Accountability

- The data controller or, in other words, the cloud client (e.g., the social protection ministry) remains responsible for complying with legal obligations originating from applicable data protection and privacy laws.
- The cloud client is responsible for selecting a cloud provider that complies with data protection and privacy legislation.
- The association between the cloud client and cloud service provider is a data controller-data processor relationship.
- Exceptionally, the cloud provider can act as a data controller. In this case, it has complete (joint) responsibility for the data processing and is required to comply with all relevant legal obligations for data protection and privacy.

- The data controller and the data processor should remain liable to data subjects for any breaches of data protection that the cloud service provider commits. The contract between them should clearly demand the cloud provider to notify the cloud client in the event of any data breach which affects the cloud client's data.

Purpose specification principle

- The data controller (i.e., cloud client) remains responsible, in cloud computing environments, for determining the purpose(s) of the processing.

[179] See Section 3.1. - Data protection and privacy standards.
[180] Kuner and Marelli 2017 (p.165-182).

That needs to be done before any personal data collection and data subjects should be informed accordingly.

- The data controller should not further process personal data for purposes incompatible with the original ones. Consequently, that is also forbidden for the cloud provider and its sub-contractors.
- Hence, a cloud service provider cannot unilaterally decide to transfer personal data or its processing to unknown cloud data centres and is not allowed to use personal data for its own purposes (for example, researching for other purposes, profiling, marketing).
- The contract between cloud provider and data controller (e.g., social protection ministry) should incorporate organisational and technical measures to mitigate risks of further processing personal data. In addition, it should provide assurances for the logging and auditing of personal data processing performed by the cloud provider (or the sub-contractors).

Lawfulness, fairness and transparency principle

- The data controller (e.g., the social protection authority) is required to have a legal basis for processing personal data.[181] The law may provide for several legal bases. Still, it is necessary to have a distinct legal basis for processing in the cloud. Therefore, there should be a case-by-case evaluation of each legal ground in every particular situation. This assessment will allow deciding if the lawful basis can be applied to the cloud or not and whether it is a new legal basis or a cumulative one.
- Transparency means that the cloud client (i.e., data controller) must inform the data subjects, before processing personal data, that they will be stored with or processed by a cloud provider.
- The cloud provider and sub-contractors (if any) must be transparent in their communication with the cloud client by informing it about all relevant issues. Only then, the data controller can assess the lawfulness of the personal data processing.
- A data controller envisioning the engagement of a cloud provider should thoroughly review the provider's terms and conditions and evaluate them from a data protection and privacy perspective.

Commented [19]: An example from social protection would be good here. The ICRC offers a good example for the Humanitarian case

[181] See Section 3.2.3. - Lawfulness, fairness and transparency.

- Essential for transparency is the notification of the cloud client of all sub-contractors (not simply those with which it has a direct contract) concerned with providing a particular cloud service.
- The contract between the cloud client and the cloud provider should contain information on the location of the data centres and the identity and location of sub-contractors. In addition, any subsequent changes to the nature of the processing should be informed to the cloud client, including types of personal data processed and the extent, manner and purpose of personal data processing by the cloud provider.

Retention limitation principle

- The cloud client is responsible for ensuring that personal data are erased as soon as they are no longer necessary. Therefore, deletion of data is a crucial concern throughout a cloud computing contract and also upon its termination.
- If a sub-contractor is replaced or withdrawn, the cloud client might either request a certificate of destruction of personal data by the cloud provider or a certificate confirming that the data were transferred to a new cloud service provider.
- Upon erasure, it is vital to ensure that each occurrence is deleted in an irreversible way (i.e., previous versions, temporary files, and even file fragments should also be deleted).
- Personal data should be deleted securely. That means either the storage media are destroyed or demagnetised, or the stored data is deleted effectively using special software that follows a recognised specification.
- The cloud client should ensure that the contract with the cloud provider (and sub-contractors, if any) contains explicit provisions for personal data erasure.

Security principle

- Social protection data controllers should choose a cloud provider that can guarantee physical, technical and organisational data security measures governing the envisaged processing of personal data. In addition, a provider that ensures compliance with these measures. A signed contract must

govern the relationship between the data controller and the data processor. It should, minimally, contain the data security requirements.

- Only authorised persons should have access to the cloud client data. Thus, the contract should include a confidentiality clause binding the cloud provider and any of its employees who may access the data.
- In addition, the least privilege principle should also apply, meaning that roles with excessive privileges should be avoided (e.g., administrators should not be entitled to access the whole cloud).
- Data controllers should ensure that the cloud service provider grants timely and reliable access to personal data. Accordingly, it's necessary to verify that the cloud provider has adopted reasonable measures to deal with the risk of interruptions, e.g., redundant storage, backup internet network links, and adequate data backup mechanisms.
- Personal data should be protected against spying and violation during their transmission and, when possible, also when they are "still". In these cases, encryption is a standard solution applied. However, proper attention needs to be taken to determine the correct protocols for encryption implementation and the management of secret keys for the encryption itself.
- The physical location of data storage is vital information. It allows acknowledging the applicable legislation and country-specific threats, such as power and network outages, and actions by hostile groups and organisations. In addition, it is essential to understand the security of data centres premises.
- The cloud provider should present the outcomes of independent audits on data security or allow the cloud client to request an independent evaluation.

Data subject rights

- Data subjects also have the rights of access, rectification, erasure, and objection regarding their personal data processed in the cloud. Therefore, the social protection data controller should ensure that the cloud provider does not impose technical and organisational obstacles for the data subjects to exercise their rights, even when subcontractors further process data.
- In the contract between the cloud client and the cloud provider, the provider's obligation to support the client in facilitating the exercise of data subject rights should be noted.

International data sharing

- Cloud services frequently involve international data sharing of personal data since stakeholders may be located in different countries. Therefore, social protection data controllers should ensure that the use of cloud services complies with applicable data protection and privacy laws to which they are subject and, also, with their internal policies.
- The contract between cloud client and cloud service provider should show how the provider complies with international data sharing legal requirements.
- A DPIA should be conducted before any international data sharing. It increases the lawfulness of such personal data processing considering data protection and privacy requirements and standards.

(ii) Biometric identification systems

Box 50 - Checklist of Good Practices: Biometric identification systems

- ☐ Ensure that one or more of the following legal bases for personal data processing apply: vital interest of the data subject or the organisation, public interest, the performance of a contract, compliance with a legal obligation
- ☐ Make sure that free, informed and documented consent of the data subject(s) concerned is obtained
- ☐ Ensure the fair and lawful processing of personal data obtained by means of biometric technologies
- ☐ Set out specific purposes of the processing of biometric data and communicate them to individuals concerned
- ☐ Process only adequate and relevant data for collection, minimising storage time and the amount of data collected
- ☐ Avoid retention of data for further processing and develop your data retention policies
- ☐ Implement adequate and proportionate security measures given the sensitivity of biometric data

- ☐ Consider the rights of data subjects informing them about the involvement of third parties, possible implications of biometric data collection, setting up adequate infrastructure to grant the right to access, objection, deletion and rectification of data
- ☐ Before (international) sharing of biometric data, ensure that a legal basis under applicable law and internal policies is provided and a DPIA is conducted
- ☐ Conduct a DPIA to clarify processing details, highlight potential risks and mitigation measures and determine if biometric data should be collected

Biometric identification systems include various technologies using the 'measurement' of physical, psychological or behavioural characteristics (e.g., voice, face, iris) for individual authentication of identification. Biometric identification is increasingly present in individuals' lives. In developing countries, the most common technologies employing biometric data are national IDs and voter IDs, compared to developed countries, which use biometric data more for forensics and security. Developed countries typically do not use biometric technology in their national identity systems.[182]

No systematic information on the use of biometric technologies in social protection programmes is available. However, it is possible to say that non-contributory programmes in low- and middle-income countries have increasingly used biometric systems to identify beneficiaries and authenticate their identity upon delivery of payments or services.[183]

The employment of such biometric identification systems could have considerable benefits for social protection programmes such as accurate individual identification, effective means against fraud and corruption, the credibility of programmes and increased donor support, efficiency due to digital processing of data, increased physical protection of individuals and lowering the threshold of bank account acquisition.

These technologies, however, also pose significant risks and challenges. These include questions about the reliability and accuracy of the collected data, technical difficulties, ethical issues, the abuse of unchangeable information and pressure by other organisations or national authorities to use the data for other purposes. In

[182] Sepúlveda Carmona 2018 (p. 5).
[183] Sepúlveda Carmona 2018 (p. 5-6).

addition, these risks might include detrimental consequences for individuals, for instance, due to false matches, surveillance, or other abuse.[184]

Thus, due to the sensitivity of biometric data, the processing of this kind of data in social protection programmes presents various challenges for data protection and privacy and data subject rights.

Box 51 - What is meant when speaking about biometrics or biometric data?

Biometrics refers to the measurement of living things. In the case of humans, these techniques are used to identify individuals by including physical, psychological and behavioural characteristics. The individual's body and person produce these traits. These are considered personal information by law, and they can lead to the uncovering of additional information by analysing the collected data. Such additional information may include diseases, drug use, an individual's emotional state, or genetic inheritance.[185]

Biometrics include the following (non-exhaustive) list of technologies and data:

- Fingerprints: They have been used the longest among biometric technologies. Fingerprint images consist of the texture pattern of a finger, which has specific landmark points called minutiae. Fingerprint readers have a low cost and are thus widely used in civil and commercial applications.

- Iris: Images of the coloured ring surrounding the human eye pupil, the iris, are captured through infrared illumination and consist of a complex texture pattern. This pattern is highly individual and very difficult to manipulate or imitate surgically. As a result, many border crossing systems use that technology for personal identification. However, sensors are costly, and their usage is limited due to the lack of legacy iris databases.

- Face: Facial recognition is an established and successful manner of identification using biometric technologies. The technology is currently used, for instance, at airports accepting biometric passports for the authentication of travellers. New facial recognition technologies identify a person and are increasingly able to ascertain an individual's age, gender, and emotional state.[186]

- Voice: Voice and speech recognition systems identify individuals, including behavioural (including movement of lips, jaw, tongue, etc.) and physiological (including vocal tract, lips, mouth etc.) characteristics. The vocal behavioural traits of

[184] Kuner and Marelli 2017 (p. 129-130).
[185] Sepúlveda Carmona 2018 (p. 3-4).
[186] Tistarelli et al. 2012 (p. 229-231)

an individual may vary and change with age and state of health. Speech recognition is sensitive to background noise and playback spoofing.[187]

Traditional biometrics such as fingerprints, facial recognition and iris detection have higher discriminatory power and a lower privacy risk than behavioural biometrics such as motor skills (including voice, gait, dynamic face features, computer mouse movements or keystroke dynamics) or body signals (including heartbeat, EEG, ECG, transpiration, eye blinking, breathing frequency and trepidation).[188]

Just like the technological options, the purposes of biometric data are manifold, including public security, public health, research and private use. These purposes might be advantageous or disadvantageous for the individual data subject. For example, identity cards and passports increasingly rely on biometric data to provide authentication and reduce the chances of fraud and identity theft. Furthermore, legal proceedings increasingly employ biometric techniques, especially for filiation disputes in civil courts.[189]

Humanitarian organisations increasingly employ biometric identification to identify individuals more effectively, to prevent fraud and misuse of humanitarian aid. The advantage of using these technologies lies in identifying people who might not have the means to prove their identity otherwise. Furthermore, these data are more difficult to counterfeit, and they allow for additional processing operations. Additionally, they increase the efficiency of humanitarian aid management, as they can more easily be digitally stored and managed.[190] These, however, also pose significant risks, and great care needs to be taken when biometrics are employed in social protection programmes. The GDPR, for instance, considers biometric data as a special kind of data that is regulated more strictly.[191]

The **data protection and privacy standards** apply to biometric identification systems. Following, relevant standards and issues will be discussed in greater detail:[192]

[187] Jain and Kumar 2012 (p. 51-52).
[188] Schumacher 2012 (p. 2018-2019).
[189] National Consultative Ethics Committee for Health and Life Sciences 2007 (p. 7).
[190] Kuner and Marelli (p. 128).
[191] GDPR 2016/679 (Art. 9).
[192] Kuner and Marelli 2017 (p. 128-141).

`

Purpose specification principle

- The purpose of data processing needs to be specified by the data controller collecting personal information.
- The objectives need to be specific, legitimate and communicated to the data subjects when data are collected.
- The purposes of biometric data collection need to refer to the initial purposes of the data subject's identification.
- In some cases, data might further be processed for historical, statistical or scientific purposes. Then, the processing needs to be compatible with the initial purpose. For that purpose, the link between the initial and the further processing needs to be considered. Furthermore, the data collection situation, the relationship between data subjects and data controllers, the nature of the personal data collected, possible risks or consequences, the existence of safeguards and the reasonable expectations of the data subjects need to be considered.

Data minimisation

- Data collected and processed should be kept to a minimum and stored for a limited time, meaning they should be adequate and relevant for processing.
- Any excess information that is collected but not required should be deleted.
- Data sets should be limited to what is proportionate. If, for instance, photographs and fingerprints are used for identification purposes, the collection of facial imagery or iris scans might not be necessary.
- To ensure data minimisation, compartmentalisation of data collected might be advisable.

Lawfulness, fairness and transparency principle

- Biometric data should be considered personal data and applicable law should regulate it. Therefore, primary data protection and privacy principles need to be applied when biometric data is collected and processed.

- Data protection and privacy law should require lawful and fair processing of personal data. Therefore, a sufficient legal basis needs to be identified for biometric data processing to be conducted.
- During all processing stages, fairness needs to be upheld in the use of data and information provision.
- Several legal bases for the processing of biometric data are vital to consider the use of these technologies. These include the vital interest of the data subject or another person, public interest, consent, the legitimate interest of the organisation, contractual obligation or compliance with legal regulation.
- Consent is the preferred legal basis for personal data processing in general and biometric data processing in particular as these are considered sensitive data. Therefore, the data subjects' consent should be obtained if possible. Obtaining consent might not be possible due to the inability of the data subject to provide it, for instance, if a person is unconscious or not legally able to prove their identity. Time and personal resources might be scarce in emergencies impeding the possibility to obtain consent. Furthermore, data subjects might have difficulties giving informed consent due to the highly complex technical nature and possible unforeseen risks inherent in the technology. In some cases, no alternatives for participating in a programme might be provided. Thus, giving consent would not be a free choice.
- Public interest may provide a legal basis for biometric data processing if the organisation cannot obtain the data subject's consent. That includes, for instance, cases when the life, security, dignity, and integrity of the data subject are threatened.

Retention limitation principle

- A data retention policy could provide security for data subjects as it describes the conditions for deletion, de-identification or access restriction.
- The data retention policies need to be developed based on the types of data collected and how they might use them in the future.

Security principle

- The use of biometric data should be carefully considered. Creating databases that include biometric information should be avoided, whenever possible.[193]
- Some legal systems consider biometric data to be sensitive data that affect the requirements for lawful processing. These are required because biometric information is unique and cannot be modified, increasing the risk for identity theft. Furthermore, future technologies using the collected biometric data today might reveal more information about the individual concerned.
- Increased and adequate security measures need to be taken due to the sensitive nature of the data collected and processed with biometrics. These might include a retention limitation policy, or compartmentalisation, encryption.
- Centralised storage of personal biometric information should be avoided.
- Biometric data should be stored in encrypted form on a smart card or similar device and limited identification data related to the data subject should be stored on such devices. Therefore, if cards and/or devices are lost or mislaid, the risk that their biometric information may be misused is limited.[194]
- DPIAs should always be carried out before using biometric data to assess the risks and possible interferences with the data subject's fundamental rights, as well as mitigation measures.
- A DPIA needs to consider that different types of biometric data have varying degrees of sensitivity. That refers, for instance, to additional information that might be inferred from data collected through iris scans. Other data, like palm vein recognition, can only be read when the data subject is participating. Therefore, these data are less sensitive.

Data subject rights

- Data subject rights include the rights to information, access, correction, deletion and objection.
- As the data are usually collected directly from the individual, the right to information should be easy to follow. However, possible implications of

[193] Sepúlveda Carmona 2018 (p. 35).
[194] Sepúlveda Carmona 2018 (p. 35).

biometric data collection and the involvement and access by third parties for the implementation of the programme should be communicated. If the participation of third parties or the possible consequences changes during programme implementation, the data subject's consent needs to be collected again.

- To enable access, objection, deletion, and rectification, organisations need to install an adequate infrastructure. Furthermore, the infrastructure should include complaint procedures.

International data sharing

- Data sharing might include third parties, such as external data processors providing biometrics technology, data transfer to a third party, or authorities requesting data about their subjects.
- Particular caution and consideration of data protection and privacy requirements should be undertaken before sharing or granting access to biometrics data.
- In the case of international data sharing, the restrictions in place by data protection and privacy laws need to be respected, and legal bases need to be established before sharing.
- A DPIA concerning international data sharing might be beneficial to strengthen the legal bases necessary to enable international data sharing.

(iii) Automated decision making

Box 52 - Checklist of Good Practices: Automated decision-making

- ☐ Ensure a specific risk assessment (i.e., DPIA) is conducted before implementing automated decision-making processes, including those based on profiling.
- ☐ Automated decision-making (without human intervention) that can directly and negatively affect the interests, rights and freedoms of individuals should be strictly restricted. It should be applied only in exceptional cases, defined by the applicable data protection and privacy legislation, and always accompanied by the implementation of adequate safeguards to the data subject's rights, freedoms and legitimate interests.

- ☐ Where exemptions allow for solely automated decision making, data subjects should have at least the right to request (in a simple way) and obtain human intervention, to express his or her point of view, and to challenge the decision.
- ☐ Ensure that human intervention (oversight of the decision) is meaningful. It should be carried out before the decision applies and done by someone who has the authority and competence to change the decision.
- ☐ Carry out regular checks to make sure that social protection data controller systems are working as intended regarding the decision-making process.
- ☐ Explain to data subjects the use of automated decision-making processes, including profiling: what information is used, where it was obtained, for what purpose it is used and what the effects might be.
- ☐ Use anonymised data in profiling activities.
- ☐ Ensure, in the case of automated decision-making (including profiling), meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Automated data processing techniques, such as algorithms, do not only allow internet users to search and access information quickly, but they are also increasingly used in **decision-making processes** that were previously completely under the responsibility of human beings.[195] Algorithms may be used to prepare human decisions or to take them directly through automated means.[196]

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. 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** and **profiling** (which can be part of an automated decision-making process).[197]

Box 53 - Potential risks of automated decision-making and profiling

[195] MSI-NET 2018.

[196] For more information about algorithms, automated decision-making, including profiling, see 'Glossary of defined terms and abbreviations'.

[197] See Box No. 11 - What is automated decision-making and profiling?

Both automated decision-making and profiling can be useful in many sectors (e.g., education, financial services, marketing, etc.), leading to quicker and more efficient decisions, especially when dealing with a large amount of data.

However, if not accompanied by the appropriate risk assessment and safeguards, they can bring significant risks for individuals rights and freedoms.

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. Through profiling techniques, for instance, sensitive personal data (such as race, political opinions, religious or philosophical beliefs; biometric and health data, etc.) can be inferred from other non-sensitive data. This raises major issues around notions of consent, transparency and personal autonomy.[198]

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.

A well-known example is the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), a risk assessment system software used in the United States 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.[199]

Who is responsible when human rights are infringed based on algorithmically prepared decisions?

Data protection and privacy 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.

Which decisions should not be fully automated?

[198] MSI-NET 2018.

[199] Privacy International 2018.

One of the potential risks of using these processing techniques is that decisions may lead to significant adverse effects. In these cases, good international practices advise that automated decision-making, including profiling, should be strictly restricted. It may be applied only in exceptional cases defined by the applicable data protection and privacy legislation and always accompanied by adequate safeguards to the data subject's rights, freedoms and legitimate interests.

For instance, the decision if an individual is entitled to a social protection programme benefit is classified as one that may lead to significant adverse effects, affecting a person's livelihood or ability to survive. Therefore, a social protection programme should not automatically evaluate if an individual is entitled to a benefit and make this decision based solely on automated processing. In this case, some human control must be present (semi-automated process).

Therefore, 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 them, such as the automatic refusal of a social benefit.

One significant concern is the time it can take to challenge these decisions and the harm beneficiaries of social protection programmes can suffer in the interim.

To address that, it would be helpful to ensure that decisions to cut off benefits, or other decisions of similar severity, cannot be made solely through automated decision-making (i.e., human intervention is required before they are implemented).

Another option would be, in case a beneficiary challenges such automated decision, the benefits are reinstated while the challenge is pending. The latest, however, may produce harm until the beneficiary is able to challenge the decision. Moreover, compensation after the fact will be little comfort to someone who has lost their home, for instance, while working their way through the process.

Box 54 - The 'SyRI case'

The District Court of the Hague concluded on 5 February 2020 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.[200] The 'SyRI case' is a landmark ruling for benefit claimants around the world. Moreover, 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".[201] Indeed, in his report on digital welfare released at the end of last year, the UN Special Rapporteur on extreme poverty 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".[202]

Because this type of processing—via an automated decision technique—is considered to be high-risk, it is advisable to carry out a specific risk assessment to evaluate if any processing is likely to result in significant adverse effects to data subjects and define what safeguarding measures must be applied.

Therefore, before using processing techniques such as automated decision-making and profiling, social protection data controllers should assess if these techniques may have a **significant adverse effect** on individuals. If the answer is: [203]

No! Then good international practices recommend data controllers should:

- Continue to carry out profiling and automated decision-making
- Ensure compliance with data protection and privacy laws and regulations
- Identify and record the lawful basis for the processing
- Have processes in place so people can exercise their rights: to information (details of the information we used to create their profile); to object to profiling; to access and rectify, and, if applicable, erase personal data
- Have additional checks in place for profiling and automated decision-making systems to protect any vulnerable groups (including children)

[200] Privacy International 2020.
[201] Henley and Booth 2020.
[202] UNOHCHR 2019.
[203] ICOc, n.d.

`

- Ensure meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences of such processing for the data subject

In addition, it would be advisable to:

- Carry out a DPIA to consider and address the risks before to start any new automated decision-making or profiling.
- Tell data subjects about the profiling and automated decision-making carried out, what information is used to create the profiles and where this information was obtained.
- Use anonymised data in profiling activities.

Yes! Then good international practices recommend data controllers should:

- Carry out a DPIA to identify the risks to individuals, show how the data controller is going to deal with them and what measures it has in place to meet the applicable legislation requirements.
    - 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.
- Carry out the processing only under the legally permitted exceptional cases (e.g., for contractual purposes, presence of an individual's explicit consent, authorised or required by law).
- Not use sensitive personal data (special category of personal data) in automated decision-making systems unless there is a lawful basis to do so, and the controller can demonstrate what that basis is. Any special category data accidentally created should be deleted.
- Explain to data subjects the use of automated decision-making processes, including profiling: what information is used, why it is used and what the effects might be.
- Ensure meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences of such processing for the data subject.
- Set up a simple way for people to ask to reconsider an automated decision.

- Identify staff within the organisation who are authorised to carry out reviews and change decisions.
- Regularly check systems for accuracy and bias and feed any changes back into the design process.

In addition, it would be advisable to:

- Use visuals to explain what information is collected and used, and why this is relevant to the process.
- Signed up to a set of ethical principles to build trust with data subjects.
- Data subjects should have at least the right to request (in a simple way) and obtain human intervention, to express his or her point of view, and to challenge the decision.
    - To qualify as human intervention, the controller must ensure that any oversight of the decision is meaningful, meaning it should be active rather than just a token gesture. It should be carried out before the decision applies and done by someone who has the authority and competence to change the decision. [204]

Finally, social protection authorities (data controllers) should carry out regular checks to make sure that their systems are working as intended regarding the decision-making process.

[204] Article 29 Working Party 2018 (p. 21).

References

Alston, Philip. 2019. "Extreme poverty and human rights". United Nations General Assembly. Accessed September 16, 2021, https://undocs.org/pdf?symbol=en/A/74/493.

Alston, Philip. 2020. "The parlous state of poverty eradication." Report of the Special Rapporteur on extreme poverty and human rights. Accessed 16 September 2021. https://chrgj.org/wp-content/uploads/2020/07/Alston-Poverty-Report-FINAL.pdf.

Asia-Pacific Economic Cooperation, APEC. 2005. "Privacy Framework." Accessed 16 September 2021. https://www.apec.org/publications/2005/12/apec-privacy-framework.

Article 29 Working Party. 2018. "Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, WP251rev.01." European Commission, Brussels. https://ec.europa.eu/newsroom/article29/items/612053/en.

Barca, Valentina and Chirchir, Richard. 2019. "Building an Integrated and Digital Social Protection Information System." GIZ. Accessed September 9, 2021. Accessed 16 September 2021. https://www.giz.de/en/downloads/giz2019-en-integrated-digital-social-protection-information-system.pdf

Barca, Valentina and Chirchir, Richard. 2014. "Single registries and integrated MISs; De-mystifying data and information management concepts." Department of Foreign Affairs and Trade Australia. Accessed 5 September 2021. https://www.opml.co.uk/files/2018-05/barca-chirchir-2014-data-information-management-social-protection.pdf?noredirect=1.

Council of Europe, Convention 108+ Convention for the protection of individuals with regard to the processing of personal data. 2018. Accessed 5 September 2021. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf.

Economic Community of West African States. 2010. "Supplementary Act A/SA.1/01/10 on personal data protection within ECOWAS." Accessed 5 September 2021. https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf.

European Data Protection Supervisor. n.d. "Data Protection Officer (DPO)." Accessed September 19, 2021. https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en.

FRA. 2018. "Handbook on European data protection law." European Union Agency for Fundamental Rights. Accessed 6 August 2021. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition.

General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

GIZ. Deutsche Gesellschaft für Entwicklungszusammenarbeit. 2020. "Data Protection for Social Protection: Key Issues for Low- and Middle - Income countries." Accessed 5 March 2021. https://enabling-digital.eu/wp-content/uploads/2021/01/GIZ_Data_Protection_For_Social_Protection.pdf.

Global Partner Digital. 2018. "Travel Guide to the Digital World: Data protection for human rights defenders." Accessed 10 February 2021.https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf

Henley, John and Booth, Robert, "Welfare Surveillance System Violates Human Rights, Dutch Court Rules," *The Guardian*, February 5, 2020. Accessed February 20, 2021. https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules.

ICOa, Information Commissioner's Office. n.d. "Data Sharing Code of Practice." Draft Code for Consultation. Accessed September 16, 2021. https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf.

ICOb, Information Commissioner's Office. n.d. "Deleting Personal Data." Accessed 9 September 2021. https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf.

ICOc, Information Commissioner's Office. n.d. "Rights related to automated decision making including profiling." Accessed September 18, 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/.

ICOd, Information Commissioner's Office. n.d. Security." Accessed September 8, 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/.

ICOe, Information Commissioner's Office. n.d. "Sample DPIA template." Accessed September 9, 2021. https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf.

ILO. International Labour Organisation. 2018. "Introduction: Social transfers." Accessed 23 September 2021. https://www.social-protection.org/gimi/gess/ShowTheme.action?id=11.

iDenfy. 2020. "Identification vs. Authentication vs. Verification: What are the differences?" Accessed September 9, 2021. https://www.idenfy.com/blog/identification-verification-authentication/.

Ioannidis, Dimosthenis; Tzovaras, Dimitrios; Dalle Mura, Gabriele; Ferro, Marcello; Valenza, Gaetano; Tognetti, Alessandro and Pioggia, Giovanni. "Gait and Anthropomorphic Profile Biometrics: A Step Forward." In *Second Generation Biometrics: The Ethical, Legal and Social Context*, edited by Emilio Mordini and Dimitrios Tzovaras, 105-129. Dordrecht: Springer, 2012.

ISPA Inter Agency Social Protection Assessments Partnership. 2016. "CODI. Core Diagnostic Instrument. 'What Matters' Guidance Note.", Accessed 5 April 2021. https://ispatools.org/tools/CODI-English.pdf.

Jain, Anil K. and Kumar, Ajay. "Biometric Recognition: An Overview." In *Second Generation Biometrics: The Ethical, Legal and Social Context*, edited by Emilio Mordini and Dimitrios Tzovaras, 49-81. Dordrecht: Springer, 2012.

Kuner, Christopher and Marelli, Massimo, Handbook on Data Protection in Humanitarian Action, International Committee of the Red Cross (ICRC), Geneva, 2017.

Leite, Phillippe; Karippacheril, Tina G.; Sun, Changqing; Jones, Theresa and Lindert, Kathy. 2017. "Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment Tool." Accessed 23 September 2021. https://openknowledge.worldbank.org/handle/10986/28284.

Lindert, Kathy; Karippacheril, Tina George; Rodriguez Caillava, Inés; Nishikawa Chavez, Kenichi. Sourcebook on the Foundations of Social Protection Delivery

Systems. Washington, DC: World Bank, 2020. Accessed September 15, 2021. https://openknowledge.worldbank.org/handle/10986/34044.

Manavis, Sarah, 'GDPR has made it easier to access our own data – and for hackers to do so too,' The New Statesman, 6 September 2019, available at: https://www.newstatesman.com/science-tech/2019/09/gdpr-easier-access-data-hackers-access-online-security-spotify [accessed on 9 September 2021].

Member States of the African Union. 2014. Malabo Convention on Cyber Security and Personal Data Protection. Accessed 23 September 2021. https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf.

MSI-NET. 2018. "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.

National Consultative Ethics Committee for Health and Life Sciences. 2007. "Opinion N° 98. Biometrics, identifying data and human rights." Accessed 19 September 2021. https://www.ccne-ethique.fr/en/publications/biometrics-identifying-data-and-human-rights#.VenJ87TDU5E.

NCSL, National Conference of State Legislatures. 2021. "Differential Privacy for Census Data Explained". Accessed 9 September 2021. https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx.

OECD. 2013. "The OECD Privacy Framework." Accessed 9 September 2021. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Privacy International. 2018. "The Keys to Data Protection: A Guide for Policy Engagement on Data Protection." Accessed 9 September 2021. https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf.

Privacy International. 2019. "Privacy, a precondition for social protection." Accessed 9 September 2021. https://privacyinternational.org/news-analysis/3029/privacy-precondition-social-protection.

Privacy International. 2020. "The SyRI Case: A Landmark Ruling for Benefits Claimants Around the World." Accessed 9 September 2021. https://www.privacyinternational.org/news-analysis/3363/syri-cas [accessed on 9 September 2021].

Sepúlveda Carmona, Magdalena. 2018. "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 Organisation, Geneva. Accessed 9 September 2021. https://www.social-protection.org/gimi/RessourcePDF.action?ressource.ressourceId=55133.

SPIAC-Ba. Social Protection Inter-agency Cooperation Board. n.d. "What is the social protection inter-agency cooperation board?" Accessed 08 September 2021. https://www.ilo.org/global/docs/WCMS_301456/lang--en/index.htm.

SPIAC-Bb. Social Protection Inter-agency Cooperation Board. n.d. "SOCIAL PROTECTION TO PROMOTE GENDER EQUALITY AND WOMEN'S AND GIRLS' EMPOWERMENT." Accessed 23 September 2021. https://www.ilo.org/wcmsp5/groups/public/@dgreports/@nylo/documents/genericdocument/wcms_674612.pdf.

Tistarelli, Massimo; Barrett, Susan E. and O'Toole, Alice J. "Facial Recognition, Facial Expression and Intention Detection." In *Second Generation Biometrics: The Ethical, Legal and Social Context*, edited by Emilio Mordini and Dimitrios Tzovaras, 229-257. Dordrecht: Springer, 2012.

United Nations, UN General Assembly. 1993. "Vienna Declaration and Programme of Action, 12 July 1993, A/CONF.157/23." Accessed 14 April 2021. https://www.refworld.org/docid/3ae6b39ec.html.

United Nations, UN General Assembly. 2018. "Resolution adopted by the General Assembly on 17 December 2018, 73/179. The right to privacy in the digital age." Accessed 8 September 2021. https://undocs.org/pdf?symbol=en/A/RES/73/179.

United Nations, UN General Assembly. 2019. "Resolution adopted by the General Assembly on 26 September 2019, 52/15, The right to privacy in the digital age." Accessed 8 September 2021.https://digitallibrary.un.org/record/3837297?ln=en.

United Nations, UN General Assembly. 2020. "Resolution adopted by the General Assembly on 16 December 2020, 75/176. The right to privacy in the digital age." Accessed 8 September 2021. https://digitallibrary.un.org/record/3896430?ln=en.

`

United Nations. n.d. "Universal Declaration of Human Rights" Accessed 05 September 2021. https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf.

United Nations. 2018. "Personal Data Protection and Privacy Principles." Accessed 23 September 2021. https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf.

UNOHCHR. United Nations Office of the High Commissioner for Human Rights. 2019. "World Stumbling Zombie-Like into a Digital Welfare Dystopia, Warns UN Human Rights Expert." Accessed 5 September 2021. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156.

WFP. World Food Programme. 2017. "Two Minutes on Social Protection." Accessed 23 August 2021. https://documents.wfp.org/stellent/groups/public/documents/communications/wfp277442.pdf?_ga=2.82500497.681773780.1592505793-2117718756.1590495840.

World Bank. 2012. "Resilience, Equity, and Opportunity. The World Bank's Social Protection and Labor Strategy 2012-2022." Accessed 23 September 2021. https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/443791468157506768/resilience-equity-and-opportunity-the-world-banks-social-protection-and-labor-strategy-2012-2022.