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

On behalf of

Federal Ministry for Economic Cooperation and Development

SPIAC-B



BEN WAGNER, CAROLINA FERRO
AND JACQUELINE STEIN-KAEMPFE

AUGUST 2022

ACKNOWLEDGEMENTS

This Implementation Guide was commissioned by GIZ's Sector Initiative Social Protection and drafted by Carolina Ferro and Ben Wagner (from Enabling-Digital.eu) and Jacqueline Stein-Kaempfe (from the World Food Programme, WFP). It is the result of a collective process that took place from 2020 to 2022. It benefited immensely from reviews and inputs by experts from the Social Protection Inter-Agency Cooperation Board (SPIAC-B) as part of a dedicated working group on Digital Social Protection based in organisations such as the International Labour Organization (ILO), Information Systems Security Association (ISSA), World Bank, European Commission Directorate-General for International Partnerships (DG INTPA), WFP, Australian Department of Foreign Affairs and Trade (DFAT), Asian Development Bank (ADB), Digital Impact Alliance (DIAL), DAI, GIZ and others. The authors wish to thank the GIZ team, especially Dominique Leska and Ralf Radermacher, without whom this document would not have been possible. A sincere thanks is due to Valentina Barca for her comments and suggestions on a previous version of this document, which helped us to improve it. We would also like to express our gratitude to all of the experts who discussed, commented and gave feedback during the process of elaboration and co-creation of this document, including: Saurav Bhattarai, Kelvin Hui, Christian Merz, Anita Mittal, Tatjana Schock and Uwe Wahser (GIZ), Rodrigo Ortiz D'avila Assumpcao and Veronika Wodsak (ILO), Michela Bonsignorio, Andres Chamba and Nichola Peach (WFP), Tina George, Conrad Daly and Phillippe Leite (World Bank), Juergen Hohmann and Dirk Homann (DG INTPA), Raul Ruggia-Frick (ISSA), Amir H. Jilani, Anand Ramesh Kumar and Wendy Walker (ADB), Abigail Bakker, Lisa Hannigan and Fazley Mahmud (DFAT), Sherman Kong and Laura McDonald (DIAL), Chloe Messenger, Rachael Steller and Ric Goodman (DAI). Finally, we would like to acknowledge the valuable contribution of Rita Gsenger from Enabling-Digital.eu in editing and improving the document.

JOINT STATEMENT OF THE SPIAC-B WORKING GROUP ON DIGITAL SOCIAL PROTECTION

We – the subscribing United Nations system organisations and bilateral development agencies, donor governments, and civil society organisations gathered under 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 ensure 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, to the extent that a country provides for good governance in public administration, 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 data protection and privacy principles into their governance framework and towards 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. This document 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 facing country-specific challenges to comply with national and international data protection and privacy standards.

While creating this Implementation Guide, we also endeavoured to agree on a common SPIAC-B language and approach to be used when communicating with partner governments to ensure that data protection and privacy unite the international development community and form the basis of our cooperation.

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 programme objectives. Therefore, we call on partner governments to establish comprehensive national legal frameworks for data protection and privacy and on social protection authorities to develop organisational data protection policies and guidelines that ensure the application of these regimes, establishing mechanisms that enable transparency and accountability and allow for 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 the participation of individuals in social protection systems are essential pathways to developing a rights-based approach and rigorous respect for personal data and privacy.

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 Social Protection Inter-agency Cooperation Board (SPIAC-B), 'What is the Social Protection Inter-Agency Cooperation Board?', [online], n.d.(a), https://www.ilo.org/global/docs/WCMS_301456/lang--en/index.htm.

CONTENTS

CONTENTS

CONTENTS

LIST OF FIGURES AND TABLES

LIST OF BOXES

DEFINITIONS AND EXPLANATIONS

CONTENTS

IMPLEMENTATION TOOLS

CHECKLIST OF GOOD PRACTICES

EXAMPLES

GLOSSARY OF DEFINED TERMS

AGGREGATED DATA – The term aggregated 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 and administrators.[2] Aggregate data does not contain personal data.

AI – Artificial intelligence is defined as the study of intelligent and rational agents that receive percepts from the environment and perform actions. 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 decisions.[3]

ALGORITHM – An algorithm refers to a clear set of finite instructions to solve a problem or a class of problems.[4]

ANONYMISATION – Anonymisation encompasses techniques that can be used to ensure that datasets containing personal data are fully and irreversibly anonymised so that they do not relate to an identified or identifiable natural person, or that the data subject is not, or is no longer, identifiable.[5] Anonymised data are datasets that do not allow for the identification of individuals or do not relate to an identifiable natural person.[6] Anonymised data is not considered personal data. Data protection and privacy frameworks do not apply to anonymised data or other aggregate or statistical data that do not relate to individual persons. This Implementation Guide, however, applies to non-personal data if it is assessed as sensitive (see below).

AUTOMATED DECISION-MAKING – Also called algorithmic decision-making, automated decision-making systems are automated or semi-automated systems using factual or inferred 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.[7]

BIG DATA OR DATA ANALYTICS – Big data describes very large datasets containing information from various sources and characterised by a large velocity. These provide greater statistical power and require innovative forms of data analysis. Data analytics refers to the analysis of such large datasets, usually in the context of predictive analytics or the analysis of user behaviour.[8]

BIOMETRIC DATA – Biometrics refers to unique human characteristics, such as individual biological traits (like the iris or fingerprint) or behavioural characteristics (like gait). An individual's biometric data is unique and cannot be changed. Hence, they are used as identifiers for passports and identity cards, among other things, and have specific implications for personal data protection and privacy.[9]

CONSENT – Consent of the data subject is a legal basis for personal data processing. According to various data protection regulations and frameworks, such as the General Data Protection Regulation (GDPR) of the European Union and the Council of Europe (CoE) Convention 108+, consent must be informed and given freely, voluntarily, and unambiguously by data subjects for personal data processing to take place legally.[10]

DATA CONTROLLER – A data controller is a natural person or legal entity (e.g. the government, United Nations agency, development organisation, private company), be it public or private, who alone or jointly with others determines the purpose and means of processing personal data. The controller is usually the main person or entity responsible to data subjects

2 Black, John; Hashimzade, Nigar and Myles, Gareth, Oxford Dictionary of Economics, Oxford University Press, Oxford, 2017, p. 479

3 Russell, Stuart and Norvig, Peter, Artificial Intelligence. A Modern Approach, Fourth Edition, Pearson, Hoboken, NJ, 2021

4 Castelluccia, Claude and Le Métayer, Daniel, Understanding Algorithmic Decision-Making: Opportunities and Challenges, European Parliamentary Research Service, Scientific Foresight Union, Brussels, 2019, p. 3

5 Kuner, Christopher and Marelli, Massimo, Handbook on Data Protection in Humanitarian Action, International Committee of the Red Cross (ICRC), Geneva, 2017, p. 8

6 University College London (UCL), 'Anonymisation and Pseudonymisation', [online], n.d., https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and; Kuner and Marelli, 2017, p. 12

7 Castelluccia and Le Métayer, 2019

8 Information Commissioner's Office (ICO), Big Data, Artificial Intelligence, Machine Learning and Data Protection, United Kingdom, n.d.(a), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

9 GDPR 2016/679, Art. 4 (14) (see European Parliament and Council of European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L119/1, 4 May 2016, pp. 1–88); and CoE Convention 108+, 2018, Art. 6 (58) (see Council of Europe, Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Council of Europe, 2018, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf)

10 GDPR 2016/679, 2016, Art 7; CoE Convention 108+, 2018, Art. 5 (42); ECOWAS, 2010, Art. 1 (see Economic Community of West African States [ECOWAS], Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Abuja, 2010, https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf)

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.[11]

DATA PROCESSING – Data processing is 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 of data.[12]

DATA PROCESSOR – A data processor is any natural person or legal entity who processes personal data on behalf of the 'data controller'.[13] This concept is not reflected in all international data protection and privacy frameworks. The data processor does not take any decisions with respect to data processing, but mainly implements the instructions of the controller. Implementing partners, financial or technological service providers and international organisations (IO) can be data processors for a government implementing a social protection programme. The data 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.[14]

DATA SUBJECT – A data subject is any individual whose personal data is being processed. In social protection programmes, data subjects include those participating in programmes as applicants/registrants and recipients/beneficiaries.[15]

DPA – A 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 charged with the application of the law through the issuing of regulations, offering of guidance, and cooperation with other authorities, public and private, when the processing of personal data might be involved.[16]

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 the mitigation and avoidance of data protection and privacy risks.[17] The DPIA should be active for the duration of the programme or initiative and monitor the rise of new threats and the changes throughout the process.[18]

DPO – A data protection office or officer is a designated individual or team working independently and advising an organisation or body on how data protection regulations are upheld and the rights of data subjects respected.[19]

INTEGRATED BENEFICIARY REGISTRY – Integrated beneficiary registries integrate the data analytics function across several programmes and their management information systems (MISs), linking information on beneficiaries into a data warehouse. They provide a consolidated overview of 'who receives what' benefits to support coordination, planning and integrated monitoring. As an example, they can serve as powerful tools to monitor and coordinate the 'supply' of social programmes, assessing overlaps, gaps and duplications across multiple programmes, while also supporting the consolidation of other functions along the delivery chain, acting as a nexus of information, and providing interlinkages between individual programme MISs and other external databases such as income tax, civil registration and, if applicable, disability databases (as well as to the social registry, if it exists).[20] Integrated beneficiary registries are one component of a SPIS (see below).

11 GDPR 2016/679, Art. 4(7); ECOWAS, 2010, Art. 1; CoE Convention 108+, 2018, Art. 2 (22)

12 ECOWAS, 2010, Art. 1; CoE Convention 108+, 2018, Art. 2 (21)

13 GDPR 2016/679, Art. 4(8); ECOWAS, 2010, Art. 1; CoE Convention 108+, 2018, Art. 2 (24)

14 GDPR 2016/679, Art. 28

15 GDPR 2016/679, Art. 4 (1)

16 GDPR 2016/679, Rec. 117–122; ECOWAS, 2010, Art. 12; Article 29 Working Party, 2017, pp. 3–6, (see European Commission, Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority, 16/EN WP 244 rev.01, Article 29 Working Party, 2017, pp. 3–6, https://ec.europa.eu/newsroom/article29/items/611235)

17 GDPR 2016/679, Art. 35, (1–3)

18 Kuner and Marelli, 2017, pp. 84–89

19 Kuner and Marelli, 2017, p. 89; GDPR 2016/679, Art. 37; CoE Convention 108+, 2018, Art 10 (87)

20 Chirchir Richard and Farooq, Shez, 'Single Registries and Social Registries: Clarifying the Terminological Confusion', Pathways' Perspectives on Social Policy in International Development, Issue No 23, 2016; Barca, Valentina and Chirchir, Richard, Building an Integrated and Digital Social Protection Information System, GIZ, 2019; Leite, Phillippe; Karippacheril, Tina G.; Sun, Changqing; Jones, Theresa and Lindert, Kathy, Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment Tool, Discussion Paper 1704, World Bank, Washington, DC, 2017

IO – An international organisation is an organisation (and its subordinate bodies) that is governed by public international law, or any other body that is set up by, or on the basis of, an agreement between two or more states (e.g. United Nations, World Bank). Development and humanitarian agencies can be, but are not necessarily, IOs – some are non-governmental organisations (NGOs), which are governed by the national laws of the jurisdiction in which they operate (for the difference between IOs and NGOs see Box 4).[21]

IT – Information technology is the use of computers to create, process, store, and exchange all kinds of electronic data and information.[22]

MIS – A management information system is a software application that supports the implementation of individual social protection programmes along each of the phases of the delivery chain. An MIS is sometimes referred to as a 'beneficiary database' or 'beneficiary operations management system'.[23]

PERSONAL DATA – Personal data refers to any information or set(s) of information that can, either by itself or together with other relevant data, 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. Personal data can be held in both electronic and physical form.[24]

PMT – Proxy means testing is usually understood as using observable characteristics of a household or its members to estimate their income or consumption, when other income data (salary slips, tax returns) are unavailable or unreliable. In practice, most PMT models use more than a dozen different variables to estimate the income of a household.[25]

PROFILING – Any form of automated processing of personal data using information relating to a natural person to evaluate and predict their behaviour and personal aspects (e.g. performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements).[26]

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 is still considered personal data.[27]

SENSITIVE PERSONAL DATA – Some data protection and privacy frameworks include the additional category of sensitive data (also called special category of personal data) as a sub-category of personal data. Sensitive personal data includes information concerning race, ethnicity, health data, sexual orientation, political opinions, religious or philosophical beliefs, membership of associations or trade unions, religious affiliation, genetic data, and biometric data (when processed solely to identify a natural person).[28]

SINGLE REGISTRY – This term is used differently by different agencies, actors and countries, so should be analysed according to the function performed. It is often[29] used as a synonym for integrated beneficiary registry (see above).

SOCIAL REGISTRY – Sometimes known as 'targeting databases', these are information systems that support the processes of outreach, intake and registration, and the assessment of needs and conditions, to determine potential eligibility for social programmes (serving one or more programme in a country). They collect and maintain socio-economic data on all registered individuals and households, regardless of whether they eventually benefit from a social programme or not. Contrary to an MIS, social registries are identity databases, but are not applications that can be used to manage social protection programmes. As such, individuals and households within social registries are not defined as 'beneficiaries', but as 'registered households'. Social registries can serve as tools for assessing the 'demand' for social programmes by profiling the specific needs and conditions of various population groups. In terms of their set-up, social registries vary significantly across countries (e.g. in terms of coverage, variables

21 Amici, Marco and Cepiku, Denita, 'Roles, Types, and Definitions of International Organizations', In: Marco Amici and Denita Cepiku (eds), Performance Management in International Organizations, Springer, Dordrecht, 2020, p. 7

22 Rennie, Richard and Law, Jonathan, A Dictionary of Physics, Oxford University Press, Oxford, 2019, p. 564

23 Barca and Chirchir, 2019, p. 12

24 GDPR 2016/679, Art. 4 (1)

25 World Bank Group, PMT-bases Social Registries. Measuring Income and Poverty using Proxy Means Tests, Social Protection & Labor team, Dhaka, Bangladesh, n.d.

26 GDPR 2016/679, Art. 4 (4), Rec. 71

27 Kuner and Marelli, 2017, p. 14

28 GDPR 2016/679, Art. 9 (1)

29 Chirchir and Farooq, 2016, p. 1

collected, institutional housing, approach to data sharing, etc.), affecting their potential uses.[30] Social registries are one component of an SPIS (see below).

SPIS – The term social protection information systems refers to the overarching system that enables the flow and management of information within the social protection sector and beyond, to other sectors (e.g. education, health or agriculture) and is a combination of the functions of a programme MIS, an integrated beneficiary registry and a social registry (see each above). An SPIS, thus, includes three pillars: support of programme-specific operations and functions, support of integrated operations and functions across the social protection sector, and nexus with a broader set of registries and information systems.[31]

ZNP – A zero-knowledge proof is a mathematical method used for verification without sharing or revealing underlying data. ZNPs enable one party to prove to another party that they know a value 'x', without conveying any information apart from the fact that they know the value. For instance, organisation 'A' could state they have beneficiary 'A' in their system, without sharing the details of that beneficiary with organisation 'B'.[32]

30 Leite et al., 2017, pp. 5–6; Barca, Valentina, Integrating Data and Information Management for Social Protection Social Registries and Integrated Beneficiary Registries, Commonwealth of Australia, Department of Foreign Affairs and Trade, Canberra, 2017, https://www.dfat.gov.au/sites/default/files/integrating-data-information-management-social-protection-full.pdf; Barca and Chirchir, 2019

31 Barca and Chirchir, 2019, p.11; Barca, Valentina, Social Protection Information Systems-ISPA Tool (forthcoming)

32 Social Protection Approaches to COVID-19: Expert Advice Helpline (SPACE), Linking Humanitarian & Social Protection Information Systems in the COVID-19 Response and Beyond, August 2020, p.10

ACRONYMS

ADB	Asian Development Bank
AI	artificial intelligence
API	application programming interface
AU	African Union
CFM	complaint and feedback mechanism (also called community feedback mechanism or grievance mechanism)
COE	Council of Europe
COMPAS	Correctional Offender Management Profiling for Alternative Sanctions
DFAT	Department of Foreign Affairs and Trade – Australia
DG INTPA	Directorate-General for International Partnerships (formerly Directorate-General for Cooperation and Development) – European Commission
DIAL	Digital Impact Alliance
DPA	data protection authority
DPIA	data protection impact assessment
DPO	data protection office/officer
ECOWAS	Economic Community of West African States
EU	European Union
GDPR	General Data Protection Regulation
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit GmbH
ICT	information and communications technology
ID	identity document
ILO	International Labour Organization
IO	international organisation
ISPA	Interagency Social Protection Assessment
ISSA	Information Systems Security Association
IT	information technology
MIS	management information system
MSI-NET	Committee of Experts on Internet Intermediaries
NGO	non-governmental organisation
OECD	Organisation for Economic Co-operation and Development
PMT	proxy means testing
SPIAC-B	Social Protection Inter-Agency Cooperation Board
SPIS	social protection information system
SYRI	system risk indication
UN	United Nations
WFP	World Food Programme
ZNP	zero-knowledge proof

ABOUT THIS GUIDE

Why an Implementation Guide on 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. As a result, they need special attention and support. In response, 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 the GIZ Sector Initiative on Social Protection, in partnership with the International Labour Organization (ILO), Information Systems Security Association (ISSA), World Bank, European Commission Directorate-General for International Partnerships (DG INTPA), World Food Programme (WFP), Australian Department of Foreign Affairs and Trade (DFAT), Asian Development Bank (ADB), Digital Impact Alliance (DIAL), and others.

The working group has developed this Implementation Guide to encourage and support partner governments in their efforts to ensure data protection and privacy in social protection systems. It is a practical and sector-specific guide, specially adapted to the context of social protection systems in low- and middle-income countries. It aims to offer guidance, increase awareness, and support people on the ground in the decisions made during the design of delivery structures for national 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.

This Guide is not a fixed, end-state manifesto, but attempts to provide guidance in such a way that each social protection system or programme can adapt the principles and practices contained within to its specific context. It builds on existing regional and international data protection and privacy regulations, conventions, guidelines, and other frameworks. It is based on, and further develops, the SPIAC-B working group on Digital Social Protection discussion initiated in the issue paper *Data Protection for Social Protection: Key Issues for Low- and Middle-Income Countries.*[33]

33 Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), Data Protection for Social Protection: Key Issues for Low- and Middle-Income countries, GIZ, 2020

Who is this guide for?

This Implementation Guide 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 (also referred to as 'social assistance'). 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 the 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 recipients/beneficiaries[34] – in other words, 'data subjects'.[35]

Why is this guide important for your work?

If you don't understand why the protection and privacy of personal data is important for your work, or you have a general idea, but don't know where to start, this guide is for you. In Part 1, this guide explains what is currently understood by personal data protection and privacy (Chapter 1) and also explores why the protection of personal data is necessary for any social protection programme (Chapter 2). Part 2 sets out the good international practices that could serve as a reference and inspiration for national data protection laws and as a framework for social protection programmes (Chapters 3–8). Finally, Part 3 provides step-by-step guidance and practical measures for implementing data protection and privacy principles in social protection programmes and for respecting individuals' rights to data protection (Chapter 9–12).

34 These two words are often used interchangeably, but sometimes indicate a slight variation in meaning: e.g. applicants are those who actively apply while registrants are more passively registered.

35 See 'Glossary of defined terms'.

PART 1

INTRODUCTION

CHAPTER 1

PERSONAL DATA PROTECTION AND PRIVACY

CHAPTER 1. PERSONAL DATA PROTECTION AND PRIVACY

1.1 WHAT IS PERSONAL DATA PROTECTION AND PRIVACY?

The privacy of an individual's **personal data** is an essential element of the right to privacy. This element may be referred to as **data privacy** and is increasingly relevant to people's lives. With the invention of computers, our personal information started being processed through digital means, moving in seconds through systems around the world, making it even more challenging to protect than our homes or our letter correspondence.[36] In this context, the concept of **personal data protection** has gained importance in relation to 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 a personal nature (such as their body, family, home, correspondence, property, thoughts, feelings, personal information) or unlawful attacks on their honour and reputation. This right is enshrined in most international and regional human rights treaties and conventions, widely ratified by nation states, and enshrined in national constitutions.

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. Through the following instruments, states are called upon to respect such rights and create laws that 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

Full enjoyment of the right to (data) privacy requires that personal data is actively protected, and its processing regulated. Therefore, data protection and privacy frameworks set up obligations for those who control or process data to take measures to protect personal data and to mitigate interference with the right to privacy. In addition, these frameworks hold data controllers and processors to account when they fail to comply with these obligations. Through specific data-related rights granted to data subjects (so-called data subject rights),[37] 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 interference with the right to privacy needs to be based on law and cannot be done without laws guaranteeing that such interference is legitimate and proportional.

36 The right to privacy in the digital age: Resolution 73/179 adopted by the General Assembly on 17 December 2018 (https://digitallibrary.un.org/record/1661346?ln=en), Resolution 42/15 adopted by the Human Rights Council on 26 September 2019 (https://digitallibrary.un.org/record/3837297?ln=en), and Resolution 75/176 adopted by the General Assembly on 16 December 2020 (https://digitallibrary.un.org/record/3896430?ln=en).

37 See Chapter 5 – Data subject rights.

In sum, while 'privacy' is broad and covers many areas of private life beyond personal data, 'personal data protection and privacy' covers the right to be free from unlawful interference with one's own personal data. 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 granting individuals rights 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 to refer to the appropriate and permissioned use, governance, and protection of personal data. 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 interchangeably and other times as different concepts.

The term **'data protection and privacy frameworks'** is used in this Implementation Guide to refer to the set of standards (whether incorporated in laws, treaties, or non-binding principles or guidelines) that 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 in this Implementation Guide.[38]

38 See Chapter 3 – Introduction: Data protection and privacy standards.

1.2 INTERNATIONAL AND REGIONAL DATA PROTECTION AND PRIVACY INSTRUMENTS

The need for data protection and privacy laws was first recognised in the 1960s by a number of countries, mostly in Europe. The transborder flow of data soon required the harmonisation of these 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.

However, **there are no universally recognised data protection and privacy standards.** What is available on an international level are international treaties between states such as the Council of Europe (CoE) Convention 108+,[39] Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection,[40] and the African Union (AU) Malabo Convention.[41] In addition, there are guidelines or principles issued by international organisations (IOs), like the United Nations (UN) and the Organisation for Economic Co-operation and Development (OECD), and finally regional bodies that have agreed upon frameworks, guidelines, or principles. For example, in 2016, the European Union (EU) issued the European General Data Protection Regulation,[42] which has direct legal effect in all EU member states, like a national law.

39 CoE, Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018

40 ECOWAS, Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 2010

41 AU, Convention on Cyber Security and Personal Data Protection, Malabo Convention, African Union, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

42 European Parliament and Council of European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), 2016

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

Data protection guidelines and principles by IOs (non-binding)

- OECD, *The OECD Privacy Framework, Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*, 1980, as amended in 2013
- UN General Assembly, *Guidelines for the Regulation of Computerised Personal Data Files*, 1990 – addresses UN member states and governmental IOs
- UN, *Personal Data Protection and Privacy Principles*, 2018 – issued by the High-Level Management Committee of the United Nations, addresses only UN organisations

International and regional data protection treaties between states (binding)

- CoE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108)*, 1981, as amended in 2018 (Convention 108+)
- ECOWAS, *Supplementary Act on Personal Data Protection within ECOWAS*, 2010
- AU, *Convention on Cyber Security and Personal Data Protection* (Malabo Convention), 2014 – not yet in force, as only 8 out of the minimum 15 states have ratified it

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

CHAPTER 2

WHY IS PERSONAL DATA PROTECTION CRITICAL FOR SOCIAL PROTECTION PROGRAMMES?

CHAPTER 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. The Social Protection Inter-Agency Cooperation Board (SPIAC-B) defines social protection as:

> *[…] 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.*[43]

Social protection is a human right[44] and can support individuals and societies with risk management, while improving resilience, equity and opportunity.[45] There are a wide range of social protection interventions, layered and sequenced in different ways in different countries. Examples include categorical programmes for children (e.g. child allowances) and old age (e.g. social pensions), conditional and unconditional cash transfers, unemployment and disability assistance and insurance, active labour market programmes, employment services, training services, social services and social work services.[46] Depending on the programme, different population groups are targeted: children, the elderly, low-income families, the unemployed, persons with disabilities, or individuals facing social risks such as youth.[47]

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 in society. In **contributory schemes**, the beneficiaries need to contribute, which, thus, determines their entitlement to benefits. For instance, social insurance schemes grant health care and social services, including cash benefits in 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 revenue often finance these schemes.[48]

In **low- and middle-income countries,** social protection programmes usually target vulnerable populations via non-contributory 'social assistance'.[49] Accordingly, this Implementation Guide seeks to support social protection practitioners in low- and middle-income countries working principally (but not exclusively) via non-contributory schemes, while facing country-specific challenges in complying with regional and international data protection and privacy standards and, as applicable, national legal frameworks.

2.2 INFORMATION MANAGEMENT IN SOCIAL PROTECTION PROGRAMMES

Social protection programmes are complex and context specific. However, all non-contributory social assistance programmes go through similar implementation phases along the delivery chain (see Figure 1) – and these phases are not hugely different for other forms of social protection.

43 Social Protection Inter-agency Cooperation Board (SPIAC-B), 'Social Protection to Promote Gender Equality and Women's and Girls' Empowerment', [online], n.d.(b), https://www.ilo.org/wcmsp5/groups/public/@dgreports/@nylo/documents/genericdocument/wcms_674612.pdf

44 United Nations, Universal Declaration of Human Rights, United Nations, 2015 (Art. 23 and 25)

45 Leite et al., 2017, p. 96

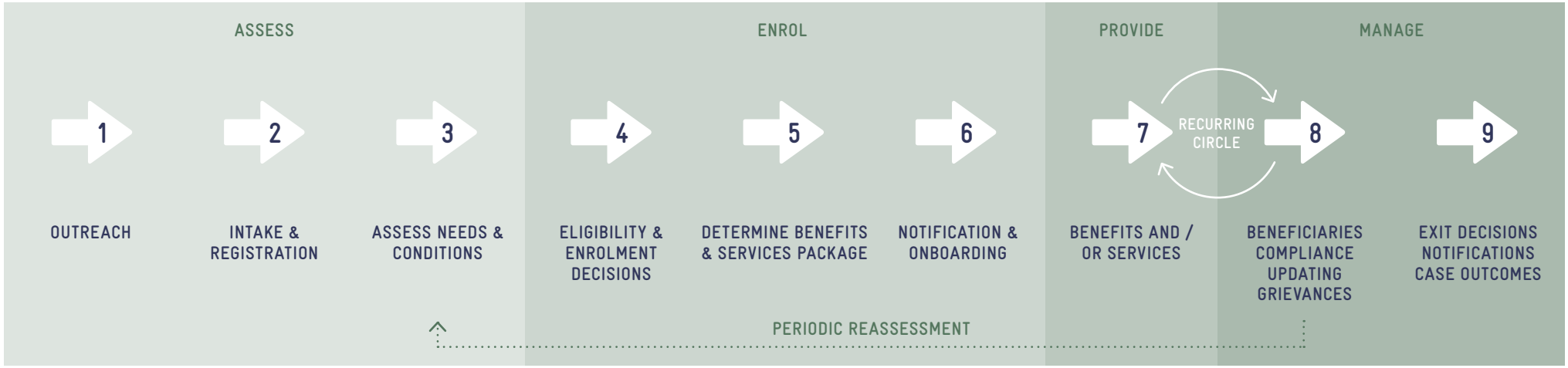
46 Lindert, Kathy; Karippacheril, Tina George; Rodriguez Caillava, Inés and Nishikawa Chavez, Kenichi, Sourcebook on the Foundations of Social Protection Delivery Systems, World Bank, Washington, DC, 2020, p. 2

47 Lindert et al., 2020, p. 3

48 International Labour Organization (ILO), 'Introduction: Social Transfers', [online], 2018, https://www.social-protection.org/gimi/gess/ShowTheme.action?id=11

49 World Food Programme (WFP), Two Minutes on Social Protection, WFP, 2017, https://documents.wfp.org/stellent/groups/public/documents/communications/wfp277442.pdf?_ga=2.82500497.681773780.1592505793-2117718756.1590495840

FIGURE 1 - SOCIAL PROTECTION DELIVERY CHAIN[50]



At the *programme level*, many social protection programmes use tailored **management information systems (MIS)**[51] to manage the delivery of these programme-specific implementation phases: from outreach, intake and registration through to supporting payments, service delivery, and case management or grievance redressal (Figure 1). In simple terms, an MIS is a tailored application software (supported by hardware, a telecommunications system, a database/registry and, of course, dedicated staff) that is designed to enable the digital flow of information required for a programme to function.[52] For example, this may include personal data relating to beneficiaries, implementation details (delivery amount, modality, location, devices), implementation partners (financial service providers, retailers) and other transactional data. Depending on the programme characteristics and design choices, programme MISs may vary quite significantly in their set-up.

At the *integrated level*, there is a growing trend towards the integration of specific functions along the delivery chain (Figure 1) across different programmes, and beyond. The overarching information system that enables integration within the social protection sector and beyond can be referred to as the **social protection information system (SPIS)**.[53] Such an information system may be designed in many different ways, depending on country choices. Some of its most important features could include:

- A **social registry** (referred to by some as a 'targeting database') – A social registry is an information system that supports – and integrates – the processes of outreach, intake and registration, and assessment of needs and conditions to determine potential eligibility for social programmes (serving one or more programmes in a country).[54] They collect and maintain socio-economic data on all registered individuals and households, regardless of whether or not they eventually benefit from a social programme. They can serve as tools for assessing the 'demand' for social programmes by profiling the specific needs and conditions of various population groups. In terms of their set-up, social registries vary significantly

50 Lindert et al., 2020, p. 11

51 The World Bank is moving towards calling these 'beneficiary operations management systems' (BOMS) (Barca and Chirchir, 2019, p. 12; Lindert et al., 2020).

52 Sepúlveda Carmona, Magdalena, Is Biometric Technology in Social Protection Programmes Illegal or Arbitrary? An Analysis of Privacy and Data Protection, Extension of Social Security (ESS), Working Paper No. 59, International Labour Organization, Geneva, 2018, p. 30; Barca and Chirchir, 2019

53 Barca and Chirchir, 2019, p. 12; Lindert et al., 2020; Barca, Social Protection Information Systems-ISPA Tool, (forthcoming)

54 In other words, they do not support the full implementation delivery chain of social assistance programmes, just intake and eligibility determination. Data is then shared with user programmes who manage these via their own MISs.

across countries (e.g. in terms of coverage, variables collected, institutional housing, approach to data sharing, etc.), which affects their potential uses.[55]

→ NOTE: Social registries typically contain socio-economic data related to the size and composition of the household (family members), income and/or expenditure, any disabilities, schooling, asset ownership, etc. However, the type of data collected varies widely across countries and ultimately depends on the targeting approach of the user programme/s and the eligibility criteria used.

- An **integrated beneficiary registry** (referred to by some as a 'single registry') – An integrated beneficiary registry that integrates data on beneficiaries across programme-specific MISs into a data warehouse. It provides an analytics function, via a consolidated overview of 'who receives what' benefits to support coordination, planning and integrated monitoring. Among other things, it can serve as a powerful tool to monitor and coordinate the 'supply' of social programmes, assessing overlaps, gaps and duplications across multiple programmes, while also supporting the consolidation of other functions along the delivery chain (payments, grievances, etc.), acting as a nexus of information, and providing interlinkages between individual programme MISs and other external databases such as the social registry (if one exists).

  → NOTE: The data these registries contain strongly depends on design choices.[56]

- **Further interoperability** with other government (and partner) databases and information systems (e.g. income tax, civil registration, disability, etc.)

These digital information systems enable the management of social protection programmes, in the process of collecting, storing, transferring and sharing a large amount of **personal and sensitive data** on:

- Applicants/registrants (the data required to assess their eligibility)
- Recipients/beneficiaries (the data required to enrol and serve/pay them)[57]

The collection and processing of personal data happens at every step of programme implementation, throughout the delivery chain and the different platforms for information management. It is for this reason that it is important for social protection authorities and managers, development partners and practitioners who process personal data, in their capacity as either data controllers or processors, to adhere to data protection and privacy principles and standards and comply with specific national and international rules that protect privacy and govern how personal information is processed.[58]

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

Some development and humanitarian agencies are what are called **international organisations (IOs)**, which operate according to their own charter and rules and are governed by international law. Others are so-called **non-governmental organisations (NGOs),** which are subject to national laws.[59]

NGOs (international and national) are under the jurisdiction of the country in which they operate and need to comply with the applicable laws. What data protection rules apply to them is not dealt with by this Implementation Guide, as this depends on the respective laws and factual circumstances in their country of operation. Instead, this Implementation Guide describes good practices regarding personal data protection and privacy, and suggests their application by NGOs, without prejudice to national laws.

IOs are governed by public international law and include organisations like the United Nations and the World Bank. Their operation in a country is based on an agreement with the host government, by which they may implement **humanitarian and development aid** projects, often integrating the host government social protection response, and providing cash transfers received from donors to vulnerable persons. IOs enjoy certain privileges and immunities to ensure that they can perform their mandate attributed to them under international

55 Leite et al., 2017, pp. iv–v); Barca and Chirchir, 2019; Lindert et al., 2020

56 Barca and Chirchir, 2019, p. 12; Lindert et al., 2020; Barca, Social Protection Information Systems–ISPA Tool, (forthcoming)

57 In social protection systems, information can be collected verbally (e.g. via interviews) or in writing (e.g. using forms). In addition, it can be stored physically (e.g. in paper files) or electronically (e.g. using computers or external hard drives, cloud storage, USB devices, computer networks). More and more frequently, and especially in the context of the digital information systems discussed in this section, the storage modality is electronic.

58 Barca and Chirchir, 2019, p. 13

59 See 'Glossary of defined terms' at the start of this guide.

law in full independence. To that extent, they are not subject to the jurisdiction of the countries in which they work.[60] "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'".[61] This has specific implications for the framing of data protection and privacy principles when IOs implement social protection programmes for, and on behalf of, or together with national governments.

2.3 WHY IS DATA PROTECTION NEEDED IN SOCIAL PROTECTION?

As discussed, social protection programmes process personal data collected from individuals, families, and households to deliver their services and benefits. Social protection authorities and practitioners should, thus, ensure that their programmes comply with national laws and/or regional and international standards that protect privacy and govern personal data. But the benefits of doing so go beyond mere legal compliance and avoiding penalties, so let's understand why it is so essential to protect this data:

- Social protection data is mainly collected from the most vulnerable groups in society. This population relies on social protection schemes and usually does not have any alternative, but to share their data, in order to receive support. Vulnerable people are less able to protect their rights and claim their entitlements than wealthier segments of the population. Therefore, protecting their data rights is vital to ensure a rights-based approach and respect for their fundamental and human rights.
- Ensuring personal data protection and privacy is a fundamental step in order for social protection programmes to reach their goals, including ensuring the quality of services and protecting minority groups and vulnerable populations. The protection of the personal data of applicants/registrants and recipients/beneficiaries generally improves the results of social protection programmes.
- Many social protection programmes in low- and middle-income countries use digital technologies (discussed above) to automate business processes and manage data. In addition, new and emerging technologies, such as biometrics, are used to establish people's identity. These may increase the risk to data protection and privacy.[62] Therefore, programmes need to establish strict security protocols and ensure compliance with data protection and privacy rules to protect data subjects' rights.[63]
- 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. As a result, individuals may suffer material, physical or symbolic harm.[64]
- Lastly, data protection and privacy are essential to creating trust among social protection authorities, practitioners, applicants, and beneficiaries. Without trust, vulnerable populations may be reluctant to access social protection services and benefits for fear that sharing their personal information will lead to harm, discrimination, stigmatisation, or surveillance, among other things.

2.4 MAIN STAKEHOLDERS AND RESPONSIBILITIES

When discussing data protection and privacy in relation to social protection systems and programmes at the country level, the main stakeholder groups and their roles and responsibilities are:

Governments: This includes national and local government 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: These are members of the government and lawmakers at the country level. They are responsible for the design of the data protection and privacy laws, which can be either sectorial or comprehensive. They establish legislation that defines the obligations and rights of different stakeholders and provides sanctions for violation.

60 ICRC Handbook, Sec. 2.4, p. 34 (Kuner, and Marelli, 2017)

61 Kuner and Marelli, 2017, p. 34

62 See Section 2.5 – Digital technologies increase the urgency of data protection.

63 Sepúlveda Carmona, 2018, p. 30

64 Sepúlveda Carmona, 2018, p. 33 (Box 11. Overview: Potential information damages, abuse or misuse that inclusion in social protection programmes may cause).

Data protection authorities (DPAs): A DPA is an independent public authority appointed 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, 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, as well as demonstrating compliance with data protection and privacy principles and legislation.

Development and humanitarian agencies and other development partners: This refers to any organisation dedicated to distributing aid and promoting economic growth and development in the areas they serve. Their role is to advise and support local governments to develop and/or improve their data protection and privacy framework and enforcement mechanisms.

Civil society: This includes civil society organisations, activists, academics, employers' and workers' organisations, and consumer protection organisations that lobby governments, lawmakers or other stakeholders to ensure that data subjects have rights over their personal data, monitor whether or not these rights are respected in practice, report violations, and raise public awareness about data protection and privacy.

2.5 DIGITAL TECHNOLOGIES INCREASE THE URGENCY OF DATA PROTECTION

Digital technologies hold great potential for the developing world.[65] They can be used to enable identification and authentication, for digital payments, and to streamline the management of information to support the design and delivery of social protection,[66] among other things. However, while digital technologies may simplify and accelerate processes, reduce some costs, increase efficiency and effectiveness, and improve transparency and inclusiveness, they also bring with them inherent challenges and risks. These include high technological costs, complexity (e.g. requiring a different skillset among administrative staff), challenges in relation to maintenance and sustainability, possible trade-offs (such as a reduction in overall equity), and risks to privacy and personal data protection.[67] Regarding data protection and privacy, examples of increased risks would be things like faster interoperability among systems, which might facilitate function creep, or enhanced data analytics, which might increase chances of de-anonymisation, profiling and surveillance.

The inherent risks and possible adverse side effects of digital technologies are enhanced by the lack of appropriate infrastructure and legal frameworks in developing countries, which have long been present in developed ones. It is generally agreed that any digital technology should only be adopted if its design and use comply with personal data protection and privacy standards. However, the combination of the processing of personal data and the adoption of digital technologies, apart from bringing many advantages, may impose considerable challenges to personal data protection and privacy, if not accompanied by a careful risk assessment and the implementation of appropriate safeguards.

2.6 IS THERE A TRADE-OFF BETWEEN THE RIGHT TO (DATA) PRIVACY AND THE RIGHT TO SOCIAL PROTECTION?

According to the Vienna Declaration – a statement that reinforces the Universal Declaration of Human Rights – "all human rights are universal, indivisible and interdependent and interrelated".[68] This is the case with privacy and social protection, which are both human rights. It is not possible to enjoy the protection of one without the other. Privacy and social protection are important aspects of a democratic society.[69]

65 Lindert et al., 2020, p. 422

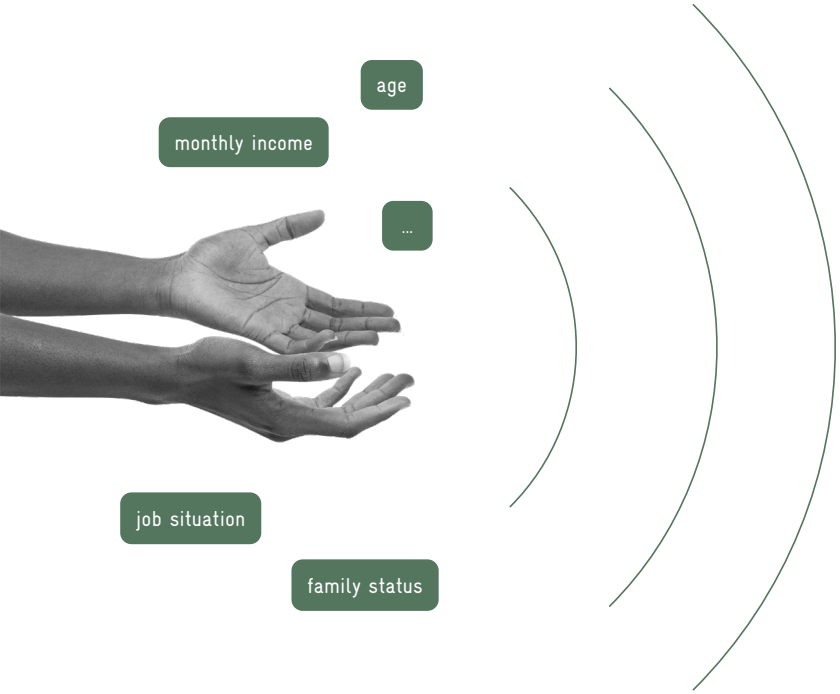
66 Barca and Chirchir, 2019, pp. 11–15

67 See Barca and Chirchir (2019) for a broader discussion of these risks and challenges.

68 UN General Assembly, Vienna Declaration and Programme of Action, 12 July 1993, A/CONF.157/23, United Nations, 1993, Art. 5

69 Privacy International, Privacy, a Precondition for Social Protection, 2019, https://privacyinternational.org/news-analysis/3029/privacy-precondition-social-protection

There is no trade-off between protecting personal data and privacy and providing effective social protection programmes and benefits, per se. However, in practice, this trade-off can exist, particularly for the most vulnerable members of society, namely: the invasion of (data) privacy in exchange for access to social protection benefits.[70] For instance, when applying for social assistance benefits, access is sometimes conditional upon increased surveillance, control and data exploitation. Moreover, in some cases, as part of government efforts to ensure that no benefits are provided to the wrong persons, individuals are required to provide biometric data (e.g. fingerprints or a retina scan) as a condition of access, without the appropriate safeguards. 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 as applicants/registrants and recipients/beneficiaries of social protection programmes.[71] Lastly, no effective social protection system is possible without personal data protection and privacy.



70 Ibid.

71 Sepúlveda Carmona, 2018, p. 12

PART 2

GOOD INTERNATIONAL PRACTICES FOR DATA PROTECTION AND PRIVACY

CHAPTER 3

INTRODUCTION: DATA PROTECTION AND PRIVACY STANDARDS

CHAPTER 3. INTRODUCTION: DATA PROTECTION AND PRIVACY STANDARDS

Several international and regional data protection instruments share a set of core data protection and privacy standards.[72] While these instruments have different names[73] and vary in scope and content, personal data protection and privacy frameworks typically consist of the following groups of standards:

Principles governing the processing of personal data (hereafter referred to as 'data protection and privacy principles')

- Purpose specification
- Data minimisation
- Lawfulness, fairness and transparency
- Accuracy
- Retention limitation
- Security
- Accountability

Data subject rights

- Right to information about personal data processing
- Right to access the personal data that is processed
- Right to data rectification
- Right to data erasure
- Right to object to processing or withdraw consent
- Rights related to automated decision-making
- Right to complain to an independent body (administrative redress)
- Right to an effective remedy (judicial redress)

Accountability, oversight and enforcement

- Legal responsibilities with respect to data protection and privacy principles and the rights of data subjects (accountability)
- An independent authority monitoring compliance with respect to data protection and privacy principles and the rights of data subjects (oversight)
- Legal redress for data subjects (enforceability)

Transborder data flow/international data sharing

Sensitive personal data

- These data protection and privacy standards need to be considered when data is qualified as personal data, when there is a remote possibility of identifying an individual in an otherwise anonymised dataset, and when the data of groups are considered sensitive. Each is discussed in more depth in the following chapters.

72 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, or in regional and national laws, exists to serve as a reliable basis for defining good international practices in personal data protection and privacy. This Implementation Guide does not claim to comprehensively define good international practices in relation to 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 – Most significant internationally agreed-upon data protection and privacy instruments. Their interpretation draws mostly on 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.

73 The terms used in this Implementation Guide are a mix drawn from the relevant data protection and privacy frameworks, as deemed most comprehensive.

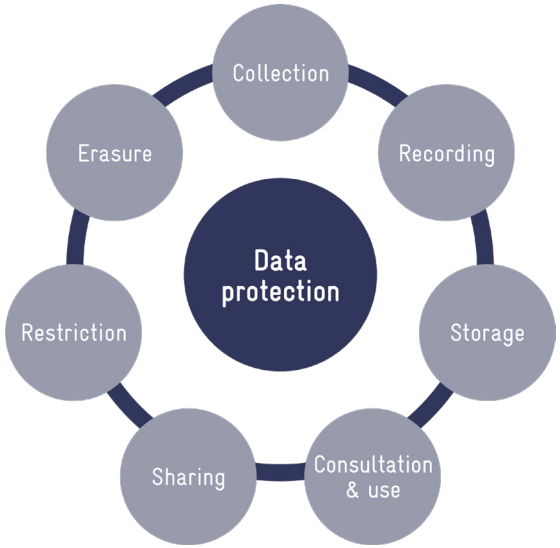
CHAPTER 4

DATA PROCESSING PRINCIPLES

CHAPTER 4. DATA PROCESSING PRINCIPLES

This chapter sets out the core principles restricting the processing of personal data, as indicated by good international practices. These need to be applied to all phases of data processing and regularly reassessed.

FIGURE 2 - DATA PROCESSING PHASES



4.1 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 in 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 are used are too numerous, they cannot be explicitly specified by the law. However, specifying and informing the data subject about the purpose(s) for which their personal data is being collected and will be processed is a way to self-impose on the data controller an obligation that data collected for one purpose will not be used for a different purpose.

A legitimate purpose (or purposes) needs to be determined for each data processing activity. For example, the purpose of data collection could be the creation of a list of beneficiaries to receive cash transfers. Another example 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.[74] As a guideline, the purpose is not considered compatible if the data subject might consider the further processing unexpected, inappropriate, or otherwise objectionable.[75]

The purpose of data processing goes hand-in-hand with its lawfulness. If the purpose of the further processing is not compatible with the initial purpose communicated to the data subject at the time of that the data was collected, then such data processing should only be permitted, if (i) the new purpose is specified, explicit and legitimate and (ii) the controller has a new legal basis, such as consent, a legal obligation, or other.[76] 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 it is, de facto, a different purpose.[77] Data, thus, can be processed for that further purpose without a new legal basis (such as the beneficiary's consent).

74 GDPR 2016/679, Art. 5 (1); CoE Convention 108+, 2018, Art. 5 (48)

75 CoE Convention 108+, 2018, Explanatory Report (Sec. 49)

76 See Section 4.3 – Lawfulness, fairness and transparency.

77 GDPR 2016/679, Art 5. (1); CoE Convention 108+, 2018, Art. 5 (50)

4.2 DATA MINIMISATION

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

Why is it important? The intrusion into the individual's private 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 principle 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 achieved with less or no personal data, or less sensitive personal data. This relates not only to data collection, but also to further data processing. Thus, data needs to be deleted if the specified purpose has been achieved or it is not necessary anymore because the purpose has changed.[78]

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

4.3 LAWFULNESS, FAIRNESS AND TRANSPARENCY

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

Why is it important? Any 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 interference.

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.

For each data processing activity, data controllers need to identify one of the legal bases set out 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 different activities. For example, governments will be authorised to process personal data for official activities on the basis of public interest and/or a legal obligation. Still, for the personal data of their staff, the processing is usually 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 their contract with the individual. Any additional data will be based on the individuals' consent and, in specific cases, on a legitimate interest. IOs are not subject to most national laws, but to their own rules (see Box 4). They process data based on the legal bases identified by their rules. These may be specific to the activities they typically implement.

The legal bases suggested for use in the area of social protection will be discussed further in this Implementation Guide.[79]

Box 5 - Legal bases for processing personal data

According to most international, regional and national data protection and privacy frameworks, processing personal data is legal in the following situations:[80]

- **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, the execution of criminal penalties, and the enforcement of civil law claims, among other things. For IOs, 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.[81]

78 See Section 4.5 – Retention limitation.

79 See Chapter 11 – How to apply data protection and privacy standards to social protection programmes.

80 See, for instance, GDPR 2016/679 (Art. 6, 7, 8, 9) and CoE Convention 108+, 2018 (Art. 5, 17) for the legal basis of consent and personal data processing. Other bases are provided by ECOWAS, 2010 and the OECD Privacy Framework, 2013 (see Organisation for Economic Co-operation and Development, The OECD Privacy Framework, OECD Publishing, 2013).

81 Kuner and Marelli, 2017, p. 67

- **Vital interests:** This basis applies when the processing of data is necessary to protect the vital interests of a data subject or another person (i.e. to protect someone's life, integrity, health, dignity, or security). For this basis to apply, it is necessary for there to be sufficient elements to consider that, in the absence of the personal data processing, the individual could be at risk of physical or psychological harm.
- **Legal obligation:** The processing of data 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 who provide evidence of being under a certain poverty level. In this case, the authority is required to collect the data to assess those conditions and ensure delivery of the benefits to the targeted persons in order to comply with its legal obligation.
- **Informed consent:** Under this basis, consent indicates the data subject's agreement to the processing of personal data relating to him/her for a specific purpose. When 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 will not always be the most appropriate legal basis.
- **Contract with the data subject:** This basis applies when 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.
- **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 interest, 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, and must not affect people's fundamental rights and freedoms. If the same result can be reasonably accomplished in another less intrusive way, the basis of legitimate interest does 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 as to what legal basis their data is being processed under.

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 in relation to giving their personal data due to their situation (e.g. in desperate need of aid). Also, it means that no unfair practices are used, such as the use of hidden data registration devices (e.g. voice recorders) or deceiving data subjects into supplying information.

4.4 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 often 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, the purpose of collecting and processing data may not be achieved. In addition, inaccurate data may lead to 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.

4.5 RETENTION LIMITATION

Personal data should only be retained in a form that permits the identification of data subjects for the period of time that is necessary to achieve the purposes for which it was collected and processed. The right to privacy requires that no personal data is kept by the data controllers if the use purpose(s) has been fulfilled or is no longer pursued.

Why is it important? The retention limitation is important to comply with the purpose specification, data minimisation, and accuracy principles. Ensuring the erasure or anonymisation of personal data when it is no longer needed reduces the risk that it will be used (or misused) for purposes different to 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, the erasure of unused data helps to reduce the burden on 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 purpose, such as archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.[82] 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.

4.6 SECURITY

Personal data, as well as the infrastructure relied upon for processing personal data, have to be secure during storage, transmission and use.

For this, systems need to be available. Therefore, appropriate **physical, technological and organisational measures** must be taken to ensure the security of data and systems, to protect personal 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 lead to harm or cause distress to people. In extreme cases, lives can be at risk. Security incidents may also cause reputational issues for data controllers and processors. Finally, information security is essential to develop a trusting relationship with data subjects.

The risks may be grouped into three categories:

- **Confidentiality:** Only authorised people or parties (acting within the scope of the authority given to them) can access, disclose, alter or delete the data.

  → RISK: Illegitimate access to data, unauthorised use or modifications

- **Integrity:** Who is modifying data is tracked.

  → RISK: Changes to 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

Some examples of the harm generated by the loss or abuse of personal data are:

- Discrimination
- Persecution
- Identity fraud
- Crime witnesses put at risk of physical harm or intimidation
- Credit card fraud or other financial loss
- Exposure to embarrassment or damage to reputation
- Fake applications for services or benefits
- Analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles.

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 on, among other things, the:

- 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 the operating system, MIS)
- Transfer of data (e-mail/Internet, application programming interface [API])
- Environment/location of the specific personal data
- Prevailing security and logistical conditions[83]

82 GDPR 2016/679 (Art. 5) and OECD Privacy Framework, 2013 (see OECD, 2013, p. 14).

83 Kuner and Marelli, 2017, p. 44

Box 6 - Security measures

Personal data security measures relate to the physical security of the premises where the personal data is stored, as well as technological and organisational security, and may include the following:[84]

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
- How to keep paper files secure (lock on cupboards)
- Technological security measures
  - System security: The security of the network and information systems, particularly those that 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: The security of the website, online services or applications, etc.
  - Device security: The security of tablets used for data collection, etc.
- 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 that this person/team has the appropriate resources and authority to do their job effectively.
  - Build a culture of security awareness within the organisation, particularly relating to personal data.
  - Provide training for staff on information security, with an emphasis on personal data.
  - Check whether or not security measures are actually being adhered to.
  - Establish standard procedures to deal with security incidents.
  - Undertake regular testing and review of the adequacy of the above security measures (are they 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 only to the protection of networks and information systems from attack. Thus, information security (e.g. the security of personal data) is broader than cybersecurity, as it also covers physical and organisational security measures.

4.7 ACCOUNTABILITY

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

Why this principle is important and some implementation aspects will be discussed in detail in Chapter 6 (Section 6.1 - Accountability: Legal obligations of data controllers and processors).

84 Information Commissioner's Office (ICO), Data Sharing Code of Practice, Draft Code for Consultation, n.d.(b)

CHAPTER 5

DATA SUBJECT RIGHTS

CHAPTER 5. DATA SUBJECT RIGHTS

The rights of data subjects are the second key pillar of international and regional data protection and privacy frameworks.[85] These frameworks recognise that data subjects should be fully informed about and, thus, enabled to better control the processing of their personal information. Data subjects' 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.[86] This chapter outlines the rights of data subjects.

5.1 RIGHT TO INFORMATION

The controller should, at the time when the personal data are collected from the data subject, or within a reasonable time if obtained from a third party, fairly and transparently inform the data subject in detail of how their personal data will be processed.

Box 7 - Checklist of good practices: What information should be provided to data subjects?

Good international practices require individuals to be provided with the following information:[87]

- ☐ The identity and the contact details of the controller
- ☐ The purpose(s) of the processing
- ☐ The legal basis for the processing
- ☐ The categories of data involved
- ☐ With which entities the personal data will be shared and for what purpose(s)
- ☐ Whether or not 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 subject has over their data in relation to the controller and processor, and how they can exercise them
- ☐ The rights that the data subject has, 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, as well as 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

5.2 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, if 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 on a lawful basis, in accordance with the information provided to them at the time of data collection, and if it is accurate. This knowledge enables them to decide whether or not 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, which might prevent data controllers from engaging in such practices.

85 In a number of international and regional data protection and privacy instruments, such as those of the OECD (OECD, 2013), UN (UN General Assembly, 1990) and APEC (APEC, 2005), the rights of the data subjects are integrated into different principles. In other instruments, such as the Malabo Convention (African Union, 2014), ECOWAS (ECOWAS, 2010) and the GDPR (European Parliament and Council of European Union, 2016), the rights of the data subject are presented in a specific section, separate 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.

86 CoE Convention 108+, 2018 (Art. 9)

87 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).

Box 8 - Checklist of good practices: Exercising the right to access

Good international practices require data subjects to be able to easily request and be given information about the processing of their personal data by the controller.[88] Access should be:

- ☐ Freely given or, if there is a charge, it should be not excessive (e.g. a reasonable fee based on administrative costs)
- ☐ Within a reasonable and stated time
- ☐ In a form that is readily intelligible to the data subject and does not require any particular expertise or knowledge to comprehend the information

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

5.3 RIGHT TO RECTIFICATION

The data subject should have the right to request and obtain the rectification (to correct, update, or modify) of their personal data from the data controller, without undue delay, to ensure that the data is accurate, complete and up-to-date. Depending on the content of the request, and without placing an unreasonable burden of proof on the data subject, the data controller may need the data subject to provide proof of the alleged inaccuracy and assess the credibility of the assertion.[89] 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.

5.4 RIGHT TO ERASURE

Certain data protection frameworks, such as those of Nigeria, South Africa, the GDPR and the CoE Convention No. 108+, include the right to erasure. This right allows data subjects, in certain circumstances (e.g. when there is no lawful basis for data processing), to request that the data controller erase their personal data.

88 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).

89 Kuner and Marelli, 2017, p. 55

Box 9 - Checklist of good practices: When can the right to erasure be exercised?

Good international practices require that data subjects have the right to have their personal data erased from the controller's database in (one of) the following instances:[90]

- ☐ Their personal data are no longer necessary in relation to the purpose(s) for which they were collected or otherwise processed.
- ☐ The data subject has withdrawn consent and there is no other legal ground for the processing.
- ☐ The data has been obtained based on a public task or legitimate interest, the data subject objects to the processing, and there are no compelling legitimate interests overriding the rights and freedoms of the data subject.
- ☐ The processing does not comply with the applicable data protection and privacy framework.
- ☐ The personal data must be erased to comply with a legal obligation to which the controller is subject.

However, the GDPR and the CoE Convention 108+ recognise limitations on this so-called 'right to be forgotten'. This right does 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).[91]

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 it is impossible or involves unreasonable effort.[92]

90 See GDPR 2016/679 (Art. 17), CoE Convention 108+, 2018 (Art. 9), Malabo Convention, 2014 (Art. 19), APEC, 2005 (Art. 29–30).

91 CoE Convention 108+, 2018 (Explanatory Report, Sec. 73), GDPR 2016/679 (Art. 17)

92 GDPR 2016/679 (Art. 19)

5.5 RIGHT TO WITHDRAW CONSENT AND TO OBJECT TO DATA PROCESSING

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,[93] but also about the implications of withholding consent. 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 that overrides the interests or rights and freedoms of the data subject, such as taxes or public health.[94] The controller needs to provide evidence of these overriding legitimate grounds to the data subject. If these grounds are not present, the controller must stop the processing and delete the data (public interest) or keep the data (legal obligation). The right to object might be absolute in some cases, for instance, when personal data are processed for direct marketing purposes.

5.6 RIGHTS RELATED TO AUTOMATED DECISION-MAKING AND PROFILING

Some international and regional data protection and privacy frameworks – e.g. the CoE Convention 108+ and the GDPR – establish data subjects' rights relating to automated decision-making.[95] According to these frameworks, data subjects should have the right not to be subject to a decision based purely on the automated processing of their 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 and the CoE Convention 108+ extend this right to include automated decision-making based on 'profiling' (see Box 10 for detailed explanation). This right works slightly different than other data subjects rights, as controllers and processors do not have to act only upon a request by a data subject. Instead, this prohibition applies independently of whether or not the data subject takes action regarding the processing of their personal data.[96]

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

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

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

96 Article 29, Working Party, 2018 (p. 19)

Box 10 - What is automated decision-making and profiling?

Automated decision-making refers to 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 sources. 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. Typical examples for social protection purposes include proxy means testing (PMT) and fraud detection algorithms.

Profiling refers to 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.[97] Profiles are created based on the personal data of the data subject, obtained directly or indirectly (meaning it can be derived or inferred from other data, and predicted). The information is analysed to classify people into different groups or sectors, using artificial intelligence, including machine-learning,[98] in order to evaluate (score, rank, assess) and predict certain things about an individual (behaviour, interests, performance) 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[99] (e.g. calculating a score through profiling that predicts the likelihood of an individual committing a future crime based on the individual belonging to such a profiled group).[100] These profiles can be used to inform decisions about individuals that may or may not be automated. To the extent that they inform automated decisions, the respective data subject rights need to be respected.

97 GDPR 2016/679 (Art. 4)

98 For more information about artificial intelligence, including machine learning, see 'Glossary of defined terms'.

99 Predictive policing involves the use of algorithms to analyse great amounts of information to predict and help prevent potential future crimes.

100 Privacy International, The Keys to Data Protection: A Guide for Policy Engagement on Data Protection, 2018, p. 57

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".[101] 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, establishing the irrelevance of the profile to be applied to his or her particular situation, when the application of algorithmic reasoning would stigmatise the individual resulting in the limitation of a right or refusal of a social benefit, or when they see their credit capacity evaluated by software only.[102]Automated decision-making, including profiling, may only be permitted if it is authorised by a law that lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.[103]

Box 11 - Checklist of good practices: Rights related to automated decision-making and profiling

Good international practices require the following:[104]

- ☐ Both automated individual decision-making and profiling should be covered in a data protection framework (however, they don't need to be dealt with together, as 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 on their lives (e.g. an automated decision regarding a refusal of a social protection benefit).
- ☐ 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

5.7 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 of the controller, to obtain an independent review of the data processing activity in question.[105] In countries 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 enforcement of data protection and privacy laws. 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 where such laws do not provide for the establishment of 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).[106] After submitting a complaint to a supervisory authority or internal office (such as a DPA or DPO), the authority/office should inform the individual of the progress and outcome of the complaint, including the possibility of a judicial remedy, if such remedy exists.

5.8 RIGHT TO AN EFFECTIVE JUDICIAL REMEDY

Individuals should have the right to an effective judicial remedy against data controllers or processors, when they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law. The CoE Convention 108+ obliges states to grant data subjects an appropriate judicial remedy for violation of the respective

101 Kuner and Marelli, 2017, p. 453

102 CoE Convention 108+, 2018 (Explanatory Report, Sec. 75)

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

104 GDPR 2016/679 (Art. 22)

105 CoE Convention 108+, 2018 (Art. 77); some frameworks foresee the necessity of providing appropriate administrative remedies in situations where privacy protections are violated, for instance, APEC, 2005 (Art. 20, 53), CoE Convention 108+, 2018 (Art. 9, 12), GDPR 2016/679 (Art. 78, 79).

106 See Section 11.3 – How to be an accountable social protection controller.

framework.[107] The GDPR, being binding on legal subjects in EU member states, 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.[108]

To facilitate the right of data subjects to access an effective remedy, individuals should be able to be represented before a supervisory authority or a court for example by non-profit organisations active in the field of data protection or human rights, at no cost.

107 CoE Convention 108+, 2018 (Art. 9, 12), GDPR 2016/679 (Art. 78, 79)
108 GDPR 2016/679 (Art. 82)

CHAPTER 6

ACCOUNTABILITY, OVERSIGHT AND ENFORCEMENT

CHAPTER 6. ACCOUNTABILITY, OVERSIGHT AND ENFORCEMENT

International and regional data protection standards 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 the exercise of the data subject rights. They are also responsible for demonstrating their compliance to the DPA (if one exists) upon request. These provisions aim to strengthen the data subject's position by increasing their ability to check compliance by controllers.

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

- **Legal obligations:** A clear regime of the responsibilities of those who process personal data, namely data controllers and processors.
- **Independent oversight:** The independent monitoring of the application of the data protection and privacy framework through a DPA, including compliance by data controllers and data processors with their obligations.
- **Administrative and legal redress:** The data subjects' right to make a complaint to the independent DPA and to an effective judicial remedy, when 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.

6.1 ACCOUNTABILITY: LEGAL OBLIGATIONS OF DATA CONTROLLERS AND PROCESSORS

Most data protection and privacy frameworks allocate the responsibility to comply with the framework to data controllers and data processors. The **data controller** is the individual or legal entity that, alone or jointly with others, determines the purpose and means of the personal data processing. This means that the data controller makes 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 the data controller.

Data protection and privacy frameworks typically see the data controller as the main entity responsible for complying with the data processing principles and upholding the data subject's rights. The processor acts on behalf of the controller and according to 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 laws.

Data protection and privacy standards should result in data controllers and data processors having certain obligations (see Table 1), in addition to other obligations under applicable laws. These obligations should be reflected in the respective data protection law.

TABLE 1 - OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

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 established in the legal agreement with the controller.
Data minimisation	Ensure that only the minimum data necessary for the fulfilment of the purpose is processed.	Ensure that only the minimum data necessary for the fulfilment of such purpose is processed, as 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 the fairness and transparency of each data processing activity.	N/A: The 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.	If the legal agreement requires the processor 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, as provided for in the legal agreement.
Security	Ensure that data is secure during each data processing activity, including transfer and storage, and that 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 the law and any particular requirements in the legal agreement.
Data subject rights	Ensure that data subjects are enabled to exercise their rights, such as to access, rectification, and erasure and, if applicable, the right to object, as well as rights related to automated decision-making. Comply with such rights. If applicable, inform and support data subjects in relation to their right to submit a complaint to an independent body such as a DPA, or to obtain judicial redress (including financial compensation).	N/A: Unless the data controller delegates some of its responsibilities to the data processor, for example, to provide data subjects with certain information about the data processing or to set-up and operate a hotline through which data subjects can exercise their rights.

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.	Do not share personal data with any third party, unless expressly instructed/authorised by the 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 a data protection impact assessment (DPIA), if applicable.	Implement a DPIA on their technologies for provision to the controller.
	Maintain records of processing activities.	Maintain records of processing activities.
	Select only processors that have sufficient guarantees to implement appropriate measures to comply with their obligations under the data protection and privacy framework and sign a legal agreement with the 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 the controller to obtain precise instructions about the data processing activity and limit its liabilities.
	Sign legal agreements that determine the allocation of responsibilities when two entities act as joint data controllers.	N/A
	Notify data subjects of any data breach, as well as the data protection authority, if one exists.	Notify the controller of any data breach.
	Be liable and compensate data subjects for any damages incurred due to violations of the data protection and privacy framework.	If the data processor is also liable to the data subjects (as per the applicable data protection framework), the processor needs to compensate data subjects for any damages incurred due to the violation of their obligations under the data protection and privacy framework or where the processor has acted outside/against the instructions of the 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.

6.2 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 12 - Independent supervisory authority/data protection authority (DPA)

What is it? A public body, as determined in each jurisdiction, that is responsible for enforcing personal data protection and privacy laws and that is tasked with monitoring and enforcing the application of such laws, including through approval requirements, investigations, and administrative fines, as well as for handling complaints and promoting awareness of rights and obligations thereunder.

The law should establish the DPA's structure, powers and mandate.[109] Good international practices require DPAs to 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 data protection and privacy laws.
- Conduct investigations on the application of such laws.
- Handle the complaints of data subjects with respect to the violation 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.

Powers:

- Impose sanctions.
- Suspend data flows.
- Issue reprimands to data controllers with respect to violations of the law.
- Order the controller to comply with the requests of data subject.
- Carry out data protection audits.
- In some cases, a data protection law can give the DPA the power to regulate certain aspects of the law, for example, to update definitions or security requirements.[110]
- Approve safeguards for transborder data flows.

A national DPA is generally established by law. However, in the absence of such laws, public authorities may have the power to establish a sectorial DPA. Whether or not, and how, this is accomplished depends on the national laws of the country.

6.3 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 DPA and receive an administrative remedy.[111] For example, judicial redress would be relevant when a data subject does 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.

109 Privacy International, 2018, pp. 86–88

110 Ibid., p. 87

111 CoE Convention 108+, 2018 (Art. 9, 124), GDPR 2016/679 (Art. 78–82)

CHAPTER 7

INTERNATIONAL DATA SHARING

CHAPTER 7. INTERNATIONAL DATA SHARING

International and regional data protection and privacy frameworks additionally recognise the importance of protecting personal data not only when processed within a given jurisdiction, but also when it "travels across borders".[112] This may occur, for example, when governments share the personal data of refugees who have crossed borders from one country to another, or of social security recipients to enable the portability of benefits across localities – but also when controllers use processors located in other jurisdictions and process data in third jurisdictions, such as cloud providers or other service providers.[113] International data sharing also occurs when a government shares personal data with an IO, and vice versa, given that any data processing by IOs is subject to their own data protection and privacy frameworks, not the national laws of the country in which they operate.[114]

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 an IO) is a new data controller, as it determines the purposes and the means of data processing. For example, a government shares citizens' personal data in a region hit by a natural disaster with an IO that rolls out an assistance programme to vulnerable people targeted by the IO.
- **Data sharing between the data controller and processor:** The receiving entity (located in a different country or an IO) processes the data on behalf of the controller. For example, a government shares the 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 provides that when the recipient is subject to another jurisdiction or is an IO, the transfer of personal data may only take place when an appropriate level of protection (based on the data protection and privacy framework of the transferring entity) is secured.[115] An appropriate level of protection for the data recipient can be ensured through:

- The law of the state or IO, 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 protection. 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 minor.

112 OECD Privacy Framework, 2013 (Art. 16–18), GDPR 2016/679 (Art. 44–50), CoE Convention 108+, 2018 (Art 14)

113 See Section 12.2 – Data protection and privacy challenges of specific technologies.

114 See Box 4 – International organisations, non-governmental organisations and applicable law.

115 CoE Convention 108+, 2018 (Art. 14)

CHAPTER 8

SENSITIVE PERSONAL DATA

CHAPTER 8. 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,[116] sensitive personal data is a particular sub-category of personal data that 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 of data subjects.

This category of data typically includes information revealing personal characteristics (including physical appearance), such as:

- Racial or ethnic origin
- Health information
- Sexual orientation
- Political opinions or affiliations
- 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)[117]
- Data relating to children

For example, biometric data allows the irreversible re-identification of individuals, as such information cannot be modified like an address or name. This increases the risk 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, 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.[118] For example, in the area of social protection, the GDPR provides that sensitive data may be processed, without the individual's consent, if the:

> *… 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.*[119]

The following are some appropriate safeguards that may prevent adverse effects for the data subject when sensitive personal data is implicated:

- Requiring the data subject's explicit consent to be obtained
- Laws covering the intended purpose and means of processing, indicating the exceptional cases when the processing of sensitive personal data is permitted
- Measures put in place following a specific risk assessment
- Specific and qualified organisational or technical security measures
- Provision for individuals to be able 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 is based on sensitive personal data, good international practice recommends that the processing should only be carried out if:

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

116 GDPR 2016/679 (Art. 9), CoE Convention 108+, 2018 (Art. 6, 55–61)

117 See 'Glossary of defined terms'.

118 GDPR 2016/679 (Art. 9), CoE Convention 108+, 2018 (Art. 6, 55–61), Malabo Convention, 2014 (Art. 14)

119 GDPR 2016/679 (Art. 9)

PART 3

HOW TO IMPLEMENT DATA PROTECTION AND PRIVACY IN SOCIAL PROTECTION PROGRAMMES

CHAPTER 9

HOW TO PROMOTE AND ADOPT STANDARDS FOR DATA PROTECTION AND PRIVACY

CHAPTER 9. HOW TO PROMOTE AND ADOPT STANDARDS FOR DATA PROTECTION AND PRIVACY

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

- Adoption or improvement of **national** data protection laws
- Issuing of an **organisational** policy for the organisation or public authority implementing the social protection programme
- Development of data management protocols for each social protection **programme**

9.1 NATIONAL DATA PROTECTION AND PRIVACY LAWS

A first fundamental, but relatively high-level and long-term, step for implementing data protection and privacy standards in any social protection programme is the formulation and adoption of national data protection and privacy laws. Or, if such laws already exist, their improvement and supplementation. In this sense, from the social protection side, authorities should encourage lawmakers to introduce or update data protection and privacy legislation.

Lawmakers in countries planning to adopt a national data protection law could take the good practices for data protection and privacy as reference and inspiration.[120] Furthermore, any international or regional data protection and privacy framework that applies to the given country needs to be taken into consideration. In addition, 'hidden' data protection standards in sector-specific laws, such as laws on information or cyber security, electronic communications, financial services, and others, need to be considered.

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

Upon the promulgation of the national data protection and privacy laws, the social protection laws, regulations, and policies may need to be amended to comply with mandatory data protection requirements and enable application of the country's data protection and privacy standards to all social protection programmes in their different phases.

9.2 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 for a social protection ministry or department and larger international NGOs implementing social protection programmes as controllers.

By putting in place 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 Part 2. However, it would not ensure external oversight or the 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 and, thus, be limited to the personal data of the applicants/registrants, and recipients/beneficiaries. However, it could also cover all personal data processed by the controller, including employees, job applicants, and vendors, in the case of international organisations, individual donors, and others.

120 See Part 2 – Good international practices for data protection and privacy.

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 this helps demonstrate compliance with the data protection and privacy laws in place.[121] Demonstrating compliance includes, among other things, showing that:

- A policy is in place.
- Staff are aware of the policy and have been trained appropriately.
- A person responsible for compliance has been appointed.
- Audits are undertaken.
- A system for handling complaints has been set up.
- There is transparency 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 DPO, legal redress for data subjects) may overlap with the policies of other organisational policies, such as those for 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 13 - Data protection and privacy policy

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

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 assessments

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 demonstrate that the organisation is taking measures to ensure compliance.[122] It is particularly important for organisations or authorities that wish to implement good standards of personal data protection and privacy in their operations, if national laws do not contain such standards.

Box 14 - 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 governance and accountability mechanisms, as deemed appropriate by the respective entity. Suggestions on how to structure a policy are as follows:

- Introduction and purpose
- Scope
- Definition of key terms
- Data protection principles:
  - Which ones you commit to
  - Appropriate guidance on how to uphold each principle
- Data subject's rights
- Governance and accountability:
  - Establish a DPO to monitor the implementation of the policy by the organisation.
  - Regulate the roles and responsibilities of staff and 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

121 Sepúlveda Carmona, 2018, p. 54

122 The GDPR 2016/679 (Art. 24) suggests that controllers implement data protection policies "where appropriate in relation to processing activities".

legal department, the compliance department, the controller/audit department, and others, with respect to the implementation of the policy.
  - Data breach management
  - Working with third party processors
  - Data transfers to third parties
- Treatment of sensitive data: The use of beneficiaries' sensitive data should be specifically regulated, in terms of permitted use purposes, legal basis, data minimisation, strict security measures and short retention periods, among other things.
- International data sharing (if applicable)
- Other general obligations of the controller,[123] such as data breach notification procedures and record-keeping
- Non-applicability
- Good practices and practical steps for staff to follow

This list is neither complete nor exhaustive. Each organisation or 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 implementation of the policy, containing guidance on points that are particularly relevant to implementing a social protection programme, such as what legal basis to choose, when and how to use biometrics (if at all), how to allow individual data subjects to exercise their rights, and 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 while 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.[124]

123 See Table 1 – Obligations of data controllers and data processors.

124 See Section 9.3 – Data management protocol for a social protection programme.

In the absence of national data protection and privacy laws that establish independent oversight and the enforceability of data subject rights, the social protection authority could consider (if and to the extent permitted by the applicable laws) putting alternative mechanisms in place until such time as 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 to oversee and enforce the data protection and privacy policy and review complaints by data subjects concerning possible violation of their rights by the controller.
- With respect to making **data subject's rights enforceable**, the ministry could consider establishing an alternative dispute resolution mechanism 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.

9.3 DATA MANAGEMENT PROTOCOL FOR A SOCIAL PROTECTION PROGRAMME

In order to incorporate data protection and privacy standards (from applicable laws and the organisational policy or, in their absence, from good international practices) into a social protection programme, it is necessary to apply the provisions of the data protection and privacy policy (or in its absence, the data protection and privacy principles) to the programme. While this does not replace laws or 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, the data management protocol, as appropriate. Such a 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 (see Section 2.2).[125] Therefore, it is important that the **data management protocol** covers at least the following points:

125 See Figure 1 – Social protection delivery chain.

- The data flow in each stage of the delivery chain, for example:
  - Is personal data needed at each stage of the delivery chain, or can certain functions be performed based on aggregate data (e.g. from international organisations or the government)?
  - Can zero-knowledge proofs (ZKPs) or other technical or organisational measures be used to minimise the amount of data being shared?
  - How will data be collected from individuals (e.g. census-type data collection vs. data collection on-demand via application)?
  - Storage of data operated by an international corporation:[126] Where will the data be stored (in country)? What are the security measures? Who has access to the data?
- All stakeholders and data protection risks for each
- 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 DPO for the respective programme
- All mitigation measures via the data protection impact assessment (DPIA) (see Chapter 10)
- Resources and capacity training for staff on the data management protocol

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

126 This is sometimes the case when governments contract private companies to support the creation and management of their information system.

CHAPTER 10

HOW TO CONDUCT A DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND ENSURE PRIVACY BY DESIGN

CHAPTER 10. HOW TO CONDUCT A DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND ENSURE PRIVACY BY DESIGN

10.1 CONDUCTING A DPIA

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 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 lead to a project design that avoids or minimises any data protection and privacy risks (privacy by design, see Box 15).[127]

Box 15 - Privacy-by-design

Systems should implement privacy-by-design, meaning that data protection and privacy is a default design objective. In other words, systems by standard should implement 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 Framework, the 'privacy-by-design' approach is interpreted broadly, meaning that technologies, processes, and practices to protect privacy should be built into the system architecture and not added on later as an afterthought.[128] 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 so as to prevent or minimise the risk of interference with the rights and fundamental freedoms of data subjects.[129]

127 Kuner and Marelli, 2017, p. 84

128 OECD, 2013, p. 104

129 CoE Convention 108+, 2018 (Art. 10)

Box 16 - Data protection impact assessment (DPIA)

What is it? A DPIA 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 in order to anticipate and mitigate risks to data subjects and data controllers.

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

Examples of situations where a DPIA is required or strongly advised by some international and regional data protection and privacy frameworks include:[130]

- When processing data through the use of new technologies
- When processing is used to track people's location or behaviour
- When processing personal data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
- When processing data concerning vulnerable categories of people (e.g. people living in conflict affected countries or socially unstable environments, refugees, internally displaced persons and discriminated minorities, migrants or patients)
- 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 data processing could result in physical harm to the data subject if it is leaked
- When systematically monitoring a publicly accessible place on a large scale
- When the processing involves combining, comparing or matching data from multiple sources
- When the processing uses profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit

130 GDPR 2016/679 (Art. 35) and CoE Convention 108+, 2018 (Art. 10, Explanatory Report, Art. 88); other frameworks, such as the OECD Privacy Framework, 2013 (p. 16) and APEC, 2005 (Art. 44), advise that a privacy risk assessment should be carried out, but do not give details.

Box 17 - Implementing a DPIA

How to implement? There are different approaches to conducting DPIAs. The following guidance draws on good international practices from a range of sources:[131]

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 to or provide a link to other documents, such as a project proposal. Summarise why you have 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 the applicable data protection and privacy frameworks and standards, as well as organisational policies.

Step 3: Describe the processing of personal data: Map the information flows detailing the following (at a minimum):

- The type of data to be collected
- Whether or not sensitive information will be collected
- How the data will be collected
- For what purpose(s) 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 or not personal data will be disclosed
- Whether or not sensitive personal data will be disclosed
- Whether or not any data will be transferred to other organisations or countries

You might find it useful to refer to a flow diagram or other way of describing data flows. Look at what types of processing are involved that are likely to entail high risk?

Step 4: Consultation process: Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals' and stakeholders' views, or justify why it is 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 5: 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?
- How will you ensure data accuracy and data minimisation?
- What information will you give data subjects?
- How will you help to support the rights of data subjects?
- What measures will you take to ensure that processors comply?
- How will you safeguard international data transfers?
- How will you ensure data deletion, also by partners?

Step 6: 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 7: Identify measures to reduce risk: Identify any additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

- Describe the risks
- Options to reduce or eliminate risk
- Effect of measure on risk: eliminated, reduced or accepted
- Residual risk: low, medium or high
- Measure approved: yes/no

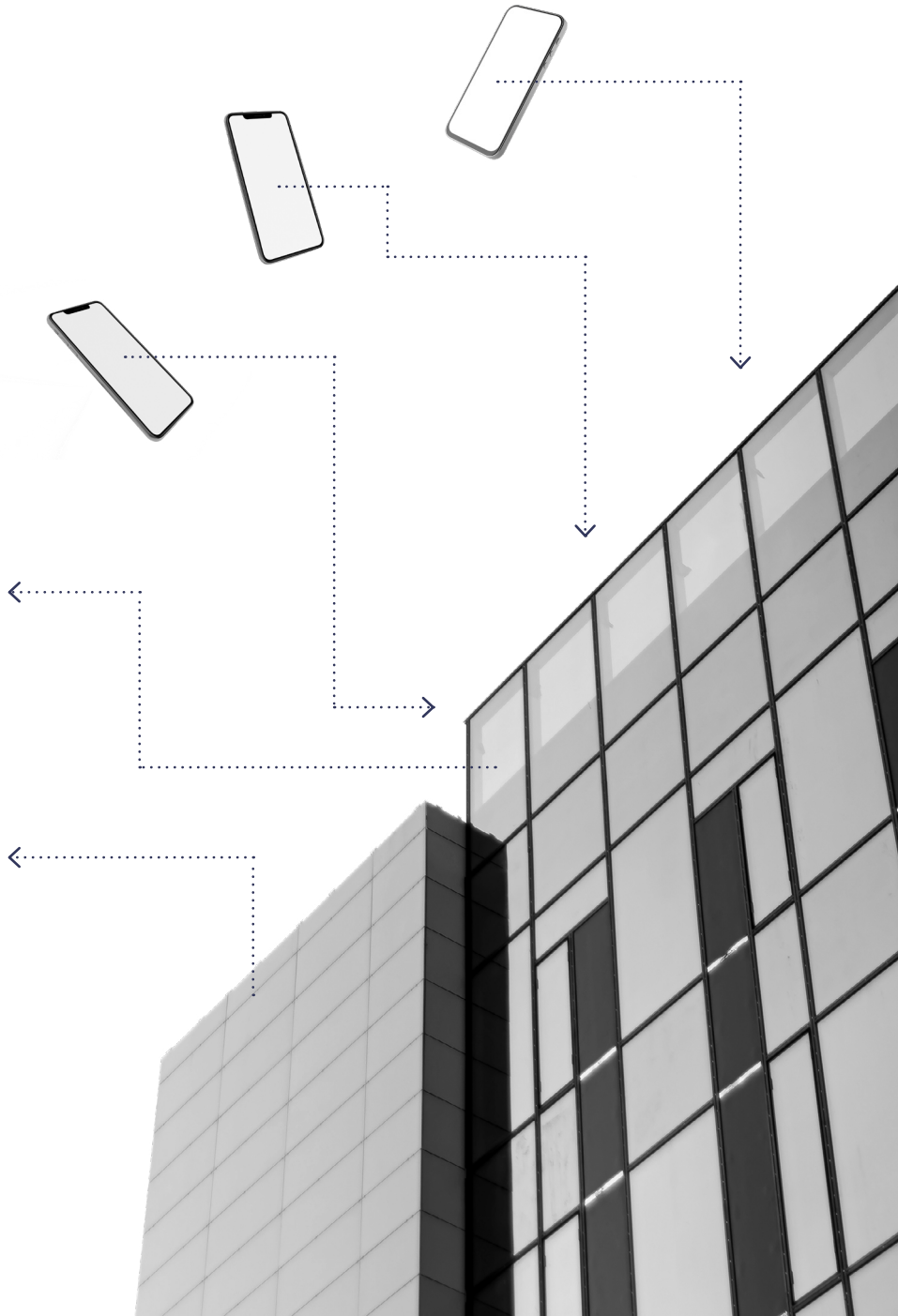
131 Information Commissioner's Office (ICO), Security, n.d.(e), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/; and Kuner and Marelli, 2017, pp. 65–67, 299–305

The Cash Learning Partnership 'Model Privacy Impact Assessment (PIA)' can be used as an example.[132]

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

10.2 HOW DO THE DPIA AND THE DATA MANAGEMENT PROTOCOL RELATE TO EACH OTHER?

The DPIA collects all relevant facts, identifies risks and suggest solutions for risk minimisation with respect to the data processing activities in the context of a new social protection programme. In contrast, the data management protocol, based on the information and solutions in the DPIA, describes how the data processing activities will be implemented. For example, the DPIA may assess the risks involved in distributing 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 banks accomplishing the roles assigned in the social protection programme. 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 the controller's minimum security measures are to ensure secure storage by the bank (list applicable technical and organisational measures), as well as when the bank has to delete the data and how to prove that it has been deleted, among other things. This section in the data management protocol will also be relevant to ensure that the bank (processor) is obliged to comply with the social protection controller's data protection and privacy requirements through the legal agreement.[133]



132 Cash Learning Partnership (CaLP), Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and e-Transfer Programmes, Annex I – Model Privacy Impact Assessment (PIA), 2013, https://www.calpnetwork.org/wp-content/uploads/2020/01/calp-beneficiary-privacy-annexes.pdf

133 See Section 6.1 – Accountability: Legal obligations of data controllers and processors.

CHAPTER 11

HOW TO APPLY DATA PROTECTION AND PRIVACY STANDARDS TO SOCIAL PROTECTION PROGRAMMES

CHAPTER 11. HOW TO APPLY DATA PROTECTION AND PRIVACY STANDARDS TO SOCIAL PROTECTION PROGRAMMES

This chapter provides concrete guidance on how to apply the data protection and privacy standards to social protection programmes through a data management protocol.[134]

11.1 HOW TO LIMIT PROCESSING IN LINE WITH THE DATA PROCESSING PRINCIPLES

11.1.1 For what legitimate purposes do social protection programmes need to collect data?

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 (e.g. provision of financial incentives for low-income families affected by COVID-19).

Box 18 - Checklist of good practices: Purpose specification principle

- ☐ Ensure the purpose specification of data: Personal data should only be collected for a determined, explicit and legitimate purpose, which is stated to the data subject at the time of data collection, with subsequent processing also compatible with this purpose. Any exceptions or deviations should not be allowed, unless permitted by law.

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, as it is not specific enough. 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 data.

Typically, the delivery of a social protection programme (including integration of some of these key phases across multiple programmes) will require different types of data for a range of sub-purposes, namely for:

- **Assessment** of needs and conditions of the affected population (non-personal data)
- **Enrolment** of beneficiaries in social protection programme (purpose of identification/verification)
- **Delivery** of social protection programme (authentication)
- **Reconciliation** of the delivery transactions
- **Monitoring** of social protection programme
- **Complaints and feedback**

The purpose(s) of processing needs to be clarified and communicated to individuals at the time of collection. In addition, social protection programmes need to be aware of the purpose(s) 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 this basis to the data subjects as well.[135]

It may happen that during the delivery of the social protection programme, events occur that require the use of personal data for other purposes than those stated at the time of data collection. For example, a bank is not able to provide 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 or not this processing is compatible with the purpose for which the data were initially collected,[136] the controller should take into account the following, among other things:

- Any link between the original purpose(s) and the purpose(s) 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
- The existence of appropriate safeguards in both the original and intended further processing

134 See Section 9.3 – Data management protocol for a social protection programme.

135 See Section 6.1 – Accountability: Legal obligations of data controllers and processors.

136 On further processing for compatible purposes, see Chapter 4 – Data processing principles.

Box 19 - Purpose specification and integration with other databases

The personal data of recipients or beneficiaries enrolled in a social protection programme are usually stored in a programme specific database (also referred to as a 'beneficiary database'). The information in programme databases is accessed and managed through software applications called programme **management information systems (MIS)** (also referred to as beneficiary operations management system [BOMS]).[137]

These programme-specific MISs can be designed to facilitate integration, interoperability, and ad-hoc data sharing[138] between the data of different programmes, thus allowing these to 'talk to each other'. This may involve using the same identifier, data standards and data formatting/dictionary, so that beneficiaries can be uniquely identified across these databases for the purpose of developing an overview of who receives what and to coordinate interventions, facilitate planning and, more generally, combine monitoring and evaluation across programmes – such as discussed in the context of **integrated beneficiary registries**.[139] Still, the different source databases will contain different data on each individual, depending on the respective programmatic purposes.

Whether the 'overview' database (often operationalised as a 'data warehouse') may **obtain access** to the data from the programme-specific beneficiary database, **without obtaining a new legal basis**, such as consent or public interest, depends on the following:

- Whether or not the integration pursues a **legitimate purpose**, such as assurance that all persons in the beneficiary 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 beneficiary programme shall not double dip in the emergency programme (fraud prevention).
- Whether or not this **purpose is compatible with the purpose** stated to the beneficiaries in the beneficiary database at the time of data collection depends on the facts and should be assessed, as advised in section 11.1.1.

If the new purpose is not compatible, the integration of databases should only occur if provided for by law and if the purpose is legitimate, meaning strictly necessary and proportional to the interference with the data subjects' rights.[140] Data sharing protocols between ministries regulating the integration of the database are often not sufficient.[141]

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, if the 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 Integrated Beneficiary Registry, integrating five programme databases – including one from WFP (called a single registry).[142]

Box 20 - Purpose specification and social registries

Recent trends, mainly driven by the World Bank, encourage the integration of the processes of outreach, intake and registration, and assessment of needs and conditions to determine potential eligibility for one or more social programme in a country via **social registries**.[143] Purpose specification requires that data be collected and used for a specific, explicit and legitimate purpose. The programmatic purpose behind a social registry is to support the process of determining eligibility for multiple programmes, each with its own eligibility criteria and programmatic focus. This is done via the systematic registration – i.e., collection of relevant data

137 See Section 2.2 – Information management in social protection programmes.

138 The extent of this will depend on many factors.

139 Barca and Chirchir, 2014, p. 24

140 "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 Carmona, 2018, p. 28).

141 See Section 11.4 – How to share data.

142 Barca and Chirchir, 2014, p. 25

143 Leite et al., 2017, pp. 66–80; Barca, 2017; also see 'Glossary of defined terms' and Section 2.1. – Social protection and personal data.

– of a large proportion of the population[144] and use of that data to feed into the eligibility determination process of each and every 'user' programme. In many cases, data on potential recipients within social registries is also ranked or grouped into categories based on socio-economic classifications (e.g. income, PMT, or other method). This enables poverty targeting within user-programmes, but does not exclude the use of social registry data for fully universal categorical programmes (e.g. all households with children under five).[145]

Importantly, from a data protection perspective, it may be that detailed and sensitive data about households (often over 100 data variables, although this varies widely depending on user-programme needs) will be stored in a social registry without that household ever being enrolled in any social protection programme.[146] This may include data that is being sourced or cross-validated against other government databases. Thus, it will be important to address how the collection of a large and sensitive dataset (to be stored in the 'social registry') that enables consolidated assessment of needs and conditions across multiple programmes – including, potentially, for programmes that do not yet exist[147] – will be compatible with the specific legitimate purpose principle.[148]

According to good international practices, personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[149] Generally speaking, when the assessment of needs and conditions (as well as other functions) can be conducted based on aggregate or pseudonymised data, this is preferred.[150] Further, consolidated targeting may cause challenges when it fulfils an undefined, imprecise or vague purpose, raising questions about whether or not it may be objectionable[151] for an individual to disclose a wide range of sensitive information about their life and, eventually, not to obtain any assistance.

Whether or not 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 function, considering all circumstances in each instance, including:

- Existing social protection programmes and policies in the given country, including the level of institutionalisation of the registry itself – and its functions – in policies and legislation
- The benefits of such a social registry for the government
- The size of the affected population that would be part of such a registry (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
- The likelihood of the majority of individuals registered in the social registry eventually being enrolled in a social programme (whether routine provision or emergency response) – If such likelihood does not exist, or only in the 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
- The rights, freedoms and interests of the individuals, particularly the right not to allow intrusion into their privacy sphere, unless for specific purposes with 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 that outweigh the disadvantages and justify the interference with the right to data protection and privacy.

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

144 Noting that the coverage of social registries varies widely, from less than 5% of a country's population too almost 100%.

145 Barca, 2017; Leite et al., 2017

146 Note, this may be the case for programme-specific MIS and registries too, although sometimes data on non-enrolled (non-beneficiary) populations are not retained in that case.

147 One important example is the use of social registry data for emergency responses (Barca and Beazley, 2019), including during COVID-19.

148 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 that are not needed for the social registry. This is why the amount of data collection for the social registry is determined by whether or it pursues a legitimate and specific purpose.

149 GDPR 2016/679, Recital 39

150 See Box 24 – The use of pseudonymised data and other forms of encrypted data sharing.

151 CoE Convention 108+ (Explanatory Report, Sec. 48)

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 cross-check beneficiary lists against mandatory sanctions lists, retain metadata for law enforcement purposes or profile beneficiaries for creditworthiness.[152]

Box 21 - 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 the services provided by the programme and the data that it will collect during the course of implementation (transactional data, data obtained through monitoring and complaints), technology has developed in a way that a lot of additional data is collected during 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)
- Timestamp data on the timing of key operations
- Data on the geolocation and movement of individuals tracked by mobile phone operators
- Data on the purchasing behaviour of individuals and, in some cases, their location tracked by retail voucher redemption application providers

If intentionally leveraged, this data may have added value for the government from a data analysis, performance, and monitoring and evaluation perspective. However, such data can also be misused, e.g. for surveillance purposes or by private sector counterparts for their own profit (see, for example, Privacy International's report on *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*[153]). Social protection programmes need to be aware of these additional forms of data collection 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 additional data as part of the services it provides or during the implementation of the programme, or will the service/technology provider collect and use it for its own purposes?
- If the social protection programme obtains additional data, for which purposes will it be used? Additional data can be used to understand beneficiaries better (data analytics), to profile them, but also just to feed technologies for machine learning purposes.[154]
  - Are these separate legitimate purposes, not listed above (in Boxes 19 and 20), about which the individuals were informed?
  - Are the purposes for which the data will be used compatible purposes which do not have to be communicated to the data subjects? This seems 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 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 interest, and whether it is acceptable for the provider to keep the additional data and use it as a controller or 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 or not 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 purposes other than specified at the outset, as well as 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 with the agreement by the commercial service provider.[155]

Any personal data that is not collected for specific and legitimate purposes, or for compatible purposes, may not be processed, as the purpose specification principle would not be fulfilled. An example would be the development of a national identification database, established initially to standardise government databases. However, over time it starts to be used for various other purposes (different and incompatible with the original purpose), from

152 Kuner and Marelli, 2017, p. 153

153 International Committee of the Red Cross (ICRC) and Privacy International, The Humanitarian Metadata Problem: "Doing no Harm" in the Digital Era, October 2018

154 See Section 11.2 – How to ensure that data subjects can exercise their rights.

155 Ibid.

school admissions to obtaining death certificates. The violation of the purpose specification data processing principle should not be 'healed' or bypassed by the fact that the individual provides his or her consent to the processing (with a new purpose) afterwards.[156] The OECD Privacy Framework, however, recognises such an exception, which has often been abused and misused.[157]

11.1.2 What data to process for each purpose and how to minimise data?

Data minimisation works in synchronicity with the purpose specification principle. Information collected in social protection programmes, regardless of the stage, should be the minimum necessary to meet the established purpose(s). For instance, the information collected for a cash or in-kind assistance operation needs to be proportionate to the purpose of carrying out this operation and the minimum necessary. Unnecessary data collection cannot be justified and may increase costs and pose risks for data subjects' rights, in both known and unpredictable ways. The collection of unnecessary data is likely to result in greater pressure to use the data for purposes other than those originally intended and to which the data subject has consented.

Box 22 - Checklist of good practices: Data minimisation principle

- ☐ Ensure data minimisation: Only collect personal data that is adequate, relevant and not excessive to accomplish the purposes established at the time of collection.
- ☐ When requesting personal data, 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 from data subjects.

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

This principle also needs to be analysed from the point of view of frequently fragmented social protection programmes run across several ministries, each collecting their own data – including humanitarian actors operating year-on-year emergency responses. There is a trade-off that requires evaluation between each programme collecting less data, multiple times (invading recipients' privacy each time and asking the same questions again and again) and a once-off national data-collection effort that serves the needs of all (e.g. via a social registry).

156 CoE Convention 108+, 2018 (Art. 5); GDPR 2016/679 (Art. 5)

157 OECD Privacy Framework, 2013, p. 14

Box 23 - Data categories necessary to fulfil data minimisation and purpose specification principles

The list below is a rule of thumb for data categories that can be seen as necessary to fulfil the specific and legitimate purpose(s) specification for implementing a social assistance programme:

Assessment of needs and conditions (will depend on eligibility criteria):

- Detailed socio-economic data (e.g. income, expenditure, household size)
- Food security
- Vulnerability data (e.g. 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 *verification*[158] that the individual is the person they claim 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. fingerprints, iris scan) are collected for the purpose of authentication and avoidance of double-dipping/fraud.[159]
- 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, or a phone number (for a mobile money account). 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).
- A phone number may be needed to *communicate* to beneficiaries that a cash transfer has been completed, the location of a distribution, or other important information regarding the cash delivery.
- If a smartphone application is 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 delivery transactions:

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

Monitoring of social protection programme:

- A phone number or other details may be needed to contact and interview beneficiaries.
- In some cases, data to authenticate beneficiaries may be necessary, however, usually, there is no reason to assume that a non-beneficiary would participate in an interview.
- Information requested from the beneficiary by the monitors may contain personal data (e.g. personal opinions).

Complaints and feedback:

- Data to authenticate caller/beneficiary (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; it can also be sensitive data, such as complaints about harassment.

At the design stage, every social protection programme needs to ask, with respect to each data variable processed throughout the delivery chain, whether or not the respective purpose can be reached without such data variables or with less intrusive data.

158 Identification is the process whereby 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 that the 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, 'Identification vs. Authentication vs. Verification: What are the Differences?', Blog, 2020, https://www.idenfy.com/blog/identification-verification-authentication/).

159 In middle and higher-income countries, registration across several government services is more common, acknowledging the fact that these are complementary (Chirchir, Richard and Valentina Barca, Building an Integrated and Digital Social Protection Information System, Technical Paper, GIZ, Bonn, 2020, p. 36). With respect to biometrics, the need to authenticate beneficiaries and the principle of data minimisation, see Section 12.2. – Data protection and privacy challenges of specific technologies.

Box 24 - The use of pseudonymised data and other forms of encrypted data sharing

Governments, IOs, and NGOs may assess, target and assist overlapping populations. When assessing needs and conditions before setting up a new programme, it may be more effective to request socio-economic and other vulnerability data from these stakeholders than to conduct time consuming and costly new assessments of the population (note, this can be inbuilt via social registries). In this case, applying the data minimisation principle could mean that the sharing entity will provide a pseudonymised list containing all the information relevant for the assessment, 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.[160]

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 must have a legal basis for sharing the data with the receiving controller who envisages another social protection programme (e.g. consent or public interest).
- The parties must enter into a data-sharing agreement.

Importantly, the humanitarian sector has also started experimenting with zero-knowledge proofs (ZKPs) (which are mathematical methods used for verification without sharing or revealing underlying data) and 'hashed' personal data[161] (algorithmically generated encrypted 'hashes'/representations of personal data as proxies for the actual data).

Data minimisation at the data collection stage can be enhanced via on-demand registration, in which applicants apply and register when in need of a particular programme, providing the data required to determine eligibility for that programme alone, instead of census like registrations, in which data is collected as a once-off exercise.[162] This will depend on the awareness and trust of individuals that registration will indeed likely result in enrolment in a social protection programme.

Box 25 - 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 and, therefore, excessive, given that donors neither intend, nor are able, to reach out to all of these beneficiaries to confirm receipt of assistance. Instead, assurance can be obtained by providing anonymised payment lists or reports (deleting identifiers, signatures, thumbprints) and a confirmation by the 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.

160 Unfortunately, sophisticated techniques that allow datasets to be de-anonymised exist (see Box 36 – Erase or anonymise personal data?). A good international practice for sharing public data and ensuring that the data from individuals and individual households remains confidential is to use 'differential privacy' (National Conference of State Legislatures (NCSL), 'Differential Privacy for Census Data Explained', [online], 2021 https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx).

161 "Organisations such as ICRC and Mastercard are exploring approaches that create algorithmically generated encrypted 'hashes' of biometric data – in other words, encrypted representations of personal data are used as proxies for the actual data, with the encryption algorithm being the proprietary technology that ensures data protection and security. Authentication and verification would be carried out by comparing the hashes, not the actual data – using a proprietary algorithm to match the hash presented by the beneficiary against the hash held by the organisation" (SPACE, 2020, p.10).

162 Barca , Valentina and Hebbar, Madhumitha, On-Demand and Up-to-Date? Dynamic Inclusion and Data Updating for Social Assistance, GIZ, 2020

11.1.3 Which legal basis to choose for the social protection programme?

Beneficiaries of social protection programmes should be clearly informed about 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 their data will be held.

Box 26 - 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, in a fair and transparent manner.
- ☐ Ensure transparent and fair information and communication with data subjects by clearly informing them, at the time of data collection, how, why and when their personal data will be processed, both when they have provided this directly to a controller and when 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 subject's consent is informed, given freely 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. When consent cannot be obtained, exceptions should be very limited and applied on an individual case-by-case basis, with heightened levels of transparency, and another legal and legitimate basis for personal data processing is required.
- ☐ Offer data subjects alternatives that allow them to continue to receive assistance should they not provide, or object to the programme's processing of, their personal data, especially in the case of sensitive personal data.

Legal basis[163]

Under the principle of the lawfulness of data processing, a legitimate legal basis is required for personal data processing operations to take place. The social protection controller, namely, the social protection ministry/authority,[164] needs to determine the different legal bases on which it intends to process the data for the respective purposes of the social assistance programme, prior to the collection and 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 typical range of legal bases** (namely, consent, contract with the data subject, legal obligation, public interest, vital interest, legitimate interests),[165] which legal basis should a public authority choose for the implementation of a social protection programme?

- **Processing is 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, under which, 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 or not the national social protection laws oblige the social protection authorities to provide social assistance and under what conditions. The 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.
- **Processing is 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 explicitly oblige* the social protection authority to provide social assistance to legally entitled persons, but still foresee that the social protection authority shall implement certain social protection activities for persons determined to be needy, when there is

163 See Section 4.3 – Lawfulness, fairness and transparency.

164 For a detailed discussion of how IOs should select the legal basis for humanitarian cash and in-kind assistance programmes, see Kuner and Marelli (2017, pp. 59–73). For the selection of the legal basis for projects in which IOs support national social protection programmes as joint controllers or processors, see Box 29 – Legal basis and joint programmes of IOs and social protection authorities.

165 See Section 4.3 – Lawfulness, fairness and transparency.

sufficient budget or in unforeseen situations (such as the provision of emergency assistance to affected populations in the case of natural or manmade disasters). Also, it could be that social protection laws provide for certain activities to be carried out 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.[166] This would cover the respective assessments, enrolment, delivery, reconciliation and monitoring.

- **Processing is necessary in order to protect vital interests:** Data processing may serve both 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.[167]
- **Processing is necessary for a legitimate interest, but not overriding data subject rights and freedoms:** Public authorities may rely on the legal basis of legitimate interest.[168] This mirrors the requirement that authorities may only act on the basis of laws and may not 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 the law provides for this and the respective safeguards are in place.
- **Processing is necessary for the performance of a contract with the data subject is not a legitimate legal basis for the provision of social protection:** This is due to the power differential between social protection providers and recipients, as a result of which social protection recipients may feel compelled to provide their data under a contract, even if they would otherwise not wish to share their data.
- **Consent by the data subject to the processing of data:** Consent by the data subject is the most 'popular' legal basis for the processing of personal data. However, in the context of social protection programmes implemented by public authorities that act on the basis of laws, there is no room for individuals to provide their consent to the processing, if, and 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 must 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 rely on consent?

Although consent could be seen as a more inclusive or empowering legal basis, in most cases, this is not the case. First, even if individuals are asked for their consent, such consent may not be valid given that individuals often have no real choice to refuse to consent due to need and vulnerability. The vast majority of social protection programmes do not offer any alternative assistance for those who do not consent to the processing of their personal data.[169] In this case, asking for consent is not meaningful, unless there are ways to minimise personal data processing.

Second, processing data based on public interest does not mean that individuals cannot dispute the processing of their data. 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.[170] In all cases, the term 'necessary' is to be strictly construed. The data processing needs to be truly necessary, 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 information to the data subject about the data processing (transparency) and to process the data fairly (fairness).**

If the only legal basis that national data protection laws provide for is consent, the reason for this restriction would have to be assessed, including whether the public authorities are

166 CoE Convention 108+, 2018 (Explanatory Report Sec. 47); GDPR 2016/679 (Recital 45)

167 CoE Convention 108+, 2018 (Explanatory Report Sec. 47)

168 GDPR 2016/679 (Art. 6)

169 See Box 28 – Consent: Some specific conditions to be considered valid.

170 See Section 5.5 – Right to withdraw consent and to object to data processing.

subject to the law or whether the law can be interpreted in a way that other legal bases (such as public interest or legal obligation) can be relied upon in addition to consent. In this case, 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, each data processing activity should be assessed in detail in relation to which legal basis it relies on. 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 for the call centre to collect individual consent from each data subject, as the processor on behalf of the social protection authority (the data controller). Monitoring should always be based on public interest or legal obligation, if applicable.

Box 27 - Lawful processing of sensitive data

The conditions under which sensitive data like biometrics, health or disability data can be lawfully used for the implementation of a social protection programme also depends on the manner in which national laws regulate the use of sensitive data. If the use of sensitive data is generally prohibited, as under the GDPR and CoE Convention 108+, no legal basis would be sufficient for such processing. Instead, 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 in the case of social protection laws.[171] In the absence of such a regulation by national law, it is strongly suggested to use sensitive data only if appropriate safeguards are in place. The consent of the data subject alone does not suffice. The use of biometrics should be strongly discouraged in such cases.

If consent is used as a legal basis for a processing activity in the context of the social protection programme, the following should be taken into account (Box 28).

Box 28 - Consent: Some specific conditions to be considered valid

In some international and regional data protection and privacy frameworks,[172] consent needs to fulfil specific conditions to be considered valid. Good international practices require consent 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 when the personal data is collected, or as soon as reasonably practical thereafter.
- **Freely given:** Consent is regarded as freely given if the data subject has the genuine and 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:[173]
  - Characteristics of the data subject, such as illiteracy, disability, age
  - Health status, gender and sexual orientation
  - Location of the data subject, such as a detention facility, resettlement camp, remote area
  - Environmental and other factors, such as unfamiliar surroundings, incomprehensible language or concepts
  - 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 the data subject belongs
  - Complexity of the envisaged processing operation, particularly if complex new technologies are employed

171 See Chapter 8 – Sensitive personal data.

172 GDPR (2016/679); CoE Convention 108+, 2018

173 Kuner and Marelli, 2017, p. 46

- **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.
- **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. In addition, it is important to record any limitations/conditions on the use of their 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 tied to a specific purpose, processing activity and/or 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 may or may 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.

Consent should be given by:

- **Clear affirmative action:** Consent requires an active process by the individual, rather than a passive opt-out process. Mere silence, inactivity or pre-validated forms or boxes do not, therefore, constitute consent.
- **A statement:** Alternatively, consent can be given by an oral or written statement (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, as 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 in relation to 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 operation, due to the scale of the operation, or if the data is obtained from a third party (e.g. an IO)
- The consent cannot be valid because the individual is particularly vulnerable or has no real choice to refuse consent
- Digital technologies are involved and the risks are difficult for data subjects to fully appreciate[174]

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

174 Kuner and Marelli, 2017, p. 58

Box 29 - Legal basis and joint programmes of IOs 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 a controller). IOs often 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 IO's own data protection and privacy framework may overlap and contain deviating requirements.

In the context of national social protection programmes (which differ 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 provided by the law. Public authorities and IOs 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 national laws do not provide for any personal data protection and privacy or contain gaps, IOs 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 IOs data protection and privacy framework, during project design, as part of the data management protocol, and in the legal agreement governing their cooperation.

Transparency[175]

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. It also 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. Information needs to be provided by the controller at the time of data collection and whenever the data is intended to be (lawfully) used for another purpose.

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 suit the data subjects (i.e. in simplified language or in a way that illiterate people can comprehend).

Box 30 - Providing information to enable transparency

Good international practices stipulate that the following information be provided to data subjects:

- 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)
- Upon what legal basis the data will be processed
- The identity of all processors with whom the data is expected to be shared and for what specific purposes (enrolment, data storage, authentication, delivery of cash or food, monitoring)
- How to exercise their rights as data subject (to access, update, correct or delete data or to complain about the data processing, and the right to object or withdraw consent)[176]
- Their right to withhold their data and the implications, particularly any alternatives to obtaining 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), being transparent to the public, the media and civil society organisations about the details of the data processing using such technologies. Accountability would also require publishing the contracts entered into with the technology providers (excluding confidential information like price).

175 See Section 4.3 – Lawfulness, fairness and transparency.

176 See Section 11.2 – How to ensure that data subjects can exercise their rights.

Box 31 - 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 project implementation, may object to the processing of their data. Controllers should try to find out what the specific reason for their 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.

The importance of conducting a DPIA, particularly consultations with the concerned population, can be stressed as a way to prevent these types of problems from the beginning of the programme. 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 easy, and there is no step-by-step procedure 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. Programme designers and implementers 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.

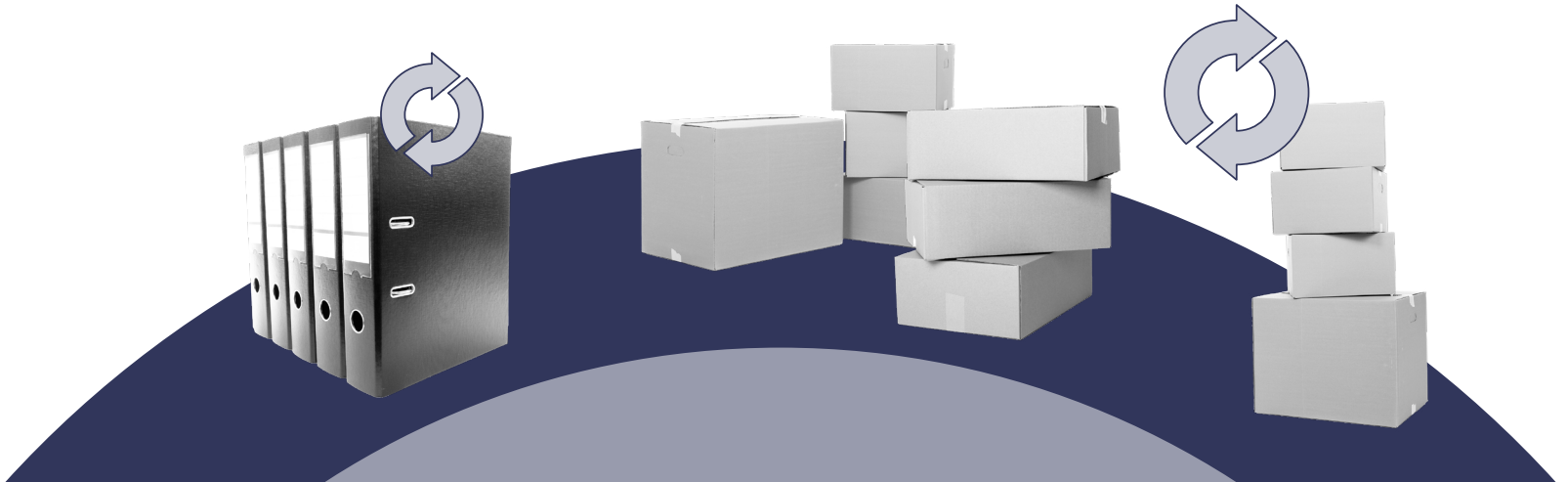
If it is not possible to offer a genuine alternative to individuals receiving assistance, potential beneficiaries need to be informed about the implications of withholding their data.

11.1.4 How and when to ensure the accuracy of personal data?

In different data processing phases (collection, registration, storage, use and sharing) in the social protection delivery chain, personal data should be accurate, complete and, when 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 32 - 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, as complete as possible and, when necessary, 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 and implementing the procedures for that to happen.
- ☐ Conduct regular spot checks on the accuracy and relevance of the personal data recorded.



Box 33 - How to implement the data accuracy principle?

In practice, this means that social protection programmes should:

Plan data accuracy: Before personal information is collected or received:

- Determine the minimum data fields needed for the specified purposes (the less data collected, the easier it is to keep It up-to-date).
- If data is received from third parties, obtain a dataset description (metadata), 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.
- Identify mechanisms for keeping data accurate and up-to-date, for example, through a regular census, integrating databases (e.g. linking data to civil registries, in places where deaths, births, marriages, etc. are registered, considering the privacy implications thereof)[177] and 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 the data collection exercise, if required.

Ensure any information collected is correct and corresponds to reality:

- 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 for proof of residence/address or income/payslip to prove that the ID presented belongs to the person presenting it.

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?

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 data subject's right to rectification).
- Define who is responsible for updating personal data, as well as the procedures and protocols for this to happen.
- Periodically ask individuals to update their details, especially if the information could have serious implications for them.
- Keep an historical record of changes (updates, rectifications, erasures) to data.
- Conduct regular spot checks on the accuracy and relevance of the personal data recorded.

While it is important that personal data is up-to-date, it is not always necessary for all aspects of the data to be up-to-date. How up-to-date the data needs to be depends on the purpose for which the social protection programme is using 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 updating every 3 to 3.5 years is recommended".[178]

The effort to ensure data accuracy should increase according to the importance of having personal data accurate. When personal data is being used to make decisions that may significantly affect the individual concerned or his/her family, social protection programmes need to put more effort into ensuring accuracy.

177 See Section 11.1 – How to limit processing in line with the data processing principles.

178 Irrazaval, 2004, cited in Barca and Chirchir, 2014, p. 39

11.1.5 When to delete data?

Box 34 - Checklist of good practices: Retention limitation principle

- ☐ Ensure application of the retention limitation principle: Personal data should be retained in a form that permits the identification of data subjects for no longer than the time required for the purposes for which such data was originally collected/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 data management protocol.
- ☐ Establish a retention policy and schedules specifying the retention period for all the personal data that is held, determining how it will be subsequently securely deleted from database 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 the request of the data subjects), why and for how long they hold personal data in a form that permits the 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).[179]
- The data needs to be retained for legal or regulatory requirements, such as for income tax, audit purposes or for litigation (legal obligation would be the lawful basis).

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

179 See Box 19 – Purpose specification and integration with other databases.

Box 35 - 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),[180] specifically for personal data, which should include the following:

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

If no such retention policy exists, the social protection programme manager should determine, in the data management protocol,[181] the retention period for all data types processed for the purposes of the social protection programme.

Regarding social registries, as their overall purpose is to target people from a pool of potential recipients, data retention is applicable via established parameters to decide when the targeting is no longer a legitimate purpose. For instance, a parameter could be that if an individual has not been targeted for any social protection programme for ten years, then their data should be deleted. Many programmes include more frequent recertification obligations (e.g. every 2 or 3 years).[182]

180 See Section 9.2 – Organisational data protection and privacy policy.

181 See Section 9.3 – Data management protocol for a social protection programme.

182 Barca and Hebbar, 2020

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

Box 36 - 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 data does not equate to deleting it.

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:[183]

- There is no intention to use or access the data again or to share it with any other organisation.
- Appropriate technical and organisational security measures are used.
- There is commitment to permanently delete the information if, or when, this becomes possible.

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 difficult 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-identify the individuals whose personal data was contained in the dataset rendered anonymous. Thus, the data subjects are no longer anonymous.[184]

Social protection programmes should test the anonymised dataset 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.

11.1.6 How to ensure the security of data processed by social protection programmes?

Box 37 - 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, or entity 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 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 put in place monitoring mechanisms to ensure security safeguards are in place.
- ☐ Ensure that 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

183 Information Commissioner's Office (ICO), Rights Related to Automated Decision Making Including Profiling, n.d.(d), 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/

184 A 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).

national laws, including the data protection and privacy regime, as well as any data localisation laws, and carefully consider the 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 authorised and limited by data protection and privacy laws, regulations, frameworks or internal guidelines, and needs appropriate safeguards.[185]

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:

- **Reviewing existing policies:** In particular, policies relating to information security and the confidentiality of business information, to ensure that personal data is covered and that the physical, technological and organisational measures for the protection of personal data are reflected.[186] Otherwise, update policies. IT policies require information owners to classify information as strictly confidential, confidential, official use, or public and then develop standard security measures related to these classifications. The personal data of beneficiaries should generally be classified as strictly or highly confidential data and enjoy the 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:** It is important to implementation the organisational measures,[187] in particular the training of staff on the most common sources of data security breaches, namely:
  - Keep equipment and paper records secure and inaccessible for unauthorised individuals (in cupboards, lock equipment with passwords whenever leaving the computer, etc.).
  - Do not send personal data files by unsecured email.
  - Keep passwords secure.
- **Guidelines:** Specific guidelines should be developed for social protection programme managers on what security aspects to consider when setting up a social protection programme. Such guidelines would usually be part of the guidelines on how to implement the organisational data protection and privacy policy principles in social protection programmes.

The next step is to put in place security safeguards for the envisaged social protection programme. The social protection manager should ensure the following:

- Involve information security specialists in the DPIA to assess, in line with the technological and physical security measures:
  - The security of servers where personal data is stored
  - The security of the network
  - The security of software processing personal data:
    - The programme database
    - The software application MIS to manage the programme database and automate core business processes
    - The integration of programme databases through integrated MIS – access to both databases should be limited to authorised staff only
  - The security of hardware processing personal data, such as:
    - Tablets for data collection
    - Functional identity cards with pictures or even biometrics
    - Electronic voucher cards
    - Fingerprint readers, in case they store biometrics and other personal data
    - Smartphones used by beneficiaries to access benefits or exercise their privacy rights, to the extent possible
  - The security of data transfer technology (encrypted email, API, clouds with access by data sender and recipient)

185 See Section 12.2 – Data protection and privacy challenges of specific technologies.

186 See Chapter 9 – How to promote and adopt standards for data protection and privacy.

187 See Section 9.2 – Organisational data protection and privacy policy.

  - With respect to any software or hardware provided by a third party, assess the provider's organisation, technological and physical security measures, including:
    - » Location of server where database is stored, including when the clouds of service providers are used
    - » The provider's internal personal data processing system
    - » Any platform for the exchange of beneficiary lists, reports, and other personal data
    - » Any applications for use by data subjects to access their benefits, for example in the case of mobile banking or mobile money
- Implement the 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.
- Regularly assess the risk of the security measures to ensure that they are up-to-date – to be reflected in the data management protocol.
- Reflect any security requirements relating to service providers identified in the DPIA in the contracts with such providers.[188]
- 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. This should 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 by authorised staff of the social protection authority or other authorised users of third parties (service providers, partners) on a need-to-know basis. The biggest threats to the security and integrity of an information system come from authorised users, not from external actors such as hackers.[189] Persons who have been trusted with access may disclose data intentionally or unintentionally (human error). In addition, cultural factors may cause the disclosure of data not deemed to be confidential. This reinforces the importance of setting appropriate operating procedures and training staff on the confidentiality of personal information and data subjects' right to privacy.

Specific procedures should be followed when sharing personal datasets with third parties.[190] 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). Instead, it needs to be asked whether or not there is a **legitimate purpose** that justifies combining different and unrelated personal datasets, thereby interfering more heavily with data subjects' right to privacy.[191]

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, or other economic or social disadvantages. Most breaches occur as a result of human error.

Usually, organisations and authorities have non-personal data specific security incident management plans in place, which cover the handling of security incidents with respect to the 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, including the following:

- 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.
- The specific responsibilities of the respective organisational departments, such as the data protection office/officer, information owner, department where the incident occurred, IT department, communication department, legal department, etc.

188 See Chapter 10 – How to conduct a data protection impact assessment (DPIA) and ensure privacy by design.

189 Inter Agency Social Protection Assessments Partnership (ISPA), CODI. Core Diagnostic Instrument. 'What Matters' Guidance Note, ISPA Tools, 2016, https://ispatools.org/tools/CODI-English.pdf

190 See Section 11.4 – How to share data.

191 See Section 11.1 – How to limit processing in line with the data processing principles.

- The immediate response to a security incident, such as investigation of how the data breach occurred, the scope of the breach, what data is at risk, the immediate mitigation measures, and notification obligations to data protection authority.
- The long-term response to the security incident, public communication (i.e. to the press), review of the legal rights of the controller against processors and/or potential rights of data subjects against the controller, and notification of data subjects.

Box 38 - Breach notification to data protection authority and/or data subjects

The breach notification should include, as a minimum:

- Type of incident and nature of the breach
- Date of the incident
- Cause of breach
- Those affected
- Type of personal data compromised
- Number of people whose data was compromised
- Likely consequences
- Measures taken to address the breach and mitigate any 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.

11.2 HOW TO ENSURE THAT DATA SUBJECTS CAN EXERCISE THEIR RIGHTS

Box 39 - Checklist of good practices: Rights of data subjects

- ☐ Respect, promote and facilitate the exercise of the rights of data subjects.
- ☐ Widely disseminate awareness of the rights of data subjects among organisation 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 collected, with 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 or not to share their personal data.
- ☐ Ensure the right to access and challenge: Enable data subjects to easily obtain (request and be given) confirmation of whether or not a controller is processing personal data concerning them and, when this is the case, access to such data and information about its processing (collection, storage or use). If the request for information is refused, the data subject should have the right to be given the reasons why, and to challenge such denial.
- ☐ Ensure the right to rectify and erase: Data subjects should be allowed to rectify (correct, update or modify) personal data processed about them to ensure that such data is accurate, complete and kept up-to-date. Data subjects should, in certain circumstances, also 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 interest, data subjects should be able to 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 that 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 have the right to not be subject to purely automated decision-making, including profiling, which produces legal or other significant effects for them. Where exemptions allow for solely automated decision-making (including, for example, PMT), 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 the right to an effective remedy: Data subjects should be able to submit a complaint to an independent supervisory authority and to request an effective judicial remedy via the courts when they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law.

When designing and implementing social protection programmes, social protection authorities, development and humanitarian agencies, and social protection practitioners, in general, should take certain steps to ensure that the data subjects' rights are respected, namely: map the data subjects' rights under the applicable frameworks, determine the data subjects' rights under the social protection programme, inform the data subjects about data processing and their rights at time of data collection, allow data subjects to request access, rectify, erase, object to and intervene in automated decision-making during the social protection programme, and ensure that data subjects have the right to submit a complaint to a data protection authority, as well as the right to a judicial remedy. These steps are discussed in the following subsections.

11.2.1 Map data subjects' rights under applicable frameworks

Social protection programmes should map which rights of the data subjects are recognised in:

- The applicable data protection and privacy laws
- The applicable regional or international frameworks
- The organisational data protection and privacy policy to which the data controller is subject

11.2.2 Determine data subjects' rights under the social protection programme

In the absence of such frameworks, the data subject rights under the particular social protection programme should be determined, as per the good practices and standards presented in this Implementation Guide, and shall reflect those in the data management protocol.[192] The rights of data subjects with respect to a social protection programme implemented by a public authority (controller) comprise two different types of rights: rights exercisable against the controller and the right to redress:

Firstly, the rights **exercisable against the controller,** which should include the following:[193]

- 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 can be divided into the rights that are granted at data collection (see 11.2.3) and those that can be asserted during the implementation of the social protection programme (see 11.2.4).

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

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

Given the social nature of data processing, when the person's best interest is the overarching rationale, people's right to object and to data erasure should be, in principle, always preserved, even when the applicable lawful basis is a legal obligation. Specific exceptions to this might be discussed, but people's fundamental right to decide about the use of their data in social protection programmes should, ideally, be ensured.

Secondly, there is the **right to redress,** in cases where the controller did not comply with the above rights, or violated other provisions of the applicable data protection and privacy framework, leading to harm to the data subjects. This right includes the following:

- Right to submit a complaint to an independent body
- Right to an effective judicial remedy, including financial compensation

192 See Section 11.1 – How to limit processing in line with the data processing principles.

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

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

11.2.3 At time of data collection: Inform data subject about data processing and their rights

Data subjects need to be provided with all information necessary for them to make an informed decision about whether or not to share their personal data when applying for a service or benefit. The **data management protocol should provide that the data subject shall be informed** about:

- Data 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 right to submit a complaint to an independent body or to obtain legal redress (in court), and how to avail themselves of these rights
- 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 is given depends on how the data is collected, for example:

- If the data is collected by a census, 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 through diverse means, depending on the circumstances, for example, in a sensitisation session to which data subjects are invited through a text message.

11.2.4 During social protection programme: Allow data subject to request access, rectify, erase, object to and intervene in automated decision-making

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

CFMs can be set-up for an individual social protection programme or cover several programmes in a country, even for various controllers. CFMs are not to be confused with organisation-internal mechanisms to address complaints by a data subject about the processing by a controller.[194] Such complaints should not be accepted by the CFM, but beneficiaries asked to directly contact the respective internal office 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, when a data subject communicates the reason(s) why they wish to withdraw their data. A DPIA should be mandatory when:

- A third-party implements the CFM
- Third-party technology is used to collect, manage, and store the information on data subjects for their identification and their complaint/requests
- Personal data will be shared with other IOs or NGOs, particularly in the case of multi-agency hotlines

The DPIA assesses two broad areas of data protection, namely:

- Whether or not 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

194 See Section 12.1 – Steps for ensuring privacy compliance by technology providers.

privacy standards).[195] The DPIA will serve as a guideline to design the CFM in a data protection compliant way.[196]

- Whether or not the CFM appropriately allows data subjects to exercise their rights (the second pillar of data protection and privacy standards).[197]

Box 40 - CFM call centre: Compliance with data protection principles

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

- How to provide information? For example, on an answering machine, on the details of the data processing, including the legal basis (typically consent), and how to collect consent.
- Which data needs to be collected for which purposes? For example, if the card does not work and the beneficiary requires a new one, the social protection programme needs to check the issue and call the beneficiary back, for which purpose it needs the beneficiary's name, phone number and electronic voucher card number. The beneficiary's name, phone number and detailed information are also needed when a protection case is reported.
- When does personal data not need to be collected? For example, a caller may not require feedback (e.g. if he/she reports that in a given location sacks of rice are rotten or one out of several ATMs does not work).
- How can the call centre operator's access to information be minimised and the abuse of data for different purposes be avoided? For example, a technology can be used that irrevocably closes the window when 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. Another safeguard is a '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 what cases will data be shared with other agencies? For example, if a caller asks to be included in a social protection programme of a different controller (e.g. implemented by a different IO)?
- When will data be deleted? For example, data with respect to technical issues having been resolved may be deleted within a short time frame, but data with respect to protection cases or potential litigation 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 call centre operators.

Following the completion 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.[198]

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

- A clear allocation of responsibilities: If there is a data protection office, all data subject requests should be channelled to, and assessed, by that office. If there is no DPO, the suggested responses to requests by operators should be approved by the programme manager in order to ensure consistent responses; the programme manager should also decide about potentially fraudulent access requests, requests for deletion or objection to processing.
- Processes to inform the data subject about the acceptance or rejection of a request, within a given timeline (set by law or the organisational policy, if not by the data management protocol) and a sound reason.
- How and where to record the data subject requests and their fulfilment/rejection.
- On all rights: How the caller can be verified as a beneficiary of the social protection programme or as a legal representative of the beneficiary with authorisation to access the data (power of attorney); what documentation is acceptable (for example, ID number, birth

195 See Chapter 10 – How to conduct a data protection impact assessment (DPIA) and ensure privacy by design.

196 See Box 16 – Data protection impact assessment (DPIA).

197 See Chapter 5 – Data subject rights.

198 OECD Privacy Framework, 2013

data and address, power of attorney, in case of the representative) and what is not, in order to avoid fraudulent access requests.[199]

- 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 easily accessible for individuals to obtain access and/or a copy, but still secure.
  - 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, this may require public records of births, deaths, marriages).
  - What to do in cases where no proof can be provided (change of address for instance).
  - How to set up processes, ideally automated, to ensure that processors and joint controllers will be informed of the rectification.
- The right to erasure:
  - 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.[200]
  - How to ensure that data is erased within the established retention periods.
  - How to set up processes, ideally automated, to ensure that processors and joint controllers will be informed of the erasure.
- The right to object to the data processing:
  - How to determine whether or not processing needs to continue despite the right to object, namely, in which cases will there be legitimate grounds for the processing that override their interests, rights and fundamental freedoms.[201]

199 Manavis, 2019

200 See Box 31 – What if individuals do not want to provide their personal data or object to the processing?

201 See GDPR 2016/679 (Art. 21).

11.2.5 Right to submit a complaint to a DPA and the 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:

- A complaint form should be available to data subjects (on paper and online).
- The contact information regarding the data protection and privacy authority should be easily accessible to data subjects.
- States should provide a procedure/mechanism for the data subjects to take action against a supervisory authority when it has failed to deal with their complaint.
- Data subjects 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 a public defender free of charge for people without resources to pay for a private lawyer).

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 DPA exists, but the public authority has a DPO or the social protection programme has established a DPO, 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 DATA CONTROLLERS/PROCESSORS/DPA 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, or, if no DPA, then the DPO
Obtain judicial remedy	Controller, processor, DPA	Court, if provided by law

11.3 HOW TO BE AN ACCOUNTABLE SOCIAL PROTECTION CONTROLLER

Box 41 - 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 that personal data protection and the right to privacy are covered, and compliance with the organisational and/or domestically applicable data protection regime.
- ☐ Ensure that a DPIA is undertaken before processing personal data (i.e. before data collection), and define what safeguarding measures will be applied, especially when the processing is likely to pose a high risk to the rights and freedoms of natural persons.
- ☐ Establish clear lines of accountability, under which 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 needs 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 pose a high risk to the rights and freedoms of natural persons, inform the relevant supervisory authority (if one exists) and the affected data subjects about the loss or unauthorised acquisition of their personal data (breach notification) in an appropriate and timely manner.
- ☐ Establish an effective CFM that data subjects are aware of and which they can access to file requests to access, rectify, erase or object to/complain about data processing.
- ☐ Ensure that the CFM includes an independent supervisory authority that has the power to receive complaints, investigate them and apply sanctions (administrative remedy) 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:[202]

- 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.

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** that reflect the data protection and privacy standards.[203] In terms of accountability, such policies should have:

- A clear internal framework of data protection and privacy rights and obligations of data subjects and controllers that can be enforced against them through contractual means
- If established as suggested in this Implementation Guide and permitted under national laws, an external and independent ad-hoc oversight body to which data subjects can submit complaints, otherwise the DPO will assume this task
- Possibility of data subjects obtaining efficient legal redress in court

202 See Chapter 6 – Accountability, oversight and enforcement.

203 See Chapter 3 – Introduction: Data protection and privacy standards and Chapter 6 – Accountability, oversight and enforcement.

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 subjects' rights and freedoms. This is 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 requires a lot of data from vulnerable individuals.

The public authority should establish or appoint a DPO, which acts as the first point of contact for all data protection and privacy concerns in the organisation. In addition, among other things, the DPO may provide guidance on how to conduct a DPIA, implement data subjects' rights, approve international data sharing, and handle sensitive data, as well as lead the response to data security breaches and even support the adoption of the data protection and privacy policy. If there is no external DPA, the DPO can assume the task to monitor compliance with the data protection and privacy policy, if applicable, and assess and decide on complaints by data subjects. In that case, its 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), not through the CFM.

Box 42 - Data protection office or officer (DPO)

A DPO needs to provide tools and guidance for organisations on how to comply with existing data protection and privacy regulations when processing the personal data of any data subjects, such as staff, customers or beneficiaries. A 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, it must perform its function independently. Therefore, organisations should avoid conflicts of interest, and staff of the organisation should not instruct the DPO about its duties. The DPO should manage its own budget and not report to any direct supervisor, be an employee in a contract, or be a data processing controller.

The appointment of a DPO is specified, for instance in the GDPR,[204] which clarifies the requirement of installing a DPO whenever data processing is carried out by a public authority; when the regular and systematic monitoring of individuals on a large scale is necessary during processing; or when the data processed is of a particular category (including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health data or sexual orientation).[205] The CoE Convention 108+ specifies the instalment of a DPO as an obligation of the data controller to ensure personal data protection and privacy.[206] Equally, it is suggested that social protection programmes or development and humanitarian organisations appoint a DPO to ensure the accountability of data controllers, in alignment with data protection and privacy regulations and data security.[207]

Without data protection and privacy laws and organisational policies, there is no accountability, oversight, or enforceability. Data management protocols demonstrate that a controller envisages complying with the data protection and privacy standards set therein. They are, however, not binding on the controller (unless obligations are assumed in contracts, for example, with joint controllers), not examined by any external oversight body, and are not enforceable by data subjects.

11.4 HOW TO SHARE DATA

Box 43 - 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, minimum safeguards established against hackers, and sanctions and redress measures to address successful cyberattacks.

204 GDPR 2016/679, Art. 37

205 GDPR 2016/679, Art. 9

206 CoE Convention 108+, 2018, p. 25

207 Kuner and Marelli, 2017, p. 46

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

- The transfer of personal data from one controller to another, or both ways
- The joint processing of personal data by one or more controllers
- 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 the last point, 'the processing of personal data by a processor on behalf of a controller', has been extensively described in this Implementation Guide.[208] It requires a **data processing agreement.**

The exchange of data between controllers, under the first point, could occur, when a social protection ministry exchanges data with a large NGO acting as controller of social protection datasets and registered in the same jurisdiction, each using the dataset for their own purposes. 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 GDPR does not even require data sharing agreements for this scenario. **International data sharing,** however, may cause a deterioration (or improvement) in the safeguards that the data is subject to when it crosses borders, for example, for the use of a social protection ministry of a neighbouring state or by an IO.[209]

Joint controllers, under the second point, determine the purpose and means of data processing jointly. For example, two IOs implementing a cash transfer jointly: one agency assumes the assessments, targeting and monitoring, the other implements the cash transfers. The GDPR expressly requires a legal agreement for this type of activity.[210] For accountability purposes, it is good practice to establish legal agreements between separate and joint controllers, and data-sharing protocols between government agencies.

Box 44 - Data-sharing agreement between controllers

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

Why is it important? It is important in order 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 understanding of their particular roles and responsibilities
- Outlines what will occur with personal data when received by the other controller
- Establishes rules and procedures, particularly on who and how information about the processing and their rights is provided to data subjects

Box 45 - Establishing a data-sharing agreement between controllers

How to establish? Obtain advice from a legal department/lawyer in order to ensure that the agreement reflects appropriate safeguards depending on the volume and sensitivity of the data that will be transferred between the controllers.

Some suggestions on what to include in the agreement are:[211]

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 broadly

Which other organisations will be involved in data sharing:

- Contact details of the DPO of other organisations and other key members of staff
- Procedures for including additional organisations in the data-sharing arrangement
- Procedures for dealing with cases in which an organisation needs to be excluded from the sharing agreement

What data items are going to be shared:

- Explain in detail the types of data the organisation is intending to share with other organisations.

208 See Chapter 4 – Data processing principles.

209 See Chapter 7 – International data sharing.

210 GDPR 2016/679 (Art. 26)

211 ICO, n.d.(a)

The responsibilities of the controllers:

- Both controllers should be subject to some data protection and privacy 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 (DPO).

Whether or not the data been collected lawfully, for legitimate purposes and is accurate and up-to-date:

- The controller who shares the data shall warrant that it has processed the data in compliance with applicable data protection laws and, in particular, that it has collected only necessary data, lawfully, and for legitimate purposes, and that the data is accurate and up-to-date; if not, the controller will provide information about inaccuracies.

The legal basis for sharing data:

- 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.

Any sensitive personal data:

- The relevant conditions for processing should be documented.

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 for the data processing done by it. And the old controller will remain responsible to respect the data subject rights (such as the right of access to information, right to object, and requests for rectification and erasure) with respect to the processing conducted by it. 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 is 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 should be able to choose to contact any controller.

What happens in case of a data breach happening to one controller?

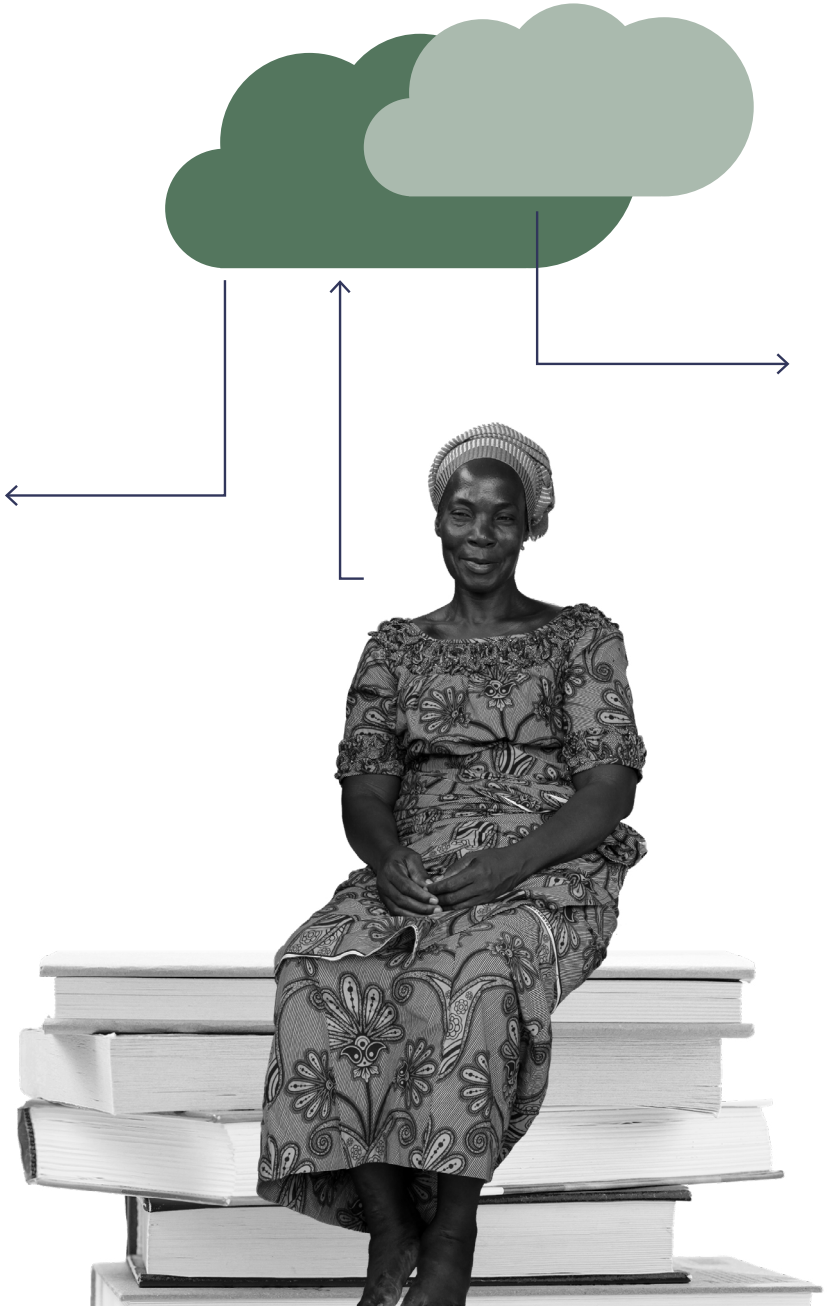
- The agreement should include an indemnity clause to cover the situation when an individual claims compensation for a data breach happening to one of the controllers to cover the controller who has not suffered a data breach.
- If the data subject claims compensation from the controller who has not suffered a data breach, that controller should notify the other controller.

Box 46 - 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.[212] As a consequence, the exchange of personal data between bodies that are part of one legal entity (i.e. controller) – for example, two ministries of the same country – 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 (beyond memorandums of understanding, and so forth). However, public authorities may have a separate legal personality than the state.[213] 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** be agreed upon with basically the same information as relevant for the data sharing agreement, with the following particularities:

- The new purpose(s) 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.
- The controller (the government, represented by the requesting ministry) needs to identify a legal basis for the new purpose(s), unless such a purpose is compatible with the purpose that was stated to individuals at the time of data collection.



212 This needs to be reviewed and confirmed in each country's case by lawyers admitted to practice in the respective jurisdiction.

213 Again, this needs to be reviewed and confirmed by lawyers admitted to practice in the respective jurisdiction.

CHAPTER 12

HOW TO WORK WITH PROVIDERS OF DIGITAL TECHNOLOGY

CHAPTER 12. HOW TO WORK WITH PROVIDERS OF DIGITAL TECHNOLOGY

Technology providers are currently taking on more of the processes involved in the delivery of social protection programmes, which were previously carried out by the social protection data controller. 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 sometimes not stored on local servers, but in the cloud. In another example, some beneficiaries receive their benefits over smartphones and, in the absence of government-issued ID cards, can (or must) identify and authenticate themselves through their fingerprints, iris or using other biometrics.

Cooperation with providers of digital or data-driven technologies, whether cloud-based technologies, technologies allowing for automated decision-making, big data for data analytics, or artificial intelligence, always requires a **comprehensive risk assessment** before any engagement. In addition, agencies must ensure precise and enforceable contracts and close compliance monitoring concerning the best data protection and privacy standards and the observance of other human rights,[214] although the observance of other human rights is beyond the scope of this Implementation Guide.[215]

It is also critical to avoid problems with vendor lock-in in relation to external technology providers. This means not becoming dependent on a single technology provider and, for example, not being able to switch to a different vendor without incurring substantial costs, legal constraints, or technical incompatibilities. It is important to prioritise systems and technologies that can be used independently afterwards. Above all, agreements must allow local staff to be trained in the use (and, where possible, the development) of technologies and systems. The goal of any technological procurement should always be to develop an independent local ecosystem within which local staff and local providers have control over, and are able to make key modifications to, critical systems being used.

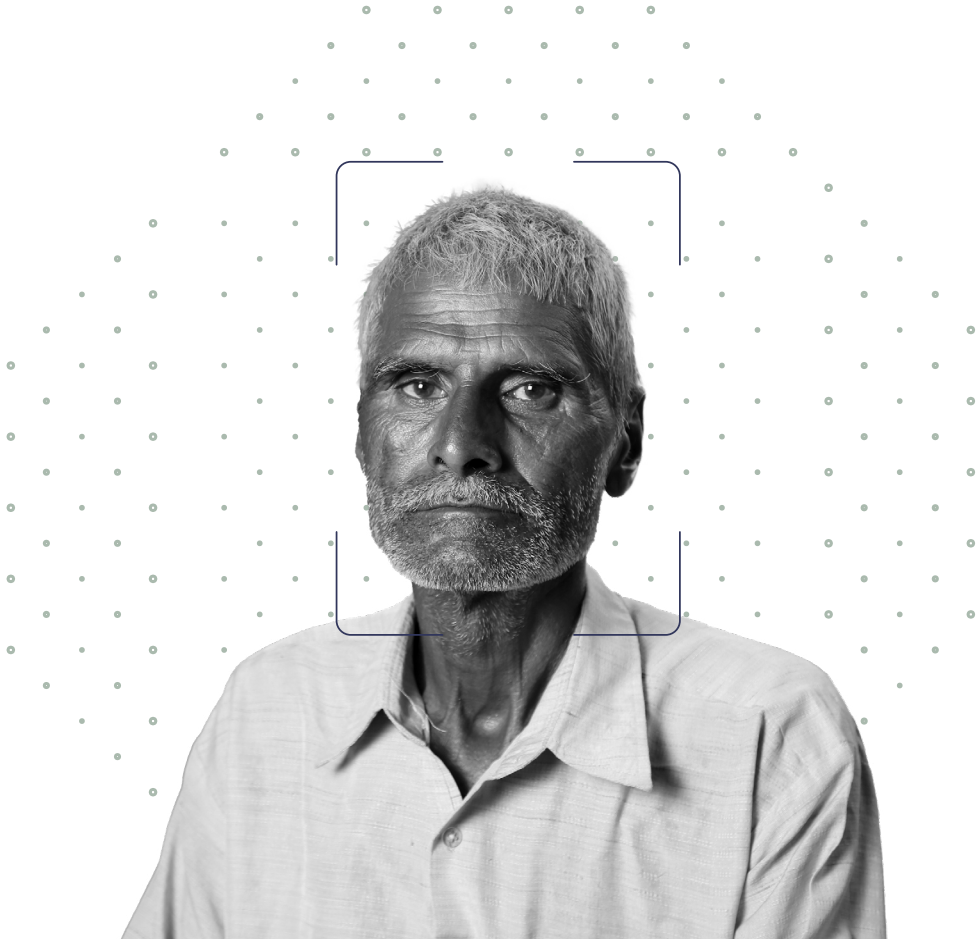
214 Alston, Philip, Extreme Poverty and Human Rights, United Nations General Assembly, 2019, p. 15

215 For further information, see Alston, 2019 and Alston, Philip, The Perilous State of Poverty Eradication, Report of the Special Rapporteur on Extreme Poverty and Human Rights, 2020.

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

12.1 STEPS FOR ENSURING PRIVACY COMPLIANCE BY TECHNOLOGY PROVIDERS

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



12.1.1 During the due diligence phase

The following information should be gathered from the vendor:

- **Data protection and privacy laws** applicable to the vendor and, in the case of cross-border data flows, any international or regional data protection frameworks binding the state in which the vendor is incorporated
- **Legal assessment** on whether or not the laws contain the main elements of data protection and privacy standards presented by this Implementation Guide; if they do not, make suggestions as to:
  - How the processor will achieve accountability and provide evidence, for example, the organisational data protection and privacy policy (including its security incident plan and data retention policy), as well as binding commitments to adhere to the code of conduct approved by supervisory authorities
  - How independent oversight can be obtained, for example, through membership in professional associations that 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
  - Processing and 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 also acts as a controller, for which data, for which purpose(s), and on what legal basis (e.g. when a financial service provider processes beneficiary data to implement cash transfers as a processor, under the law, it also needs to carry out know-your-customer (KYC) checks and, thus, use the data as a controller)
  - Whether or not and how the 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 purpose(s) (e.g. profiling, automated decision-making)
  - Security:
    - » Where is the data stored and through which jurisdictions will it travel?
    - » How is the data secured against data security breaches?
    - » In the case of sensitive data stored in clouds, how could the data be secured against access by the provider without compromising the service (e.g. encryption applied by the controller)?
  - In relation to data retention, how will personal data be deleted from all systems (describe the risk of identification of data subjects following deletion)?
  - Which AI, machine learning or other algorithms, if any, will be used during the data processing?
  - Will a cloud-based service be used?
  - If yes, is the use of the cloud-based service absolutely necessary?
  - Will any biometric data be collected?
  - If yes, is the collection of biometric data collected absolutely necessary?
  - What steps have been taken to mitigate the risk of misuse of biometric data by current and future service providers and public authorities?
- **If technology interfaces with data subjects,** collect 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[216]
- **Audit and/or investigation reports** by DPAs in the last 10 years (including reasons, outcomes, fines, and measures implemented, including adjustments of services/technologies)

216 Alston, 2019, p. 16

- **Detailed information with respect to data security breaches** in the last 10 years (including the cause of the 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)

12.1.2 Put in place a specific process that allows informed decisions to be made weighing all privacy and other risks

- **Assess all information provided through a cross-functional team** representing the DPO 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.**

12.1.3 Award the contract

The awarded contract should include:

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

12.1.4 Monitor compliance

- **Regular audits**
  - Independent audits that ensure that existing systems are in compliance with what has been contractually agreed
- **Security tests**
  - Independent third-party security tests to ensure that existing systems are in compliance with what has been contractually agreed

12.2 DATA PROTECTION AND PRIVACY CHALLENGES OF SPECIFIC TECHNOLOGIES

12.2.1 Cloud-based information systems

Creating a digital and integrated information system is a crucial step in developing a national social protection system.[217] In some cases, these rely on cloud computing and cloud-based solutions.

Box 47 - Checklist of good practices: Cloud-based information systems

- ☐ The data controller should ensure that the use of cloud services complies with the 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.
- ☐ Select 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 signing and ensure that it contains adequate data protection and privacy standards, accountability mechanisms, data security (technical, physical and organisational) measures, confidentiality provisions, and mechanisms that facilitate the exercise of data subject rights.
- ☐ Ensure that the cloud service provider complies with international legal requirements for data sharing.
- ☐ Conduct regular audits of the personal data processing performed by the cloud provider (or the sub-contractors) and of cloud-based storage system security measures.

217 Barca and Chirchir, 2019, p. 5

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 the short term. However, cloud services may also pose additional challenges for data protection and privacy. Among them are lack of transparency about the processing operation and absence of control over the data.[218]

For social protection programmes, the most relevant risks are:

- The use of services from unprotected locations
- The interception of sensitive information
- Weak authentication
- Data being stolen from the cloud service provider (e.g. by hackers)
- Lack of control over data

Box 48 - 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 that manages and operates data storage as a service. Social protection programmes in low- and middle-income countries often lack robust 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 that careful consideration is given to the security controls offered by using cloud technologies. Before deciding to rely on private cloud storage, the data controller is expected to carry out a specific risk assessment. Furthermore, the data controller is responsible for selecting a cloud provider that complies with data protection and privacy principles and legislation and that conducts regular audits and has in place system security measures on cloud-based storage.

Before personal data are stored in a cloud, social protection programmes should:[219]

- Initiate a DPIA on the intended storage in the cloud.
- Conduct due diligence on the cloud service provider to ensure that it takes data protection and privacy into serious consideration.
- Discuss data protection and privacy openly with the cloud service provider and evaluate whether or not it is capable of fulfilling its data protection obligations.
- Carefully review the contract with the cloud service provider before signing and ensure that it contains adequate data protection and privacy standards.

Data protection and privacy standards also apply to cloud services.[220] The relevant data protection and privacy standards and issues in relation to cloud services are as follows:[221]

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 the 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.
- The cloud provider should not act, or be appointed, as a data controller by the social protection provider, as this would mean that the cloud provider would have (joint) responsibility for the data processing, which is not recommended.
- Under the GDPR, the data controller and the cloud provider are directly liable to data subjects for any breaches of data protection that the cloud service provider commits. In some other jurisdictions, only the controller is responsible. Therefore, the contract between them should clearly demand that the cloud provider notify the controller in the event of any data breach that affects the cloud client's data.

218 Kuner and Marelli, 2017, p. 162

219 Kuner and Marelli, 2017, pp. 169–173

220 See Chapter 3 – Introduction: Data protection and privacy standards.

221 Kuner and Marelli, 2017, pp. 165–182

Purpose specification principle:

- The data controller (i.e. cloud client) remains responsible, in cloud computing environments, for determining the purpose(s) of the processing, which needs to be done before any personal data is collected – and data subjects should be informed accordingly.
- The data controller should not further process personal data for a purpose(s) incompatible with the original purpose(s). Consequently, such data processing 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, research for other purposes, profiling, marketing).

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.[222] The law may provide for several legal bases.
- A legal basis is needed for each processing activity. In this case, uploading data into the cloud is a data processing activity that requires a specific lawful basis.
- Therefore, there should be a case-by-case evaluation of each legal ground in every particular situation. This assessment will allow the controller to decide 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. the data controller) must inform the data subjects, before processing personal data, that their data will be stored with, or processed by, a cloud provider.
- A data controller envisioning the engagement of a cloud provider should thoroughly review the provider's terms and conditions and evaluate it from a data protection and privacy perspective.
- The controller needs to inquire about all sub-contractors of the cloud service provider.
- 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.

Retention limitation principle:

- The controller (and its processor, the cloud provider) is responsible to the data subjects to erase their personal data as soon as they are no longer necessary for the processing purpose(s). Therefore, the deletion of data is a crucial concern in a cloud computing contract and upon its termination.
- Each occurrence must be 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 that 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, as well as 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, at a minimum, 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 is 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 from spying and violation during their transmission and, if possible, also when they are 'still'. In these cases, encryption is the standard solution

222 See Section 4.3 – Lawfulness, fairness and transparency.

applied. However, proper attention needs to be paid to determine the correct protocols for the implementation of encryption and the management of secret keys for the encryption itself.

- The physical location of stored data 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 the premises of data centres.
- 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 have the right to access data, to data rectification and erasure, and to object to their personal data being processed in the cloud. Therefore, the social protection data controller should ensure that the cloud provider supports the controller when data subjects exercise these rights.
- 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 usually involve international data sharing of personal data, as the service provider is typically not located in the jurisdiction where it provides the service. It may use sub-processors in (often several) other jurisdictions. Therefore, social protection data controllers should make sure to select cloud service providers that comply with the data protection and privacy laws to which they are subject and, also, with their internal policies.
- The contract between the 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 may identify risks and risk mitigation measures for such personal data processing.

12.2.2 Biometric identification systems

Biometric identification systems include various technologies that use the 'measurement' of physical, psychological or behavioural characteristics (e.g. voice, face, iris) for the authentication or identification of individuals. Biometric identification is becoming increasingly popular. The most common technologies employing biometric data are national IDs and voter IDs.

However, not all biometrics in ID documents are the same. A key differentiator is where the biometric data itself is stored. Some biometric data is stored in a central repository, which is particularly problematic as it can be searched and people profiled based on biometric characteristics. In contrast, biometric data stored on the ID itself is, by design, purpose limited and can only be used as an authentication layer for the ID document itself. This type of decentralised storage of biometric ID data can help prevent misuse.

Box 49 - Checklist of good practices: Biometric identification systems

- ☐ Biometric data should be considered sensitive personal information (not just personal data), meaning that additional security and data protection layers are necessary.
- ☐ Ensure that the free, informed and documented consent of the concerned data subject(s) is obtained.
- ☐ Information should be presented to data subjects describing what biometrics are and why they are risky, and setting out the specific purpose(s) of the processing of their biometric data.
- ☐ Consider the rights of data subjects and inform them about the involvement of third parties, the possible implications of biometric data collection, and the setting up of adequate infrastructure to grant the right to access, objection, deletion and rectification of data.
- ☐ Explicit consent should be the preferred legal basis. Social protection programmes should provide an alternative identification mechanism to people who do not want to release their biometric data.
- ☐ Given the sensitivity of biometric data, implement adequate and proportionate security measures.
- ☐ Collect and process only adequate and relevant data and minimise storage time and the amount of data collected.

- ☐ Ensure the fair and lawful processing of personal data obtained using biometric technology.
- ☐ No biometric database should be generated, but rather data should be stored in data subject token.
- ☐ There should be no sharing of biometrics.
- ☐ Always allow for the withdrawal of consent, the right to object and the right to erasure.
- ☐ Conduct a DPIA to clarify processing details, highlight potential risks and mitigation measures, and determine if biometric data should be collected.
- ☐ Avoid the retention of data for further processing and develop data retention policies.
- ☐ Establish a data retention timeframe (for example, two years from the last assistance received by the beneficiary).

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 the digital processing of data, increased physical protection of individuals, and a lowering of the threshold for bank account acquisition. However, there is systematic information on the use of biometric technologies in social protection programmes and these technologies pose significant risks and challenges, including issues with 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 addition, these risks might include detrimental consequences for individuals, for instance, due to false matches, surveillance, or other abuse.[223]

We believe that the use of biometric technologies should be avoided whenever possible. Biometric technologies are not a panacea for problems with authentication and produce numerous risks and problems when used. For example, one of the most extensive centralised biometric databases globally, which is also used for social protection, exists in Afghanistan.[224] However, August 2021 events in Afghanistan had numerous negative consequences for the database and its beneficiaries. This example demonstrates clearly why centralised biometric databases, and many other uses of biometric technologies, are to be avoided.

223 Kuner and Marelli, 2017, pp. 129–130

224 This report was prepared based on information available as of 31 July 2021. ADB placed on hold its assistance in Afghanistan effective 15 August 2021. ADB Statement on Afghanistan | Asian Development Bank (published on 10 November 2021), Manila

Box 50 - 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, and they can lead to the uncovering of additional information by analysing the biometrics. Such additional information may include diseases, drug use, an individual's emotional state, or genetic inheritance.[225]

Biometrics include the following (non-exhaustive) list of technologies and data:

- **Fingerprints:** Fingerprints 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 are low cost and, thus, widely used in civil and commercial applications.
- **Iris:** Images of the coloured ring surrounding the pupil of the human eye – the iris – are captured through infrared illumination and consist of a complex textured pattern. This pattern is highly individual and very difficult to manipulate or imitate surgically. As a result, many border crossing systems use iris technology for personal identification. However, iris sensors are costly, and their use limited due to the lack of legacy databases for irises.
- **Face:** Facial recognition is an established and successful method of biometric identification. 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.[226]
- **Voice:** Voice and speech recognition systems identify individuals, including behavioural (including the movement of lips, jaw, tongue, etc.) and physiological (including vocal tract, lips, mouth etc.) characteristics. The vocal behavioural traits of an individual may vary and change with age and state of health. Speech recognition is sensitive to background noise and playback spoofing.[227]

225 Sepúlveda Carmona, 2018, pp. 3–4

226 Tistarelli, Massimo; Barrett, Susan E. and O'Toole, Alice J., 'Facial Recognition, Facial Expression and Intention Detection', In: Emilio Mordini and Dimitrios Tzovaras (eds), Second Generation Biometrics: The Ethical, Legal and Social Context, Springer, Dordrecht, 2012, pp. 229–231

227 Jain, Anil K. and Kumar, Ajay, 'Biometric Recognition: An Overview', In: Emilio Mordini and Dimitrios Tzovaras (eds), Second Generation Biometrics: The Ethical, Legal and Social Context, Springer, Dordrecht, 2012, pp. 51–52

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, electroencephalogram,[228] electrocardiogram,[229] transpiration, eye blinking, breathing frequency and trepidation).

Due to the sensitivity of biometrics, the GDPR, for instance, considers biometric data as a special category of data processing that is prohibited unless expressly permitted.[230]

The **data protection and privacy standards** apply to biometric identification systems. The relevant standards and issues are discussed in greater detail in the following:[231]

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 purpose(s) of the data subject's identification.
- In some cases, data might be processed further 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 data subjects' reasonable expectations need to be considered.

Data minimisation:

- Datasets 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, compartmentalising and firewalling data is advisable, rather than pooling data.

Lawfulness, fairness and transparency principle:

- Biometric data should be considered personal data, regulated by the applicable law. Therefore, primary data protection and privacy principles need to be applied when biometric data is collected and processed.
- Data protection and privacy laws 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 the provision of information.
- Several legal bases for the processing of biometric data are relevant to consider the use of these technologies. These include the vital interests of the data subject or another person, public interest, consent, the legitimate interest of the organisation, contractual obligations, or compliance with legal regulations.
- Consent is the preferred legal basis for the processing of personal data, in general, and biometric data processing, in particular, as these are considered sensitive data. Therefore, the data subjects' consent should be obtained if possible. However, 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 difficulty giving informed consent due to the highly complex and technical nature of, and possible unforeseen risks inherent in, the technology. In some cases, an alternative to enable the data subject to participate in a programme might not be provided. Thus, the giving of consent would not be a free choice.

228 Electroencephalogram measures the electrical brain activity and detects abnormalities in an individual's brain waves (John Hopkins Medicine, 'Electroencephalogram (EEG)', [online], n.d.(b), https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/electroencephalogram-eeg).

229 Electrocardiogram measures the electrical activity of the heart (John Hopkins Medicine, 'Electrocardiogram', [online], n.d.(a), https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/electrocardiogram).

230 GDPR 2016/679 (Art. 9)

231 Kuner and Marelli, 2017, pp. 128–141

- Public interest may provide a legal basis for biometric data processing if the organisation cannot obtain the data subject's consent. This 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 and access restriction.
- The data retention policy needs to be developed based on the types of data collected and how they might be used in the future.

Security principle:

- 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 or encryption.
- Creating central databases that include biometric information should be avoided whenever possible.[232]
- 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.[233]
- A DPIA should always be carried out before using biometric data to assess the risks and any possible interference with the data subject's fundamental rights, and to inform the development of mitigation measures.
- A DPIA needs to consider the fact that different types of biometric data have varying degrees of sensitivity. This refers to, for instance, 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 right 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, the possible implications of biometric data collection and the involvement of, and access by, third parties for the implementation of the programme should be communicated to the data subject. If the participation of third parties or the possible consequences change during programme implementation, the data subject's consent needs to be obtained again.
- To enable access, objection, deletion and rectification, organisations need to install adequate mechanisms and infrastructure, including complaint procedures.

International data sharing:

- No biometric data should be shared with third parties, such as external data processors providing biometrics technology or authorities requesting data access.

232 Sepúlveda Carmona, 2018, p. 35

233 Ibid., p. 35

12.2.3 Automated decision-making

Automated data processing techniques, such as algorithms, not only allow Internet users to search and access information quickly, but are also increasingly used in **decision-making processes** that were previously completely under the responsibility of human beings.[234] Algorithms may be used to prepare human decisions or to take them directly through automated means.[235]

Box 51 - Checklist of good practices: Automated decision-making

- ☐ Ensure that 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 individuals' interests, rights, and freedoms should be strictly restricted. For example, automated decision-making has been used to restrict access to programmes that help the unemployed find their way back into the labour market in Austria and to identify fraud (frequently incorrectly), leading to a reduction in benefit payments in Australia and the Netherlands.
- ☐ As a consequence, automated decision-making poses a considerable risk, both to the rights of beneficiaries and the core mission of the social protection providers. This Implementation Guide recommends that fully automated decisions should never be used to determine access to social protection, or the degree or amount of social protection received. Cases in Australia and Sweden have shown that once social protection systems make mistakes of this kind, it becomes nearly impossible to rectify them manually, challenging the very purpose of the social protection system.
- ☐ Having fully acknowledged these concerns and challenges, should social protection providers still wish to implement automated decisions in a limited manner, they should apply them only in exceptional cases, defined by applicable data protection and privacy legislation, and always accompanied by the implementation of adequate safeguards to protect the data subjects' rights, freedoms and legitimate interests. In addition, data subjects should have at least the right to request (in a simple way) and obtain human intervention, express their point of view, and challenge the decision.
- ☐ Social protection providers must ensure that human intervention (oversight of the decision) is meaningful. It should be carried out before the decision applies and be done by someone who has the authority and competence to change the decision. Providers should also carry out regular checks to ensure that social protection data controller systems are working as intended regarding the decision-making process. Furthermore, social protection providers should 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. Finally, providers should ensure, in the case of automated decision-making (including profiling), the provision of meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.
- ☐ Automated decision-making techniques can be used to support unemployed social protection beneficiaries by informing them of skills' trainings they were not previously aware of or opportunities they had previously missed. In doing so, the automated decision-making system needs to be completely honest and transparent about its deficiencies and biases in an easily understandable way so that the beneficiary can meaningfully evaluate the automated advice they are receiving. The final decision on how to respond to this advice should always remain with the beneficiary and not be linked to the provision of other measures or forms of social protection support.
- ☐ In the example mentioned in the previous point, there are likely to be biases and the misrepresentation of skills and opportunities based on the data used and the system's design. These biases could, for example, include discriminatory assumptions about skills or professional ability related to gender. The providers would need to take steps to mitigate these biases, while acknowledging to beneficiaries that they cannot entirely prevent them. They also need to ensure that transparency and accountability mechanisms are integrated into the decision-making process, providing regular audits of the process.

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

235 For more information about algorithms, automated decision-making, including profiling, see 'Glossary of defined terms'.

With the intention of reducing costs, there is a growing usage of automated systems by social protection programmes.[236] Automation can save costs for applicants and beneficiaries, but, at the same time, it may also have data protection and privacy implications and broader negative effects on human rights and social protection. Special concerns arise when considering **automated decision-making** and **profiling** (which can be part of an automated decision-making process).[237]

Box 52 - Potential risks of automated decision-making and profiling

Automated decision-making and profiling can be useful in many sectors (e.g. education, financial services, marketing, etc.) when dealing with large amounts of data. However, if not accompanied by the appropriate risk assessment and safeguards, it can pose 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 associated challenge stems from automated data processing techniques, as they allow for the generation of new data that can be inferred or constructed even if data subjects did not originally provide it. 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 significant issues around notions of consent, transparency and personal autonomy.[238]

Another major concern is related to new data processing methodologies like AI, in which decisions are based on machine learning from a potentially biased dataset. For example, a model trained on data from the United States or the People's Republic of China would only be fully effective when implemented in these contexts. Moreover, any dataset based on human data inherently carries biases that can never be entirely prevented or removed, but only mitigated to a certain degree. Consequently, automated decision-making can produce inaccurate, unfair or discriminatory decisions, making 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 a judge formally makes the final decision, the automated decision made by a programme can be decisive and has led to inaccurate, discriminatory and unfair decisions. The problem stems from the design of the algorithm and the dataset, which have been shown to incorrectly calculate recidivism, i.e. the likelihood of an offender to re-offend, by repeated scientific evaluations. In this context, what is highly problematic is that the incorrect calculation of recidivism is a form of racial discrimination justified by a seemingly objective algorithmic system.[239]

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 and issues such as fairness, transparency, and accountability. At the same time, it is essential to be clear that data protection and privacy safeguards will not prevent incorrect decisions from being made. For example, if a dataset or the system design is biased, this will inevitably happen, regardless of whether or not this is a fair use of personal data. Transparency and accountability safeguards are, thus, critical to ensure that when incorrect decisions are made, they can be rectified swiftly, and appropriate remedies implemented as rapidly as possible.

Which decisions should not be fully automated?

One of the potential risks of using these processing techniques is that decisions may lead to significant adverse effects. Good international practices advise that automated decision-making, including profiling, should be highly limited in these cases, and applied only in limited 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 as to whether or not an individual is entitled to a social protection programme's benefits 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

236 Eubanks, 2011 and 2018

237 See Box 10 - What is automated decision-making and profiling?

238 MSI-NET, 2018

239 Privacy International, 2018

automatically evaluate if an individual is entitled to a benefit and make this decision based solely on automated processing. In this case, a priori, human control must be present to evaluate the decision and ensure it is accurate (semi-automated process). Moreover, the human being must ensure meaningful human control of the automated system, rather than just human beings rubber-stamping the decisions made by an algorithm. Therefore, the 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 this issue, decisions to cut off benefits, or other decisions of a similar serious nature, should not be made based solely on automated decision-making alone (i.e. meaningful human intervention and oversight should be required before such decisions are implemented). Another option would be, in the case where a beneficiary challenges such automated decision, the benefits are reinstated while the challenge is pending. However, harm may still be produce until the beneficiary is able to challenge the decision. Moreover, compensation after the fact is of little comfort to someone who has lost their home, for instance, while working their way through the process.

Box 53 - The 'SyRI case'

The District Court in 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.[240] As part of the SyRI case, an automated system was used to identify benefit fraud, often incorrectly. This automated system used numerous variables, including one based on nationality, with the assumption that holders of multiple passports were more likely to commit fraud. The resulting discriminatory decisions by SyRI were challenged in court, but were considered legitimate decisions by Dutch courts for many years.

The automated decisions incorrectly claiming fraud mainly affected marginalised groups in the Netherlands, as they were made about individuals who were not, or not solely, Dutch nationals. Benefit claimants subject to these decisions were being legally required to repay large sums of money, often facing financial ruin and losing their homes and livelihoods in the process. The SyRI system led to the children of claimants who were incorrectly determine to be guilty of tax fraud being removed from their families in 1,115 cases.[241]

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".[242] 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 about the grave risk of "stumbling, zombie-like, into a digital welfare dystopia".[243]

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 could have a **significant adverse effect** on individuals.

240 Privacy International, The SyRI Case: A Landmark Ruling for Benefits Claimants Around the World, 2020

241 NL Times, 'Over 1,100 Children Taken from Homes of Benefits Scandal Victims', [online], 2021, https://nltimes.nl/2021/10/19/1100-children-taken-homes-benefits-scandal-victims

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

243 United Nations Office of the High Commissioner for Human Rights (UNOHCHR), 'World Stumbling Zombie-Like into a Digital Welfare Dystopia, Warns UN Human Rights Expert', [online], OHCHR News Events, 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156

If the answer is no,[244] then good international practices stipulate that 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.
- Put processes in place so that people can exercise their rights, e.g. to information (details of the information used to create their profile), to object to profiling, to access and rectify their personal data, and, if applicable, to erase personal data.
- Have additional checks in place for profiling and automated decision-making systems to protect members of vulnerable groups (including children) from negative effects on their human rights stemming, both directly and indirectly, from the automated decision-making systems.
- 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.
- Carry out a DPIA to consider and address the risks before starting 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.

If, yes, then good international practices stipulate that 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 show what measures it has in place to meet the applicable legislation requirements. As part of the 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 for 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 about the use of automated decision-making processes, including profiling (what information is used, why it is used, and the effects).
- Ensure meaningful information about the logic involved in the decision-making process and the significance and the envisaged consequences of such processing for the data subject.
- Set up a simple way for people to ask for an automated decision to be reconsidered.
- 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, the following are advisable:

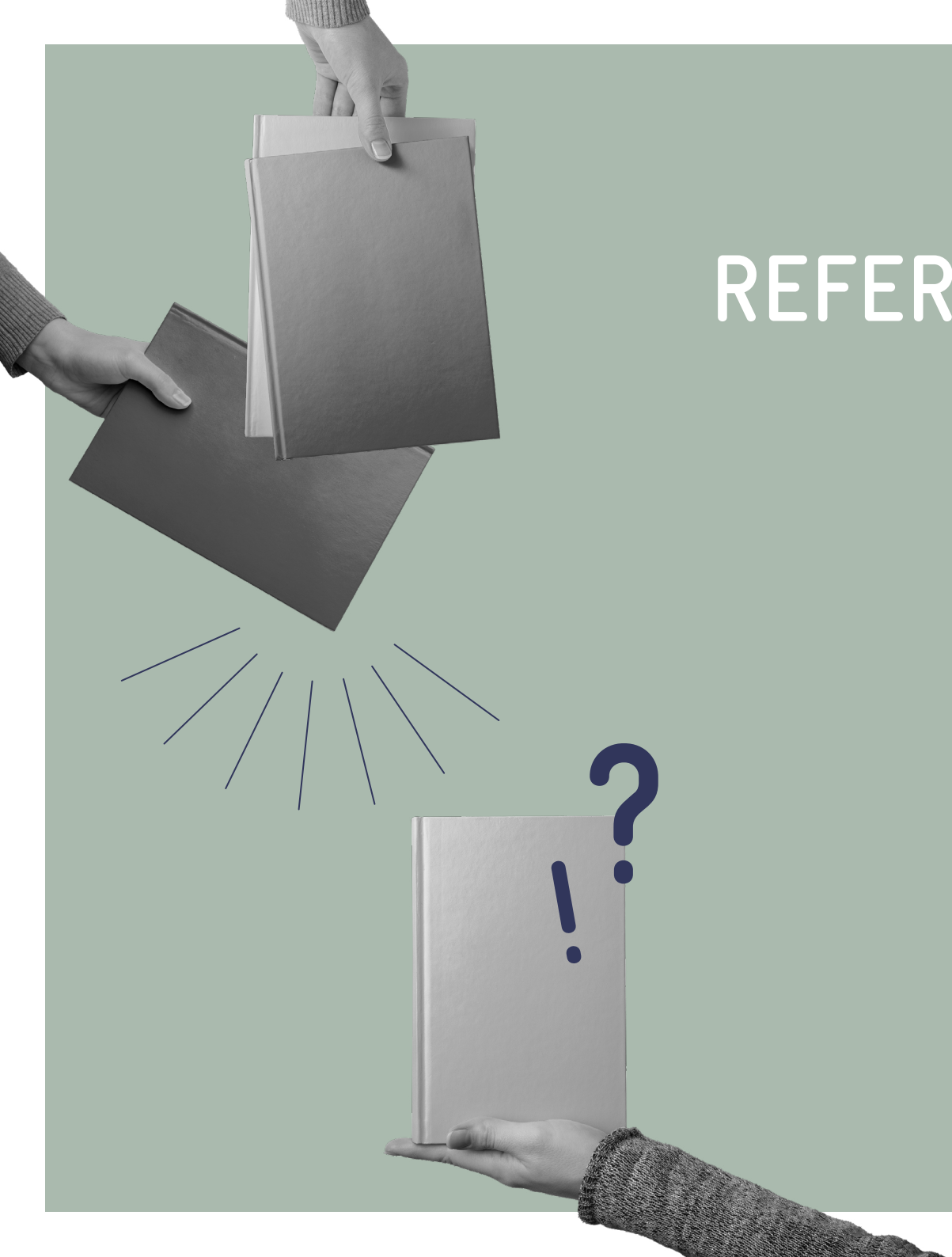
- Use visuals to explain what information is collected and used and why this is relevant to the process.
- Sign up to a set of ethical principles to build trust with data subjects.
- Data subjects should have at least the right to request (in a simple way) and obtain human intervention, express their point of view, and challenge the decision. In order 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 should be done by someone who has the authority and competence to change the decision. [245]

Finally, social protection authorities (data controllers) should carry out regular checks to ensure that their systems are working as intended regarding the decision-making process.

244 Information Commissioner's Office (ICO), Rights Related to Automated Decision Making Including Profiling, n.d.(d), 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/

245 Article 29, Working Party, 2018 (p. 21)

REFERENCES



REFERENCES

- African Union, *Convention on Cyber Security and Personal Data Protection*, Malabo Convention, African Union, 2014, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 23 September 2021)
- Alston, Philip, *Extreme Poverty and Human Rights*, United Nations General Assembly, 2019, https://digitallibrary.un.org/record/1648309 (accessed 16 September 2021)
- Alston, Philip, *The Perilous State of Poverty Eradication*, Report of the Special Rapporteur on Extreme Poverty and Human Rights, 2020, https://chrgj.org/wp-content/uploads/2020/07/Alston-Poverty-Report-FINAL.pdf (accessed 16 September 2021)
- Amici, Marco and Cepiku, Denita, 'Roles, Types, and Definitions of International Organizations', In: Marco Amici and Denita Cepiku (eds), *Performance Management in International Organizations*, Springer, Dordrecht, 2020, pp. 7–40
- Asia-Pacific Economic Cooperation (APEC), *Privacy Framework*, APEC Secretariat, Singapore, 2005, https://www.apec.org/publications/2005/12/apec-privacy-framework (accessed 16 September 2021)
- Barca, Valentina, *Integrating Data and Information Management for Social Protection Social Registries and Integrated Beneficiary Registries*, Commonwealth of Australia, Department of Foreign Affairs and Trade, Canberra, 2017, https://www.dfat.gov.au/sites/default/files/integrating-data-information-management-social-protection-full.pdf
- Barca, Valentina and Beazley, Rodolfo, *Building on Government Systems for Shock Preparedness and Response: The Role of Social Assistance Data and Information Systems*, DFAT, Canberra, 2019
- Barca, Valentina and Chirchir, Richard, *Single Registries and Integrated MISs; De-Mystifying Data and Information Management Concepts*, DFAT, Canberra, 2014, https://www.opml.co.uk/files/2018-05/barca-chirchir-2014-data-information-management-social-protection.pdf?noredirect=1 (accessed 5 September 2021)
- Barca, Valentina and Chirchir, Richard, *Building an Integrated and Digital Social Protection Information System*, GIZ, 2019, https://www.giz.de/en/downloads/giz2019-en-integrated-digital-social-protection-information-system.pdf (accessed 16 September 2021)
- Barca, Valentina and Hebbar, Madhumitha, *On-Demand and Up-to-Date? Dynamic Inclusion and Data Updating for Social Assistance*, GIZ, 2020, https://socialprotection.org/sites/default/files/publications_files/GIZ_DataUpdatingForSocialAssistance_3.pdf
- Black, John; Hashimzade, Nigar and Myles, Gareth, *Oxford Dictionary of Economics*, Oxford University Press, Oxford, 2017
- Cash Learning Partnership (CaLP), *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and e-Transfer Programmes*, Annex I - Model Privacy Impact Assessment (PIA), 2013, https://www.calpnetwork.org/wp-content/uploads/2020/01/calp-beneficiary-privacy-annexes.pdf (accessed 3 February 2022)
- Castelluccia, Claude and Le Métayer, Daniel, *Understanding Algorithmic Decision-Making: Opportunities and Challenges*, European Parliamentary Research Service, Scientific Foresight Union, Brussels, 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624261/EPRS_STU(2019)624261_EN.pdf (accessed 16 November 2021)
- Chirchir, Richard and Barca, Valentina, *Building an Integrated and Digital Social Protection Information System*, Technical Paper, GIZ, Bonn, 2020, https://socialprotection.org/sites/default/files/publications_files/GIZ_DFID_IIMS%20in%20social%20protection_long_02-2020.pdf (accessed July 2021)
- Chirchir, Richard and Farooq, Shez, 'Single Registries and Social Registries: Clarifying the Terminological Confusion', *Pathways' Perspectives on Social Policy in International Development*, Issue No 23, 2016, https://www.developmentpathways.co.uk/wp-content/uploads/2016/11/Single-and-Social-Registries-1.pdf (accessed 18 November 2021)
- Council of Europe (COE), *Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data*, Council of Europe, 2018, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf (accessed 5 September 2021)
- Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), *Data Protection for Social Protection: Key Issues for Low- and Middle-Income Countries*, GIZ, 2020, https://socialprotection.org/sites/default/files/publications_files/GIZ_Data_Protection_For_Social_Protection.pdf (accessed 5 March 2021)

- Economic Community of West African States (ECOWAS), *Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS*, Abuja, 2010, https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf (accessed 5 September 2021)
- Eubanks, Virginia, *Digital Dead End. Fighting for Social Justice in the Information Age*, The MIT Press, Cambridge, MA, 2011
- Eubanks, Virginia, *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*, St Martin's Press, New York, 2018
- European Commission, *Guidelines for Identifying a Controller or Processor's Lead Supervisory Authority*, 16/EN WP 244 rev.01, Article 29 Working Party, 2017 https://ec.europa.eu/newsroom/article29/items/611235 (accessed 16 November 2021)
- European Commission, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, WP251rev.01, Article 29 Working Party, 2018, https://ec.europa.eu/newsroom/article29/items/612053/en (accessed 16 November 2021)
- European Data Protection Supervisor, 'Data Protection Officer (DPO)' [online], n.d., https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en (accessed 19 September 2021)
- European Parliament and Council of European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*, Official Journal of the European Union L119/1, 4 May 2016, pp. 1–88, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (accessed 18 February 2022)
- European Union Agency for Fundamental Rights (FRA), *Handbook on European Data Protection Law*, 2018, https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (accessed 6 August 2021)
- Global Partner Digital, *Travel Guide to the Digital World: Data Protection for Human Rights Defenders*, 2018, https://www.gp-digital.org/wp-content/uploads/2018/07/travelguidetodataprotection.pdf (accessed 10 February 2021)
- Henley, John and Booth, Robert, 'Welfare Surveillance System Violates Human Rights, Dutch Court Rules', *The Guardian*, 5 February 2020, https://www.theguardian.com/technology/2020/feb/05/welfare-surveillance-system-violates-human-rights-dutch-court-rules (accessed 20 February 2021)
- iDenfy, 'Identification vs. Authentication vs. Verification: What are the Differences?', Blog, 2020, https://www.idenfy.com/blog/identification-verification-authentication/ (accessed 9 September 2021)
- Information Commissioner's Office (ICO), *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, United Kingdom, n.d.(a), https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (accessed 16 November 2021)
- Information Commissioner's Office (ICO), *Data Sharing Code of Practice*, Draft Code for Consultation, n.d.(b), https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf (accessed 16 September 2021)
- Information Commissioner's Office (ICO), *Deleting Personal Data*, n.d.(c), https://ico.org.uk/media/for-organisations/documents/1475/deleting_personal_data.pdf (accessed 9 September 2021)
- Information Commissioner's Office (ICO), *Rights Related to Automated Decision Making including profiling*, n.d.(d), 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/ (accessed 18 September 2021)
- Information Commissioner's Office (ICO), *Security*, n.d.(e), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ (accessed 8 September 2021)
- Information Commissioner's Office (ICO), *Sample DPIA Template*, n.d.(f), https://ico.org.uk/media/2258461/dpia-template-v04-post-comms-review-20180308.pdf (accessed 9 September 2021)
- International Committee of the Red Cross (ICRC) and Privacy International, *The Humanitarian Metadata Problem: "Doing no Harm" in the Digital Era*, October 2018
- International Labour Organization (ILO), 'Introduction: Social Transfers', [online], 2018, https://www.social-protection.org/gimi/gess/ShowTheme.action?id=11 (accessed 23 September 2021)
- Inter Agency Social Protection Assessments Partnership (ISPA), *CODI. Core Diagnostic Instrument. 'What Matters' Guidance Note*, ISPA Tools, 2016, https://ispatools.org/tools/CODI-English.pdf (accessed 5 April 2021)

- 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: Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, Dordrecht, 2012, pp. 105–129
- Jain, Anil K. and Kumar, Ajay, 'Biometric Recognition: An Overview', In: Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, Dordrecht, 2012, pp. 49–81
- John Hopkins Medicine, 'Electrocardiogram', [online], n.d.(a), https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/electrocardiogram (accessed 17 November 2021)
- John Hopkins Medicine, 'Electroencephalogram (EEG)', [online], n.d.(b), https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/electroencephalogram-eeg (accessed 16 November 2021)
- 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, *Social Registries for Social Assistance and Beyond: A Guidance Note & Assessment Tool*, Discussion Paper 1704, World Bank, Washington, DC, 2017, https://openknowledge.worldbank.org/handle/10986/28284 (accessed 23 September 2021)
- Lindert, Kathy; Karippacheril, Tina George; Rodriguez Caillava, Inés and Nishikawa Chavez, Kenichi, *Sourcebook on the Foundations of Social Protection Delivery Systems*, World Bank, Washington, DC, 2020, https://openknowledge.worldbank.org/handle/10986/34044 (accessed 15 September 2021)
- 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, https://www.newstatesman.com/science-tech/2019/09/gdpr-easier-access-data-hackers-access-online-security-spotify (accessed 9 September 2021)
- MSI-NET, *Algorithms and Human Rights: Study on the Human Rights Dimensions of Automated Data Processing Techniques and Possible Regulatory Implications*, Prepared by the Committee of Experts on Internet Intermediaries (MSI-NET), DGI (2017)12, Council of Europe, Strasbourg, 2018
- National Conference of State Legislatures (NCSL), 'Differential Privacy for Census Data Explained', [online], 2021 https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx (accessed 9 September 2021)
- National Consultative Ethics Committee for Health and Life Sciences, *Opinion N° 98. Biometrics, Identifying Data and Human Rights*, 2007, http://assets.comitedebioetica.es/files/documentacion/biometric_identifying_data_and_human_rights.pdf (accessed 19 September 2021)
- NL Times, 'Over 1,100 Children Taken from Homes of Benefits Scandal Victims', [online], 2021, https://nltimes.nl/2021/10/19/1100-children-taken-homes-benefits-scandal-victims (accessed 18 November 2021)
- Organisation for Economic Co-operation and Development (OECD), *The OECD Privacy Framework, Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*, 1980, as amended in 2013, OECD Publishing, 2013, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed 9 September 2021)
- Privacy International, *The Keys to Data Protection: A Guide for Policy Engagement on Data Protection*, 2018, https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf (accessed 9 September 2021)
- Privacy International, *Privacy, a Precondition for Social Protection*, 2019, https://privacyinternational.org/news-analysis/3029/privacy-precondition-social-protection (accessed 9 September 2021)
- Privacy International, *The SyRI Case: A Landmark Ruling for Benefits Claimants Around the World*, 2020, https://privacyinternational.org/news-analysis/3363/syri-case-landmark-ruling-benefits-claimants-around-world (accessed 9 September 2021)
- Rennie, Richard and Law, Jonathan, *A Dictionary of Physics*, Oxford University Press, Oxford, 2019
- Russell, Stuart and Norvig, Peter, *Artificial Intelligence. A Modern Approach*, Fourth Edition, Pearson, Hoboken, NJ, 2021
- Sepúlveda Carmona, Magdalena, *Is Biometric Technology in Social Protection Programmes Illegal or Arbitrary? An Analysis of Privacy and Data Protection*, Extension of Social Security (ESS), Working Paper No. 59, International Labour Organization, Geneva, 2018, https://www.social-protection.org/gimi/RessourcePDF.action?ressource.ressourceId=55133 (accessed 9 September 2021)
- Social Protection Approaches to COVID-19: Expert Advice Helpline (SPACE), *Linking Humanitarian & Social Protection Information Systems in the COVID-19*

Response and Beyond, August 2020, https://reliefweb.int/sites/reliefweb.int/files/resources/SPACE_Information%20Systems%20in%20the%20COVID-19%20Response_v1_0.pdf (accessed 5 February 2021)

- Social Protection Inter-agency Cooperation Board (SPIAC-B), 'What is the Social Protection Inter-Agency Cooperation Board?', [online], n.d.(a), https://www.ilo.org/global/docs/WCMS_301456/lang--en/index.htm (accessed 8 September 2021)
- Social Protection Inter-agency Cooperation Board (SPIAC-B), 'Social Protection to Promote Gender Equality and Women's and Girls' Empowerment', [online], n.d.(b), https://www.ilo.org/wcmsp5/groups/public/@dgreports/@nylo/documents/genericdocument/wcms_674612.pdf (accessed 23 September 2021)
- Tistarelli, Massimo; Barrett, Susan E. and O'Toole, Alice J., 'Facial Recognition, Facial Expression and Intention Detection', In: Emilio Mordini and Dimitrios Tzovaras (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context*, Springer, Dordrecht, 2012, pp. 229–257
- University College London (UCL), 'Anonymisation and Pseudonymisation', [online], n.d., https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and (accessed 15 November 2021)
- United Nations, *Universal Declaration of Human Rights*, United Nations, 2015, https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf (accessed 5 September 2021)
- United Nations, *Personal Data Protection and Privacy Principles*, United Nations, 2018, https://unsceb.org/sites/default/files/imported_files/UN-Principles-on-Personal-Data-Protection-Privacy-2018_0.pdf (accessed 23 September 2021)
- UN General Assembly, *Guidelines for the Regulation of Computerised Personal Data Files*, Adopted by General Assembly resolution 45/95 of 14 December 1990, United Nations, 1990
- UN General Assembly, *Vienna Declaration and Programme of Action*, 12 July 1993, A/CONF.157/23, United Nations, 1993, https://www.refworld.org/docid/3ae6b39ec.html (accessed 14 April 2021)
- UN General Assembly, *Resolution Adopted by the General Assembly on 17 December 2018, 73/179. The Right to Privacy in the Digital Age*, United Nations, 2018, https://undocs.org/pdf?symbol=en/A/RES/73/179 (accessed 8 September 2021)
- UN General Assembly, *Resolution Adopted by the General Assembly on 26 September 2019, 52/15, The Right to Privacy in the Digital Age*, United Nations, 2019, https://digitallibrary.un.org/record/3837297?ln=en (accessed 8 September 2021)
- UN General Assembly, *Resolution Adopted by the General Assembly on 16 December 2020, 75/176. The Right to Privacy in the Digital Age*, United Nations, 2020, https://digitallibrary.un.org/record/3896430?ln=en (accessed 8 September 2021)
- United Nations Office of the High Commissioner for Human Rights (UNOHCHR), 'World Stumbling Zombie-Like into a Digital Welfare Dystopia, Warns UN Human Rights Expert', [online], OHCHR News Events, 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156 (accessed 5 September 2021)
- World Bank, *Resilience, Equity, and Opportunity. The World Bank's Social Protection and Labor Strategy 2012–2022*, World Bank, Washington, DC, 2012, https://documents.worldbank.org/pt/publication/documents-reports/documentdetail/443791468157506768/resilience-equity-and-opportunity-the-world-banks-social-protection-and-labor-strategy-2012-2022 (accessed 23 September 2021)
- World Bank Group, *PMT-bases Social Registries. Measuring Income and Poverty using Proxy Means Tests*, Social Protection & Labor team, Dhaka, Bangladesh, n.d., https://olc.worldbank.org/sites/default/files/1.pdf (accessed 17 February 2022)
- World Food Programme (WFP), *Two Minutes on Social Protection*, WFP, 2017, https://documents.wfp.org/stellent/groups/public/documents/communications/wfp277442.pdf?_ga=2.82500497.681773780.1592505793-2117718756.1590495840 (accessed 23 August 2021)

LIST OF BOXES

LIST OF BOXES

DEFINITIONS AND EXPLANATIONS

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 a personal nature (such as their body, family, home, correspondence, property, thoughts, feelings, personal information) or unlawful attacks on their honour and reputation. This right is enshrined in most international and regional human rights treaties and conventions, widely ratified by nation states, and enshrined in national constitutions.

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. Through the following instruments, states are called upon to respect such rights and create laws that 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

Box 2 - A word on terminology

In this Implementation Guide the term **'data protection and privacy'** will be used to refer to the appropriate and permissioned use, governance, and protection of personal data. 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 interchangeably and other times as different concepts.

The term **'data protection and privacy frameworks'** is used in this Implementation Guide to refer to the set of standards (whether incorporated in laws, treaties, or non-binding principles or guidelines) that 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 in this Implementation Guide.[1]

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

Data protection guidelines and principles by IOs (non-binding)

- OECD, *The OECD Privacy Framework, Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data*, 1980, as amended in 2013
- UN General Assembly, *Guidelines for the Regulation of Computerised Personal Data Files*, 1990 – addresses UN member states and governmental IOs
- UN, *Personal Data Protection and Privacy Principles*, 2018 – issued by the High-Level Management Committee of the United Nations, addresses only UN organisations

1 See Chapter 3 – Introduction: Data protection and privacy standards.

International and regional data protection treaties between states (binding)

- CoE, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108)*, 1981, as amended in 2018 (Convention 108+)
- ECOWAS, *Supplementary Act on Personal Data Protection within ECOWAS*, 2010
- AU, *Convention on Cyber Security and Personal Data Protection* (Malabo Convention), 2014 – not yet in force, as only 8 out of the minimum 15 states have ratified it

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

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

Some development and humanitarian agencies are what are called **international organisations (IOs)**, which operate according to their own charter and rules and are governed by international law. Others are so-called **non-governmental organisations (NGOs),** which are subject to national laws.[2]

NGOs (international and national) are under the jurisdiction of the country in which they operate and need to comply with the applicable laws. What data protection rules apply to them is not dealt with by this Implementation Guide, as this depends on the respective laws and factual circumstances in their country of operation. Instead, this Implementation Guide describes good practices regarding personal data protection and privacy, and suggests their application by NGOs, without prejudice to national laws.

IOs are governed by public international law and include organisations like the United Nations and the World Bank. Their operation in a country is based on an agreement with the host government, by which they may implement **humanitarian and development aid** projects, often integrating the host government social protection response, and providing cash transfers received from donors to vulnerable persons. IOs enjoy certain privileges and immunities to ensure that they can perform their mandate attributed to them under international

2 See 'Glossary of defined terms' at the start of this guide.

Box 5 - Legal bases for processing personal data

According to most international, regional and national data protection and privacy frameworks, processing personal data is legal in the following situations:[3]

- **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, the execution of criminal penalties, and the enforcement of civil law claims, among other things. For IOs, 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.[4]
- **Vital interests:** This basis applies when the processing of data is necessary to protect the vital interests of a data subject or another person (i.e. to protect someone's life, integrity, health, dignity, or security). For this basis to apply, it is necessary for there to be sufficient elements to consider that, in the absence of the personal data processing, the individual could be at risk of physical or psychological harm.
- **Legal obligation:** The processing of data 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 who provide evidence of being under a certain poverty level. In this case, the authority is required to collect the data to assess those conditions and ensure delivery of the benefits to the targeted persons in order to comply with its legal obligation.
- **Informed consent:** Under this basis, consent indicates the data subject's agreement to the processing of personal data relating to him/her for a specific purpose. When the processing is based on consent, the controller shall be able to demonstrate that the data subject has

3 See, for instance, GDPR 2016/679 (Art. 6, 7, 8, 9) and CoE Convention 108+, 2018 (Art. 5, 17) for the legal basis of consent and personal data processing. Other bases are provided by ECOWAS, 2010 and the OECD Privacy Framework, 2013 (see Organisation for Economic Co-operation and Development, The OECD Privacy Framework, OECD Publishing, 2013).

4 Kuner and Marelli, 2017, p. 67

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 will not always be the most appropriate legal basis.

- **Contract with the data subject:** This basis applies when 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.
- **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 interest, 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, and must not affect people's fundamental rights and freedoms. If the same result can be reasonably accomplished in another less intrusive way, the basis of legitimate interest does not apply. Examples of potential legitimate interests are IT security and fraud prevention.

Box 6 - Security measures

Personal data security measures relate to the physical security of the premises where the personal data is stored, as well as technological and organisational security, and may include the following:[5]

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
- How to keep paper files secure (lock on cupboards)

- Technological security measures
  - System security: The security of the network and information systems, particularly those that 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: The security of the website, online services or applications, etc.
  - Device security: The security of tablets used for data collection, etc.
- 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 that this person/team has the appropriate resources and authority to do their job effectively.
  - Build a culture of security awareness within the organisation, particularly relating to personal data.
  - Provide training for staff on information security, with an emphasis on personal data.
  - Check whether or not security measures are actually being adhered to.
  - Establish standard procedures to deal with security incidents.
  - Undertake regular testing and review of the adequacy of the above security measures (are they 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 only to the protection of networks and information systems from attack. Thus, information security (e.g. the security of personal data) is broader than cybersecurity, as it also covers physical and organisational security measures.

5 Information Commissioner's Office (ICO), Data Sharing Code of Practice, Draft Code for Consultation, n.d.(b)

Box 10 - What is automated decision-making and profiling?

Automated decision-making refers to 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 sources. 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. Typical examples for social protection purposes include proxy means testing (PMT) and fraud detection algorithms.

Profiling refers to 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.[6] Profiles are created based on the personal data of the data subject, obtained directly or indirectly (meaning it can be derived or inferred from other data, and predicted). The information is analysed to classify people into different groups or sectors, using artificial intelligence, including machine-learning,[7] in order to evaluate (score, rank, assess) and predict certain things about an individual (behaviour, interests, performance) 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[8] (e.g. calculating a score through profiling that predicts the likelihood of an individual committing a future crime based on the individual belonging to such a profiled group).[9] These profiles can be used to inform decisions about individuals that may or may not be automated. To the extent that they inform automated decisions, the respective data subject rights need to be respected.

6 GDPR 2016/679 (Art. 4)

7 For more information about artificial intelligence, including machine learning, see 'Glossary of defined terms'.

8 Predictive policing involves the use of algorithms to analyse great amounts of information to predict and help prevent potential future crimes.

9 Privacy International, The Keys to Data Protection: A Guide for Policy Engagement on Data Protection, 2018, p. 57

Box 12 - Independent supervisory authority/data protection authority (DPA)

What is it? A public body, as determined in each jurisdiction, that is responsible for enforcing personal data protection and privacy laws and that is tasked with monitoring and enforcing the application of such laws, including through approval requirements, investigations, and administrative fines, as well as for handling complaints and promoting awareness of rights and obligations thereunder.

The law should establish the DPA's structure, powers and mandate.[10] Good international practices require DPAs to 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 data protection and privacy laws.
- Conduct investigations on the application of such laws.
- Handle the complaints of data subjects with respect to the violation 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.

Powers:

- Impose sanctions.
- Suspend data flows.
- Issue reprimands to data controllers with respect to violations of the law.
- Order the controller to comply with the requests of data subject.
- Carry out data protection audits.

10 Privacy International, 2018, pp. 86–88

- In some cases, a data protection law can give the DPA the power to regulate certain aspects of the law, for example, to update definitions or security requirements.[11]
- Approve safeguards for transborder data flows.

Box 13 - Data protection and privacy policy

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

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 assessments

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 demonstrate that the organisation is taking measures to ensure compliance.[12] It is particularly important for organisations or authorities that wish to implement good standards of personal data protection and privacy in their operations, if national laws do not contain such standards.

Box 15 - Privacy-by-design

Systems should implement privacy-by-design, meaning that data protection and privacy is a default design objective. In other words, systems by standard should implement 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 Framework, the 'privacy-by-design' approach is interpreted broadly, meaning that technologies, processes, and practices to protect privacy should be built into the system architecture and not added on later as an afterthought.[13] Privacy should become part of institutional or organisational priorities, programmes objectives, design processes, and planning operations.

Box 16 - Data protection impact assessment (DPIA)

What is it? A DPIA 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 in order to anticipate and mitigate risks to data subjects and data controllers.

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

Examples of situations where a DPIA is required or strongly advised by some international and regional data protection and privacy frameworks include:[14]

- When processing data through the use of new technologies
- When processing is used to track people's location or behaviour
- When processing personal data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic

11 Ibid., p. 87

12 The GDPR 2016/679 (Art. 24) suggests that controllers implement data protection policies "where appropriate in relation to processing activities".

13 OECD, 2013, p. 104

14 GDPR 2016/679 (Art. 35) and CoE Convention 108+, 2018 (Art. 10, Explanatory Report, Art. 88); other frameworks, such as the OECD Privacy Framework, 2013 (p. 16) and APEC, 2005 (Art. 44), advise that a privacy risk assessment should be carried out, but do not give details.

data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

- When processing data concerning vulnerable categories of people (e.g. people living in conflict affected countries or socially unstable environments, refugees, internally displaced persons and discriminated minorities, migrants or patients)
- 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 data processing could result in physical harm to the data subject if it is leaked
- When systematically monitoring a publicly accessible place on a large scale
- When the processing involves combining, comparing or matching data from multiple sources
- When the processing uses profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit

Box 19 - Purpose specification and integration with other databases

The personal data of recipients or beneficiaries enrolled in a social protection programme are usually stored in a programme specific database (also referred to as a 'beneficiary database'). The information in programme databases is accessed and managed through software applications called programme **management information systems (MIS)** (also referred to as beneficiary operations management system [BOMS]).[15]

These programme-specific MISs can be designed to facilitate integration, interoperability, and ad-hoc data sharing[16] between the data of different programmes, thus allowing these to 'talk to each other'. This may involve using the same identifier, data standards and data formatting/dictionary, so that beneficiaries can be uniquely identified across these databases for the purpose of developing an overview of who receives what and to coordinate interventions, facilitate planning and, more generally, combine monitoring and evaluation across programmes – such as discussed in the context of **integrated beneficiary registries**.[17] Still, the different source databases will contain different data on each individual, depending on the respective programmatic purposes.

Whether the 'overview' database (often operationalised as a 'data warehouse') may **obtain access** to the data from the programme-specific beneficiary database, **without obtaining a new legal basis**, such as consent or public interest, depends on the following:

- Whether or not the integration pursues a **legitimate purpose**, such as assurance that all persons in the beneficiary 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 beneficiary programme shall not double dip in the emergency programme (fraud prevention).
- Whether or not this **purpose is compatible with the purpose** stated to the beneficiaries in the beneficiary database at the time of data collection depends on the facts and should be assessed, as advised in section 11.1.1.

If the new purpose is not compatible, the integration of databases should only occur if provided for by law and if the purpose is legitimate, meaning strictly necessary and proportional to the interference with the data subjects' rights.[18] Data sharing protocols between ministries regulating the integration of the database are often not sufficient.[19]

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, if the 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

15 See Section 2.2 – Information management in social protection programmes.

16 The extent of this will depend on many factors.

17 Barca and Chirchir, 2014, p. 24

18 "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 Carmona, 2018, p. 28).

19 See Section 11.4 – How to share data.

managed in this way. One example would be Kenya's Integrated Beneficiary Registry, integrating five programme databases – including one from WFP (called a single registry).[20]

Box 20 - Purpose specification and social registries

Recent trends, mainly driven by the World Bank, encourage the integration of the processes of outreach, intake and registration, and assessment of needs and conditions to determine potential eligibility for one or more social programme in a country via **social registries**.[21] Purpose specification requires that data be collected and used for a specific, explicit and legitimate purpose. The programmatic purpose behind a social registry is to support the process of determining eligibility for multiple programmes, each with its own eligibility criteria and programmatic focus. This is done via the systematic registration – i.e., collection of relevant data – of a large proportion of the population[22] and use of that data to feed into the eligibility determination process of each and every 'user' programme. In many cases, data on potential recipients within social registries is also ranked or grouped into categories based on socio-economic classifications (e.g. income, PMT, or other method). This enables poverty targeting within user-programmes, but does not exclude the use of social registry data for fully universal categorical programmes (e.g. all households with children under five).[23]

Importantly, from a data protection perspective, it may be that detailed and sensitive data about households (often over 100 data variables, although this varies widely depending on user-programme needs) will be stored in a social registry without that household ever being enrolled in any social protection programme.[24] This may include data that is being sourced or cross-validated against other government databases. Thus, it will be important to address how the collection of a large and sensitive dataset (to be stored in the 'social registry') that enables consolidated assessment of needs and conditions across multiple programmes – including, potentially, for programmes that do not yet exist[25] – will be compatible with the specific legitimate purpose principle.[26]

According to good international practices, personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[27] Generally speaking, when the assessment of needs and conditions (as well as other functions) can be conducted based on aggregate or pseudonymised data, this is preferred.[28] Further, consolidated targeting may cause challenges when it fulfils an undefined, imprecise or vague purpose, raising questions about whether or not it may be objectionable[29] for an individual to disclose a wide range of sensitive information about their life and, eventually, not to obtain any assistance.

Whether or not 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 function, considering all circumstances in each instance, including:

- Existing social protection programmes and policies in the given country, including the level of institutionalisation of the registry itself – and its functions – in policies and legislation
- The benefits of such a social registry for the government
- The size of the affected population that would be part of such a registry (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
- The likelihood of the majority of individuals registered in the social registry eventually being enrolled in a social programme (whether routine provision or emergency response)

20 Barca and Chirchir, 2014, p. 25

21 Leite et al., 2017, pp. 66–80; Barca, 2017; also see 'Glossary of defined terms' and Section 2.1. - Social protection and personal data.

22 Noting that the coverage of social registries varies widely, from less than 5% of a country's population too almost 100%.

23 Barca, 2017; Leite et al., 2017

24 Note, this may be the case for programme-specific MIS and registries too, although sometimes data on non-enrolled (non-beneficiary) populations are not retained in that case.

25 One important example is the use of social registry data for emergency responses (Barca and Beazley, 2019), including during COVID-19.

26 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 that are not needed for the social registry. This is why the amount of data collection for the social registry is determined by whether or it pursues a legitimate and specific purpose.

27 GDPR 2016/679, Recital 39

28 See Box 24 - The use of pseudonymised data and other forms of encrypted data sharing.

29 CoE Convention 108+ (Explanatory Report, Sec. 48)

– If such likelihood does not exist, or only in the 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
- The rights, freedoms and interests of the individuals, particularly the right not to allow intrusion into their privacy sphere, unless for specific purposes with 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 that outweigh the disadvantages and justify the interference with the right to data protection and privacy.

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

Box 21 - 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 the services provided by the programme and the data that it will collect during the course of implementation (transactional data, data obtained through monitoring and complaints), technology has developed in a way that a lot of additional data is collected during 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)
- Timestamp data on the timing of key operations
- Data on the geolocation and movement of individuals tracked by mobile phone operators
- Data on the purchasing behaviour of individuals and, in some cases, their location tracked by retail voucher redemption application providers

If intentionally leveraged, this data may have added value for the government from a data analysis, performance, and monitoring and evaluation perspective. However, such data can also be misused, e.g. for surveillance purposes or by private sector counterparts for their own profit (see, for example, Privacy International's report on *The Humanitarian Metadata Problem: "Doing No Harm" in the Digital Era*[30]). Social protection programmes need to be aware of these additional forms of data collection 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 additional data as part of the services it provides or during the implementation of the programme, or will the service/technology provider collect and use it for its own purposes?
- If the social protection programme obtains additional data, for which purposes will it be used? Additional data can be used to understand beneficiaries better (data analytics), to profile them, but also just to feed technologies for machine learning purposes.[31]

  – Are these separate legitimate purposes, not listed above (in Boxes 19 and 20), about which the individuals were informed?

  – Are the purposes for which the data will be used compatible purposes which do not have to be communicated to the data subjects? This seems 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 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 interest, and whether it is acceptable for the provider to keep the additional data and use it as a controller or 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 or not such data use is acceptable.

30 International Committee of the Red Cross (ICRC) and Privacy International, The Humanitarian Metadata Problem: "Doing no Harm" in the Digital Era, October 2018

31 See Section 11.2 – How to ensure that data subjects can exercise their rights.

Box 25 - 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 and, therefore, excessive, given that donors neither intend, nor are able, to reach out to all of these beneficiaries to confirm receipt of assistance. Instead, assurance can be obtained by providing anonymised payment lists or reports (deleting identifiers, signatures, thumbprints) and a confirmation by the 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.

Box 27 - Lawful processing of sensitive data

The conditions under which sensitive data like biometrics, health or disability data can be lawfully used for the implementation of a social protection programme also depends on the manner in which national laws regulate the use of sensitive data. If the use of sensitive data is generally prohibited, as under the GDPR and CoE Convention 108+, no legal basis would be sufficient for such processing. Instead, 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 in the case of social protection laws.[32] In the absence of such a regulation by national law, it is strongly suggested to use sensitive data only if appropriate safeguards are in place. The consent of the data subject alone does not suffice. The use of biometrics should be strongly discouraged in such cases.

Box 31 - 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 project implementation, may object to the processing of their data. Controllers should try to find out what the specific reason for their 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.

The importance of conducting a DPIA, particularly consultations with the concerned population, can be stressed as a way to prevent these types of problems from the beginning of the programme. 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 easy, and there is no step-by-step procedure 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. Programme designers and implementers 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, potential beneficiaries need to be informed about the implications of withholding their data.

Box 42 - Data protection office or officer (DPO)

A DPO needs to provide tools and guidance for organisations on how to comply with existing data protection and privacy regulations when processing the personal data of any data subjects, such as staff, customers or beneficiaries. A 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, it must perform its function independently. Therefore, organisations should avoid conflicts of interest, and staff of the organisation should not instruct the DPO about its duties. The DPO should manage its own

32 See Chapter 8 – Sensitive personal data.

budget and not report to any direct supervisor, be an employee in a contract, or be a data processing controller.

The appointment of a DPO is specified, for instance in the GDPR,[33] which clarifies the requirement of installing a DPO whenever data processing is carried out by a public authority; when the regular and systematic monitoring of individuals on a large scale is necessary during processing; or when the data processed is of a particular category (including racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, health data or sexual orientation).[34] The CoE Convention 108+ specifies the instalment of a DPO as an obligation of the data controller to ensure personal data protection and privacy.[35] Equally, it is suggested that social protection programmes or development and humanitarian organisations appoint a DPO to ensure the accountability of data controllers, in alignment with data protection and privacy regulations and data security.[36]

Box 44 - Data-sharing agreement between controllers

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

Why is it important? It is important in order 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 understanding of their particular roles and responsibilities
- Outlines what will occur with personal data when received by the other controller
- Establishes rules and procedures, particularly on who and how information about the processing and their rights is provided to data subjects

33 GDPR 2016/679, Art. 37

34 GDPR 2016/679, Art. 9

35 CoE Convention 108+, 2018, p. 25

36 Kuner and Marelli, 2017, p. 46

Box 46 - 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.[37] As a consequence, the exchange of personal data between bodies that are part of one legal entity (i.e. controller) – for example, two ministries of the same country – 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 (beyond memorandums of understanding, and so forth). However, public authorities may have a separate legal personality than the state.[38] 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, foraccountability purposes, it is suggested that a **data sharing protocol** be agreed upon with basically the same information as relevant for the data sharing agreement, with the following particularities:

- The new purpose(s) 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.
- The controller (the government, represented by the requesting ministry) needs to identify a legal basis for the new purpose(s), unless such a purpose is compatible with the purpose that was stated to individuals at the time of data collection.

Box 48 - 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 that manages and operates data storage as a service. Social protection programmes in low- and middle-income countries often lack robust 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

37 This needs to be reviewed and confirmed in each country's case by lawyers admitted to practice in the respective jurisdiction.

38 Again, this needs to be reviewed and confirmed by lawyers admitted to practice in the respective jurisdiction.

protection and privacy regime, as well as any data localisation laws, and that careful consideration is given to the security controls offered by using cloud technologies. Before deciding to rely on private cloud storage, the data controller is expected to carry out a specific risk assessment. Furthermore, the data controller is responsible for selecting a cloud provider that complies with data protection and privacy principles and legislation and that conducts regular audits and has in place system security measures on cloud-based storage.

Box 50 - 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, and they can lead to the uncovering of additional information by analysing the biometrics. Such additional information may include diseases, drug use, an individual's emotional state, or genetic inheritance.[39]

Biometrics include the following (non-exhaustive) list of technologies and data:

- **Fingerprints:** Fingerprints 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 are low cost and, thus, widely used in civil and commercial applications.
- **Iris:** Images of the coloured ring surrounding the pupil of the human eye – the iris – are captured through infrared illumination and consist of a complex textured pattern. This pattern is highly individual and very difficult to manipulate or imitate surgically. As a result, many border crossing systems use iris technology for personal identification. However, iris sensors are costly, and their use limited due to the lack of legacy databases for irises.
- **Face:** Facial recognition is an established and successful method of biometric identification. 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.[40]
- **Voice:** Voice and speech recognition systems identify individuals, including behavioural (including the movement of lips, jaw, tongue, etc.) and physiological (including vocal tract, lips, mouth etc.) characteristics. The vocal behavioural traits of an individual may vary and change with age and state of health. Speech recognition is sensitive to background noise and playback spoofing.[41]

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, electroencephalogram,[42] electrocardiogram,[43] transpiration, eye blinking, breathing frequency and trepidation).

Due to the sensitivity of biometrics, the GDPR, for instance, considers biometric data as a special category of data processing that is prohibited unless expressly permitted.[44]

39 Sepúlveda Carmona, 2018, pp. 3–4

40 Tistarelli, Massimo; Barrett, Susan E. and O'Toole, Alice J., 'Facial Recognition, Facial Expression and Intention Detection', In: Emilio Mordini and Dimitrios Tzovaras (eds), Second Generation Biometrics: The Ethical, Legal and Social Context, Springer, Dordrecht, 2012, pp. 229–231

41 Jain, Anil K. and Kumar, Ajay, 'Biometric Recognition: An Overview', In: Emilio Mordini and Dimitrios Tzovaras (eds), Second Generation Biometrics: The Ethical, Legal and Social Context, Springer, Dordrecht, 2012, pp. 51–52

42 Electroencephalogram measures the electrical brain activity and detects abnormalities in an individual's brain waves (John Hopkins Medicine, 'Electroencephalogram (EEG)', [online], n.d.(b), https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/electroencephalogram-eeg).

43 Electrocardiogram measures the electrical activity of the heart (John Hopkins Medicine, 'Electrocardiogram', [online], n.d.(a), https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/electrocardiogram).

44 GDPR 2016/679 (Art. 9)

Box 52 - Potential risks of automated decision-making and profiling

Automated decision-making and profiling can be useful in many sectors (e.g. education, financial services, marketing, etc.) when dealing with large amounts of data. However, if not accompanied by the appropriate risk assessment and safeguards, it can pose 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 associated challenge stems from automated data processing techniques, as they allow for the generation of new data that can be inferred or constructed even if data subjects did not originally provide it. 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 significant issues around notions of consent, transparency and personal autonomy.[45]

Another major concern is related to new data processing methodologies like AI, in which decisions are based on machine learning from a potentially biased dataset. For example, a model trained on data from the United States or the People's Republic of China would only be fully effective when implemented in these contexts. Moreover, any dataset based on human data inherently carries biases that can never be entirely prevented or removed, but only mitigated to a certain degree. Consequently, automated decision-making can produce inaccurate, unfair or discriminatory decisions, making 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 a judge formally makes the final decision, the automated decision made by a programme can be decisive and has led to inaccurate, discriminatory and unfair decisions. The problem stems from the design of the algorithm and the dataset, which have been shown to incorrectly calculate recidivism, i.e. the likelihood of an offender to re-offend, by repeated scientific evaluations. In this context, what is highly problematic is that the incorrect calculation of recidivism is a form of racial discrimination justified by a seemingly objective algorithmic system.[46]

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 and issues such as fairness, transparency, and accountability. At the same time, it is essential to be clear that data protection and privacy safeguards will not prevent incorrect decisions from being made. For example, if a dataset or the system design is biased, this will inevitably happen, regardless of whether or not this is a fair use of personal data. Transparency and accountability safeguards are, thus, critical to ensure that when incorrect decisions are made, they can be rectified swiftly, and appropriate remedies implemented as rapidly as possible.

45 MSI-NET, 2018

46 Privacy International, 2018

IMPLEMENTATION TOOLS

Box 14 - 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 governance and accountability mechanisms, as deemed appropriate by the respective entity. Suggestions on how to structure a policy are as follows:

- Introduction and purpose
- Scope
- Definition of key terms
- Data protection principles:
  - Which ones you commit to
  - Appropriate guidance on how to uphold each principle
- Data subject's rights
- Governance and accountability:
  - Establish a DPO to monitor the implementation of the policy by the organisation.
  - Regulate the roles and responsibilities of staff and 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, with respect to the implementation of the policy.
  - Data breach management
  - Working with third party processors
  - Data transfers to third parties
- Treatment of sensitive data: The use of beneficiaries' sensitive data should be specifically regulated, in terms of permitted use purposes, legal basis, data minimisation, strict security measures and short retention periods, among other things.
- International data sharing (if applicable)
- Other general obligations of the controller,[47] such as data breach notification procedures and record-keeping
- Non-applicability
- Good practices and practical steps for staff to follow

This list is neither complete nor exhaustive. Each organisation or 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 implementation of the policy, containing guidance on points that are particularly relevant to implementing a social protection programme, such as what legal basis to choose, when and how to use biometrics (if at all), how to allow individual data subjects to exercise their rights, and 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 while 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.[48]

Box 17 - Implementing a DPIA

How to implement? There are different approaches to conducting DPIAs. The following guidance draws on good international practices from a range of sources:[49]

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 to or provide a link to

47 See Table 1 – Obligations of data controllers and data processors.

48 See Section 9.3 – Data management protocol for a social protection programme.

49 Information Commissioner's Office (ICO), Security, n.d.(e), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/; and Kuner and Marelli, 2017, pp. 65–67, 299–305

other documents, such as a project proposal. Summarise why you have 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 the applicable data protection and privacy frameworks and standards, as well as organisational policies.

Step 3: Describe the processing of personal data: Map the information flows detailing the following (at a minimum):

- The type of data to be collected
- Whether or not sensitive information will be collected
- How the data will be collected
- For what purpose(s) 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 or not personal data will be disclosed
- Whether or not sensitive personal data will be disclosed
- Whether or not any data will be transferred to other organisations or countries

You might find it useful to refer to a flow diagram or other way of describing data flows. Look at what types of processing are involved that are likely to entail high risk?

Step 4: Consultation process: Consider how to consult with relevant stakeholders: Describe when and how you will seek individuals' and stakeholders' views, or justify why it is 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 5: 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?
- How will you ensure data accuracy and data minimisation?
- What information will you give data subjects?
- How will you help to support the rights of data subjects?
- What measures will you take to ensure that processors comply?
- How will you safeguard international data transfers?
- How will you ensure data deletion, also by partners?

Step 6: 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 7: Identify measures to reduce risk: Identify any additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

- Describe the risks
- Options to reduce or eliminate risk
- Effect of measure on risk: eliminated, reduced or accepted
- Residual risk: low, medium or high
- Measure approved: yes/no

The Cash Learning Partnership 'Model Privacy Impact Assessment (PIA)' can be used as an example.[50]

50 Cash Learning Partnership (CaLP), Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in Cash and e-Transfer Programmes, Annex I – Model Privacy Impact Assessment (PIA), 2013, https://www.calpnetwork.org/wp-content/uploads/2020/01/calp-beneficiary-privacy-annexes.pdf

Box 23 - Data categories necessary to fulfil data minimisation and purpose specification principles

The list below is a rule of thumb for data categories that can be seen as necessary to fulfil the specific and legitimate purpose(s) specification for implementing a social assistance programme:

Assessment of needs and conditions (will depend on eligibility criteria):

- Detailed socio-economic data (e.g. income, expenditure, household size)
- Food security
- Vulnerability data (e.g. 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 *verification*[51] that the individual is the person they claim 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. fingerprints, iris scan) are collected for the purpose of authentication and avoidance of double-dipping/fraud.[52]
- 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, or a phone number (for a mobile money account). 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).
- A phone number may be needed to *communicate* to beneficiaries that a cash transfer has been completed, the location of a distribution, or other important information regarding the cash delivery.
- If a smartphone application is 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 delivery transactions:

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

Monitoring of social protection programme:

- A phone number or other details may be needed to contact and interview beneficiaries.
- In some cases, data to authenticate beneficiaries may be necessary, however, usually, there is no reason to assume that a non-beneficiary would participate in an interview.
- Information requested from the beneficiary by the monitors may contain personal data (e.g. personal opinions).

Complaints and feedback:

- Data to authenticate caller/beneficiary (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; it can also be sensitive data, such as complaints about harassment.

51 Identification is the process whereby 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 that the 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, 'Identification vs. Authentication vs. Verification: What are the Differences?', Blog, 2020, https://www.idenfy.com/blog/identification-verification-authentication/).

52 In middle and higher-income countries, registration across several government services is more common, acknowledging the fact that these are complementary (Chirchir, Richard and Valentina Barca, Building an Integrated and Digital Social Protection Information System, Technical Paper, GIZ, Bonn, 2020, p. 36). With respect to biometrics, the need to authenticate beneficiaries and the principle of data minimisation, see Section 12.2. – Data protection and privacy challenges of specific technologies.

Box 24 - The use of pseudonymised data and other forms of encrypted data sharing

Governments, IOs, and NGOs may assess, target and assist overlapping populations. When assessing needs and conditions before setting up a new programme, it may be more effective to request socio-economic and other vulnerability data from these stakeholders than to conduct time consuming and costly new assessments of the population (note, this can be inbuilt via social registries). In this case, applying the data minimisation principle could mean that the sharing entity will provide a pseudonymised list containing all the information relevant for the assessment, 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.[53]

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 must have a legal basis for sharing the data with the receiving controller who envisages another social protection programme (e.g. consent or public interest).
- The parties must enter into a data-sharing agreement.

Importantly, the humanitarian sector has also started experimenting with zero-knowledge proofs (ZKPs) (which are mathematical methods used for verification without sharing or revealing underlying data) and 'hashed' personal data[54] (algorithmically generated encrypted 'hashes'/representations of personal data as proxies for the actual data).

Box 28 - Consent: Some specific conditions to be considered valid

In some international and regional data protection and privacy frameworks,[55] consent needs to fulfil specific conditions to be considered valid. Good international practices require consent 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 when the personal data is collected, or as soon as reasonably practical thereafter.
- **Freely given:** Consent is regarded as freely given if the data subject has the genuine and 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:[56]
  - Characteristics of the data subject, such as illiteracy, disability, age
  - Health status, gender and sexual orientation
  - Location of the data subject, such as a detention facility, resettlement camp, remote area
  - Environmental and other factors, such as unfamiliar surroundings, incomprehensible language or concepts
  - Data subject's position concerning others, such as belonging to a minority group or ethnicity

53 Unfortunately, sophisticated techniques that allow datasets to be de-anonymised exist (see Box 36 - Erase or anonymise personal data?). A good international practice for sharing public data and ensuring that the data from individuals and individual households remains confidential is to use 'differential privacy' (National Conference of State Legislatures (NCSL), 'Differential Privacy for Census Data Explained', [online], 2021 https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx).

54 "Organisations such as ICRC and Mastercard are exploring approaches that create algorithmically generated encrypted 'hashes' of biometric data – in other words, encrypted representations of personal data are used as proxies for the actual data, with the encryption algorithm being the proprietary technology that ensures data protection and security. Authentication and verification would be carried out by comparing the hashes, not the actual data – using a proprietary algorithm to match the hash presented by the beneficiary against the hash held by the organisation" (SPACE, 2020, p.10).

55 GDPR (2016/679); CoE Convention 108+, 2018

56 Kuner and Marelli, 2017, p. 46

- Social, cultural and religious norms of families, communities, or other groups to which the data subject belongs
- 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.

◦ **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. In addition, it is important to record any limitations/conditions on the use of their 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 tied to a specific purpose, processing activity and/or 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 may or may 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.

Consent should be given by:

◦ **Clear affirmative action:** Consent requires an active process by the individual, rather than a passive opt-out process. Mere silence, inactivity or pre-validated forms or boxes do not, therefore, constitute consent.

◦ **A statement:** Alternatively, consent can be given by an oral or written statement (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, as 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 in relation to 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 operation, due to the scale of the operation, or if the data is obtained from a third party (e.g. an IO)

◦ The consent cannot be valid because the individual is particularly vulnerable or has no real choice to refuse consent

◦ Digital technologies are involved and the risks are difficult for data subjects to fully appreciate[57]

Box 29 - Legal basis and joint programmes of IOs 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 a controller). IOs often 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 IO's own data protection and privacy framework may overlap and contain deviating requirements.

57 Kuner and Marelli, 2017, p. 58

In the context of national social protection programmes (which differ 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 provided by the law. Public authorities and IOs 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 national laws do not provide for any personal data protection and privacy or contain gaps, IOs 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 IOs data protection and privacy framework, during project design, as part of the data management protocol, and in the legal agreement governing their cooperation.

Box 30 - Providing information to enable transparency

Good international practices stipulate that the following information be provided to data subjects:

- 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)
- Upon what legal basis the data will be processed
- The identity of all processors with whom the data is expected to be shared and for what specific purposes (enrolment, data storage, authentication, delivery of cash or food, monitoring)
- How to exercise their rights as data subject (to access, update, correct or delete data or to complain about the data processing, and the right to object or withdraw consent)[58]
- Their right to withhold their data and the implications, particularly any alternatives to obtaining benefits without providing the personal data

Box 33 - How to implement the data accuracy principle?

In practice, this means that social protection programmes should:

Plan data accuracy: Before personal information is collected or received:

- Determine the minimum data fields needed for the specified purposes (the less data collected, the easier it is to keep It up-to-date).
- If data is received from third parties, obtain a dataset description (metadata), 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.
- Identify mechanisms for keeping data accurate and up-to-date, for example, through a regular census, integrating databases (e.g. linking data to civil registries, in places where deaths, births, marriages, etc. are registered, considering the privacy implications thereof)[59] and 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 the data collection exercise, if required.

Ensure any information collected is correct and corresponds to reality:

- 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 for proof of residence/address or income/payslip to prove that the ID presented belongs to the person presenting it.

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?

58 See Section 11.2 – How to ensure that data subjects can exercise their rights.

59 See Section 11.1 – How to limit processing in line with the data processing principles.

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 data subject's right to rectification).
- Define who is responsible for updating personal data, as well as the procedures and protocols for this to happen.
- Periodically ask individuals to update their details, especially if the information could have serious implications for them.
- Keep an historical record of changes (updates, rectifications, erasures) to data.
- Conduct regular spot checks on the accuracy and relevance of the personal data recorded.

Box 35 - 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),[60] specifically for personal data, which should include the following:

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

If no such retention policy exists, the social protection programme manager should determine, in the data management protocol,[61] the retention period for all data types processed for the purposes of the social protection programme.

Regarding social registries, as their overall purpose is to target people from a pool of potential recipients, data retention is applicable via established parameters to decide when the targeting is no longer a legitimate purpose. For instance, a parameter could be that if an individual has not been targeted for any social protection programme for ten years, then their data should be deleted. Many programmes include more frequent recertification obligations (e.g. every 2 or 3 years).[62]

Box 36 - 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 data does not equate to deleting it.

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:[63]

- There is no intention to use or access the data again or to share it with any other organisation.
- Appropriate technical and organisational security measures are used.
- There is commitment to permanently delete the information if, or when, this becomes possible.

60 See Section 9.2 – Organisational data protection and privacy policy.

61 See Section 9.3 – Data management protocol for a social protection programme.

62 Barca and Hebbar, 2020

63 Information Commissioner's Office (ICO), Rights Related to Automated Decision Making Including Profiling, n.d.(d), 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/

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 difficult 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-identify the individuals whose personal data was contained in the dataset rendered anonymous. Thus, the data subjects are no longer anonymous.[64]

Social protection programmes should test the anonymised dataset 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.

Box 38 - Breach notification to data protection authority and/or data subjects

The breach notification should include, as a minimum:

- Type of incident and nature of the breach
- Date of the incident
- Cause of breach
- Those affected
- Type of personal data compromised
- Number of people whose data was compromised
- Likely consequences
- Measures taken to address the breach and mitigate any 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.

Box 40 - CFM call centre: Compliance with data protection principles

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

- How to provide information? For example, on an answering machine, on the details of the data processing, including the legal basis (typically consent), and how to collect consent.
- Which data needs to be collected for which purposes? For example, if the card does not work and the beneficiary requires a new one, the social protection programme needs to check the issue and call the beneficiary back, for which purpose it needs the beneficiary's name, phone number and electronic voucher card number. The beneficiary's name, phone number and detailed information are also needed when a protection case is reported.
- When does personal data not need to be collected? For example, a caller may not require feedback (e.g. if he/she reports that in a given location sacks of rice are rotten or one out of several ATMs does not work).
- How can the call centre operator's access to information be minimised and the abuse of data for different purposes be avoided? For example, a technology can be used that irrevocably closes the window when 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. Another safeguard is a '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 what cases will data be shared with other agencies? For example, if a caller asks to be included in a social protection programme of a different controller (e.g. implemented by a different IO)?

64 A 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).

- When will data be deleted? For example, data with respect to technical issues having been resolved may be deleted within a short time frame, but data with respect to protection cases or potential litigation 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 call centre operators.

Box 45 - Establishing a data-sharing agreement between controllers

How to establish? Obtain advice from a legal department/lawyer in order to ensure that the agreement reflects appropriate safeguards depending on the volume and sensitivity of the data that will be transferred between the controllers.

Some suggestions on what to include in the agreement are:[65]

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 broadly

Which other organisations will be involved in data sharing:

- Contact details of the DPO of other organisations and other key members of staff
- Procedures for including additional organisations in the data-sharing arrangement
- Procedures for dealing with cases in which an organisation needs to be excluded from the sharing agreement

What data items are going to be shared:

- Explain in detail the types of data the organisation is intending to share with other organisations.

The responsibilities of the controllers:

- Both controllers should be subject to some data protection and privacy 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 (DPO).

Whether or not the data been collected lawfully, for legitimate purposes and is accurate and up-to-date:

- The controller who shares the data shall warrant that it has processed the data in compliance with applicable data protection laws and, in particular, that it has collected only necessary data, lawfully, and for legitimate purposes, and that the data is accurate and up-to-date; if not, the controller will provide information about inaccuracies.

The legal basis for sharing data:

- 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.

Any sensitive personal data:

- The relevant conditions for processing should be documented.

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 for the data processing done by it. And the old controller will remain responsible to respect the data subject rights (such as the right of access to information, right to object, and requests for rectification and erasure) with respect to the processing conducted by it. 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 is also held by the other controller should be deleted and inform the other controller thereof.

65 ICO, n.d.(a)

- 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 should be able to choose to contact any controller.

What happens in case of a data breach happening to one controller?

- The agreement should include an indemnity clause to cover the situation when an individual claims compensation for a data breach happening to one of the controllers to cover the controller who has not suffered a data breach.
- If the data subject claims compensation from the controller who has not suffered a data breach, that controller should notify the other controller.

CHECKLIST OF GOOD PRACTICES

Box 7 - Checklist of good practices: What information should be provided to data subjects?

Good international practices require individuals to be provided with the following information:[66]

- ☐ The identity and the contact details of the controller
- ☐ The purpose(s) of the processing
- ☐ The legal basis for the processing
- ☐ The categories of data involved
- ☐ With which entities the personal data will be shared and for what purpose(s)
- ☐ Whether or not 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 subject has over their data in relation to the controller and processor, and how they can exercise them
- ☐ The rights that the data subject has, 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, as well as 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

Box 8 - Checklist of good practices: Exercising the right to access

Good international practices require data subjects to be able to easily request and be given information about the processing of their personal data by the controller.[67] Access should be:

- ☐ Freely given or, if there is a charge, it should be not excessive (e.g. a reasonable fee based on administrative costs)
- ☐ Within a reasonable and stated time
- ☐ In a form that is readily intelligible to the data subject and does not require any particular expertise or knowledge to comprehend the information

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

Box 9 - Checklist of good practices: When can the right to erasure be exercised?

Good international practices require that data subjects have the right to have their personal data erased from the controller's database in (one of) the following instances:[68]

- ☐ Their personal data are no longer necessary in relation to the purpose(s) for which they were collected or otherwise processed.
- ☐ The data subject has withdrawn consent and there is no other legal ground for the processing.
- ☐ The data has been obtained based on a public task or legitimate interest, the data subject objects to the processing, and there are no compelling legitimate interests overriding the rights and freedoms of the data subject.
- ☐ The processing does not comply with the applicable data protection and privacy framework.
- ☐ The personal data must be erased to comply with a legal obligation to which the controller is subject.

66 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).

67 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).

68 See GDPR 2016/679 (Art. 17), CoE Convention 108+, 2018 (Art. 9), Malabo Convention, 2014 (Art. 19), APEC, 2005 (Art. 29–30).

Box 11 - Checklist of good practices: Rights related to automated decision-making and profiling

Good international practices require the following:[69]

- ☐ Both automated individual decision-making and profiling should be covered in a data protection framework (however, they don't need to be dealt with together, as 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 on their lives (e.g. an automated decision regarding a refusal of a social protection benefit).
- ☐ 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

Box 18 - Checklist of good practices: Purpose specification principle

- ☐ Ensure the purpose specification of data: Personal data should only be collected for a determined, explicit and legitimate purpose, which is stated to the data subject at the time of data collection, with subsequent processing also compatible with this purpose. Any exceptions or deviations should not be allowed, unless permitted by law.

Box 22 - Checklist of good practices: Data minimisation principle

- ☐ Ensure data minimisation: Only collect personal data that is adequate, relevant and not excessive to accomplish the purposes established at the time of collection.
- ☐ When requesting personal data, 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 from data subjects.

Box 26 - 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, in a fair and transparent manner.
- ☐ Ensure transparent and fair information and communication with data subjects by clearly informing them, at the time of data collection, how, why and when their personal data will be processed, both when they have provided this directly to a controller and when 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 subject's consent is informed, given freely 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. When consent cannot be obtained, exceptions should be very limited and applied on an individual case-by-case basis, with heightened levels of transparency, and another legal and legitimate basis for personal data processing is required.
- ☐ Offer data subjects alternatives that allow them to continue to receive assistance should they not provide, or object to the programme's processing of, their personal data, especially in the case of sensitive personal data.

69 GDPR 2016/679 (Art. 22)

Box 32 - 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, as complete as possible and, when necessary, 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 and implementing the procedures for that to happen.
- ☐ Conduct regular spot checks on the accuracy and relevance of the personal data recorded.

Box 34 - Checklist of good practices: Retention limitation principle

- ☐ Ensure application of the retention limitation principle: Personal data should be retained in a form that permits the identification of data subjects for no longer than the time required for the purposes for which such data was originally collected/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 data management protocol.
- ☐ Establish a retention policy and schedules specifying the retention period for all the personal data that is held, determining how it will be subsequently securely deleted from database or anonymised, both by the data controller and any third parties that have had access to the data.

Box 37 - 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, or entity 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 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 put in place monitoring mechanisms to ensure security safeguards are in place.
- ☐ Ensure that 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 carefully consider the 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 authorised and limited by data protection and privacy laws, regulations, frameworks or internal guidelines, and needs appropriate safeguards.[70]

Box 39 - Checklist of good practices: Rights of data subjects

- ☐ Respect, promote and facilitate the exercise of the rights of data subjects.
- ☐ Widely disseminate awareness of the rights of data subjects among organisation 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 collected, with 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 or not to share their personal data.

70 See Section 12.2 – Data protection and privacy challenges of specific technologies.

- ☐ Ensure the right to access and challenge: Enable data subjects to easily obtain (request and be given) confirmation of whether or not a controller is processing personal data concerning them and, when this is the case, access to such data and information about its processing (collection, storage or use). If the request for information is refused, the data subject should have the right to be given the reasons why, and to challenge such denial.
- ☐ Ensure the right to rectify and erase: Data subjects should be allowed to rectify (correct, update or modify) personal data processed about them to ensure that such data is accurate, complete and kept up-to-date. Data subjects should, in certain circumstances, also 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 interest, data subjects should be able to 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 that 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 have the right to not be subject to purely automated decision-making, including profiling, which produces legal or other significant effects for them. Where exemptions allow for solely automated decision-making (including, for example, PMT), 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 the right to an effective remedy: Data subjects should be able to submit a complaint to an independent supervisory authority and to request an effective judicial remedy via the courts when they consider that their rights have been violated as a result of the processing of their personal data in non-compliance with the law.

Box 41 - 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 that personal data protection and the right to privacy are covered, and compliance with the organisational and/or domestically applicable data protection regime.
- ☐ Ensure that a DPIA is undertaken before processing personal data (i.e. before data collection), and define what safeguarding measures will be applied, especially when the processing is likely to pose a high risk to the rights and freedoms of natural persons.
- ☐ Establish clear lines of accountability, under which 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 needs 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 pose a high risk to the rights and freedoms of natural persons, inform the relevant supervisory authority (if one exists) and the affected data subjects about the loss or unauthorised acquisition of their personal data (breach notification) in an appropriate and timely manner.
- ☐ Establish an effective CFM that data subjects are aware of and which they can access to file requests to access, rectify, erase or object to/complain about data processing.
- ☐ Ensure that the CFM includes an independent supervisory authority that has the power to receive complaints, investigate them and apply sanctions (administrative remedy) or refer the case to a court (judicial remedy), if applicable.

Box 43 - 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, minimum safeguards established against hackers, and sanctions and redress measures to address successful cyberattacks.

Box 47 - Checklist of good practices: Cloud-based information systems

- ☐ The data controller should ensure that the use of cloud services complies with the 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.
- ☐ Select 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 signing and ensure that it contains adequate data protection and privacy standards, accountability mechanisms, data security (technical, physical and organisational) measures, confidentiality provisions, and mechanisms that facilitate the exercise of data subject rights.
- ☐ Ensure that the cloud service provider complies with international legal requirements for data sharing.
- ☐ Conduct regular audits of the personal data processing performed by the cloud provider (or the sub-contractors) and of cloud-based storage system security measures.

Box 49 - Checklist of good practices: Biometric identification systems

- ☐ Biometric data should be considered sensitive personal information (not just personal data), meaning that additional security and data protection layers are necessary.
- ☐ Ensure that the free, informed and documented consent of the concerned data subject(s) is obtained.
- ☐ Information should be presented to data subjects describing what biometrics are and why they are risky, and setting out the specific purpose(s) of the processing of their biometric data.
- ☐ Consider the rights of data subjects and inform them about the involvement of third parties, the possible implications of biometric data collection, and the setting up of adequate infrastructure to grant the right to access, objection, deletion and rectification of data.
- ☐ Explicit consent should be the preferred legal basis. Social protection programmes should provide an alternative identification mechanism to people who do not want to release their biometric data.
- ☐ Given the sensitivity of biometric data, implement adequate and proportionate security measures.
- ☐ Collect and process only adequate and relevant data and minimise storage time and the amount of data collected.
- ☐ Ensure the fair and lawful processing of personal data obtained using biometric technology.
- ☐ No biometric database should be generated, but rather data should be stored in data subject token.
- ☐ There should be no sharing of biometrics.
- ☐ Always allow for the withdrawal of consent, the right to object and the right to erasure.
- ☐ Conduct a DPIA to clarify processing details, highlight potential risks and mitigation measures, and determine if biometric data should be collected.
- ☐ Avoid the retention of data for further processing and develop data retention policies.
- ☐ Establish a data retention timeframe (for example, two years from the last assistance received by the beneficiary).

Box 51 - Checklist of good practices: Automated decision-making

- ☐ Ensure that 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 individuals' interests, rights, and freedoms should be strictly restricted. For example, automated decision-making has been used to restrict access to programmes that help the unemployed find their way back into the labour market in Austria and to identify fraud (frequently incorrectly), leading to a reduction in benefit payments in Australia and the Netherlands.
- ☐ As a consequence, automated decision-making poses a considerable risk, both to the rights of beneficiaries and the core mission of the social protection providers. This Implementation Guide recommends that fully automated decisions should never be used to determine access to social protection, or the degree or amount of social protection received. Cases in Australia and Sweden have shown that once social protection systems make mistakes of this kind, it becomes nearly impossible to rectify them manually, challenging the very purpose of the social protection system.
- ☐ Having fully acknowledged these concerns and challenges, should social protection providers still wish to implement automated decisions in a limited manner, they should apply them only in exceptional cases, defined by applicable data protection and privacy legislation, and always accompanied by the implementation of adequate safeguards to protect the data subjects' rights, freedoms and legitimate interests. In addition, data subjects should have at least the right to request (in a simple way) and obtain human intervention, express their point of view, and challenge the decision.
- ☐ Social protection providers must ensure that human intervention (oversight of the decision) is meaningful. It should be carried out before the decision applies and be done by someone who has the authority and competence to change the decision. Providers should also carry out regular checks to ensure that social protection data controller systems are working as intended regarding the decision-making process. Furthermore, social protection providers should 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. Finally, providers should ensure, in the case of automated decision-making (including profiling), the provision of meaningful information about the logic involved, as well as the significance and envisaged consequences of such processing for the data subject.
- ☐ Automated decision-making techniques can be used to support unemployed social protection beneficiaries by informing them of skills' trainings they were not previously aware of or opportunities they had previously missed. In doing so, the automated decision-making system needs to be completely honest and transparent about its deficiencies and biases in an easily understandable way so that the beneficiary can meaningfully evaluate the automated advice they are receiving. The final decision on how to respond to this advice should always remain with the beneficiary and not be linked to the provision of other measures or forms of social protection support.
- ☐ In the example mentioned in the previous point, there are likely to be biases and the misrepresentation of skills and opportunities based on the data used and the system's design. These biases could, for example, include discriminatory assumptions about skills or professional ability related to gender. The providers would need to take steps to mitigate these biases, while acknowledging to beneficiaries that they cannot entirely prevent them. They also need to ensure that transparency and accountability mechanisms are integrated into the decision-making process, providing regular audits of the process.

EXAMPLES

Box 53 - The 'SyRI case'

The District Court in 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.[71] As part of the SyRI case, an automated system was used to identify benefit fraud, often incorrectly. This automated system used numerous variables, including one based on nationality, with the assumption that holders of multiple passports were more likely to commit fraud. The resulting discriminatory decisions by SyRI were challenged in court, but were considered legitimate decisions by Dutch courts for many years.

The automated decisions incorrectly claiming fraud mainly affected marginalised groups in the Netherlands, as they were made about individuals who were not, or not solely, Dutch nationals. Benefit claimants subject to these decisions were being legally required to repay large sums of money, often facing financial ruin and losing their homes and livelihoods in the process. The SyRI system led to the children of claimants who were incorrectly determine to be guilty of tax fraud being removed from their families in 1,115 cases.[72]

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".[73] 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 about the grave risk of "stumbling, zombie-like, into a digital welfare dystopia".[74]

71 Privacy International, The SyRI Case: A Landmark Ruling for Benefits Claimants Around the World, 2020.

72 NL Times, 'Over 1,100 Children Taken from Homes of Benefits Scandal Victims', [online], 2021, https://nltimes.nl/2021/10/19/1100-children-taken-homes-benefits-scandal-victims

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

74 United Nations Office of the High Commissioner for Human Rights (UNOHCHR), 'World Stumbling Zombie-Like into a Digital Welfare Dystopia, Warns UN Human Rights Expert', [online], OHCHR News Events, 2019, https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156

IMPRINT

Published by:
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH
On behalf of SPIAC-B working group on Digital Social Protection

Registered offices:
Bonn and Eschborn

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

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

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

Programme/project description:
Implementation Guide – Good Practices for Ensuring Data Protection and Privacy in Social Protection Systems

Author:
Ben Wagner, Carolina Ferro and Jacqueline Stein-Kaempfe

Coordination:
Dominique Leska

Editing:
Susan Sellars

Layout / Illustrations:
SCHUMACHER
Brand + Interaction Design GmbH
Art Director: Hanna-M. Bamberger
schumacher-design.de

URL links:
Responsibility for the content of external websites linked
in this publication always lies with their respective publishers.
GIZ and its SPIAC-B partners expressly dissociates itself from such content.

Responsible for the content:
Ralf Radermacher (GIZ) for the SPIAC-B
working group on Digital Social Protection
Bonn, August 2022

Supported by the

Federal Ministry
for Economic Cooperation
and Development