International Labour Organization

▶ ILO brief

Social Protection Spotlight

Date: June 2018

Minimum requirements for ensuring privacy and data protection in social protection systems

Introduction

Social protection programmes require the processing of significant amount of data, which is often of sensitive nature. Domestic and international norms establish the conditions under which processing of information is legitimate. Under the ILO Social Protection Floors Recommendation, 2012 (No. 202), States have committed to "[e]stablish a legal framework to secure and protect private individual information contained in their social security data systems" (para. 23).

Effective data protection within social protection systems requires much more than laws and regulations. This Policy Brief seeks to provide concrete recommendations on how the protection of privacy and personal data could be strengthened within specific social protection program¬mes and social protection systems in general.

Developing privacy policies and specific operational guidelines for data protection in social protection programmes

Even when countries have data protection laws, there must be specific regulations on data protection applicable to social protection systems that ensure social protection personnel are familiar with the provisions of the law and know how they should be implemented in the specific case of social protection programmes. **Several measures could support this goal:**

- Develop sector-specific data protection policies. Enacting data protection policy applicable to the entire social protection system would facilitate the implementation of consistent data protection legislation throughout a given country's social protection programmes.
- Develop data protection guidelines which would complement policy and facilitate implementation. In Ireland, for example, the Department of Social Protection has developed a Data Protection Policy alongside detailed guidelines that ensure all staff (and others who process personal data on behalf of the department) act in accordance with federal Data Protection Act principles.
- Include data protection provisions in programme operational manuals. This has been seen in flagship programmes like Chile Solidario and Prospera.

Specific regulation facilitates the operational duties of staff while freeing them from a need to understand every complexity in general data protection laws or outcome of reform. Regulations should be widely disseminated among programme staff and should be supported by formal training.

The mere existence of specific regulations or policies may not provide adequate protection in the absence of proper oversight and enforcement. Therefore, the appointment of privacy and data protection committees or officers is advisable to ensure the implementation of data security controls, monitor Management Information Systems and Information Technology security status and respond to information security incidents. These committees or officers should report directly to the highest authority within the programme or the social protection system.

Specific privacy and data protection regulations or policies should include:

- The type of information to be processed and the purpose for such information.
- How long the information will be retained.
- Who will be able to access the information, and how.
- How individuals access their proprietary information and how they can correct or update it.
- Complaints and enquiry systems that include avenues for redress.
- Expressly identifying authorities in charge of monitoring compliance.
- How regulations or policies will be promoted among staff; incentives as well as non-compliance sanctions.

Ensuring access to personal data

Social protection programme beneficiaries should have access to personal data the programme may hold, free from constraint, undue delay or expense. This includes information on processed data categories; the purpose for processing; who receives it; and the "logic" that underlies any automatic processing of personal information.

Information should be provided upon request regarding any decisions programme authorities make with reference to applicants or beneficiaries, in particular if such decisions limit or terminate benefit access. Such a consideration is key for applicants who have not successfully completed the enrolment process, enabling them to appeal exclusions.

Providing information access to beneficiaries is not only a right. It is, as well, a good mechanism for ensuring data accuracy, since beneficiaries can check their corresponding data entries. This right to access programme information is closely related to other rights such as the right to due process in administrative proceedings – including the right to be heard before decisions are taken – and the right to an effective remedy.

Individuals should be able to access their personal data:

- At any stage of the programme, free from discrimination.
- By an expeditious, economically accessible mechanism that enables them to correct or update their information as necessary.
- In an easily understood manner.

Implementing appropriate data security measures

Social protection authorities and private entities with access to social protection programme information should implement appropriate institutional, technical and physical measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

This requires social protection authorities identify, evaluate and prioritize security risks which may negatively impact beneficiaries. Assessments should be undertaken regularly when programmes adopt new technologies such as biometric identification.

Exemplary data security measures can include:

- Developing secure physical and digital infrastructure.
- Securing premises and preventing unauthorized physical access to IT infrastructure.
- Securing connections and measures to define and protect logical security perimeters, such as firewalls, intrusion-prevention and -detection systems.
- Requesting IT system authorization and authentication procedures.
- Data encryption.
- Limiting access to specific, accredited staff; employee screening and clear enunciation of roles and responsibilities.
- Regular updates on data security rules to all social protection staff, alongside information on their obligations and ongoing data security training.
- Clear distribution of data-processing responsibilities.
- Implementing organizational measures to ensure appropriate reaction to security incidents, in particular personal data breaches.

Regulating data-sharing between government agencies

To ensure positive results and minimize risks to privacy and data protection, social protection programme information sharing must be based on full transparency and must feature beneficiary consent and well-established lines of accountability. The onus should fall on social protection authorities to demonstrate that any linkage between public databases is legal, necessary and proportional to end goals, fully in line with programme/system purposes. Meaningful and proportional sanctions must be in place in case of any contravention. Sharing social protection data with law enforcement officials, intelligence bodies and other State organs whose duties are not directly linked to social protection programme purposes (for which the data was collected) should be expressly prohibited. Social protection programmes

should not be used to profile or fingerprint those living in poverty.

At a minimum, the database links should be:

- Expressly authorised by law and further regulated by a Memorandum of Understanding between the two agencies. At a minimum, the law should prescribe what information should be disclosed; to which agencies/programmes; under what circumstances; the conditions for disclosure and lines of accountability.
- Strictly necessary and proportional to end goals, fully in line with programme/system purposes and not discriminatory.
- Transparent. Individuals should be informed about shared databases; affected individuals should consent to sharing information.
- Secure. Safeguards must ensure any sharing agreements (e.g. memoranda of understanding, contracts, or head-of-agency agreements) comply with domestic legislation and international standards.
- Accountable. Precise mechanisms should be in place to monitor and evaluate the implementation and impacts of data- and information-sharing initiatives.

Regulating private sector involvement

When the private sector is involved in social protection programme-related identification, registration or payments, it is important to establish strong privacy protections tailored to the nature of the information disclosed. A system of safeguards should prevent and sanction abuses or negligence regarding information shared. It should also eliminate or minimize the possibility that private actors take advantage of their access to collected programme data for unforeseen or lucrative ends and/or to the detriment of beneficiary interests or those of society at large.

Transparent, legally binding agreements that establish, inter alia, clear roles and responsibilities for parties; safeguards to prevent abuses; strict rules for database management and security; and specific mechanisms to control external contractors (e.g. surprise inspections) should regulate private sector involvement. Overall, programme beneficiary security, privacy and personal data should take precedence over private interests.

In line with the United Nations Guiding Principles on Business and Human Rights , private companies should establish appropriate due diligence policies to identify, assess, prevent and mitigate any adverse impact on enjoyment of rights, including the right to privacy and personal data protection in connection with the business activities of the company. The Guiding Principles note that when enterprises have caused or contributed to negative human rights impacts, they have the responsibility to ensure remedies.

Contracts between social protection authorities and the private sector should enumerate:

- Benefits to the public as well as data subjects that stem from the company handling data.
- How the company will use information and how it will be managed between the company and the government.
- Who owns the data and what accreditation mechanisms will govern data access and use.
- Who is responsible for data processing related technical and procedural problems.
- Who monitors contract compliance.
- Who responds in case of abuses or negligence.
- Sanctions for breaches.

Establishing clear lines of accountability

Data protection authorities exist in some countries with data protection laws. When oversight bodies are in place, they should be afforded both mandates and resources to address social protection programme data protection issues.

Clear responsibilities and lines of accountability for privacy and data protection should be established as part of every social protection programme. One good practice is establishing specific oversight mechanisms within programmes (e.g. chief privacy officers) whose mandate is addressing data protection issues. Operational guidelines and staff manuals should also enumerate processes for reporting incidents, weaknesses and software malfunctions that may compromise privacy and data protection.

Ensuring accountability means guaranteeing transparency about how the data is collected, stored, used and potentially shared with other agencies/databases, as a fundament to raising concerns, making informed decisions or tendering complaints.

Checklist:

- At the national level, there is a well-resourced data protection authority with a mandate to address privacy and data security breaches in social protection programmes.
- At the sector level, there is an identifiable authority with final responsibility regarding privacy and data security.
- At the programme level, both an oversight mechanism (e.g. a chief privacy officer) and an express regulatory framework (i.e. operational guidelines and staff manuals) are in place.

Promoting continuous capacity-building and training of programme staff

Social protection programmes should ensure personnel can both perform technical tasks effectively (e.g. undertake data-capture, data-entry and system supervision) and also manage legal knowledge related to data- and privacy-protection. Because social protection practitioners often lack related skills, capacity-building in these areas is critical.

Staff training and awareness efforts should enable personnel to:

- Assess risks that arise from programme data collection.
- Develop better understandings of data protection principles and how they should be applied in social protection systems.
- Understand which remedies or improved practices can be activated to ensure privacy and data protection.
- Exercise managerial monitoring and supervision for privacy and data protection.

Many countries face additional challenges when ensuring necessary physical and technical support for protecting privacy and data. This may include, for example, access to adequate IT support services for those working with MIS or access to adequate physical infrastructure to undertake beneficiary interviews.

Endnotes

[1] As of June 2017, 120 countries have adopted data privacy laws, including Albania, Angola, Argentina, Bulgaria, Chile, Colombia, Costa Rica, Ghana, Mauritius, Mexico, Moldova, Morocco, Nepal, Nicaragua, Paraguay, Peru, the Philippines, Senegal, Tunisia, Vietnam and Zimbabwe. For the full list of countries see Greenleaf, G. 2017. Global Tables of Data Privacy Laws and Bills (5th Ed 2017), 145 Privacy Laws & Business International Report, 14-26. Available at SSRN: https://ssrn.com/abstract=2992986 [10 May 2018].

[2] See e.g. human rights instruments such as the Universal Declaration of Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17), the Convention on the Rights of the Child (Article 16), and the International Convention on the Protection of All Migrant Workers and Members of Their Families (Article 14). See also specific instruments dealing with the protection of personal data, such as the United Nations Guidelines for the Regulation of Computerized Personal Data Files (1990), the Organization for Economic Cooperation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013), the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) (1985), Additional Protocol to Convention 108 regarding supervisory authorities and transborder data flows (1999) and Council Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (1995) (EU Data Protection Directive)..

[3] Decree No. 235 (2004), which regulates the application of Law No. 19.949, that created Chile Solidario establishes the responsibility of the Ministry of Planning and Cooperation (Ministerio de Planificacion y Cooperación, MIDEPLAN), in guaranteeing the protection of privacy and data of beneficiaries (Art. 7). In October 2011, MIDEPLAN became the Ministry of Social Development.

[4] Decree of 30 December 2014, Arts. 9 and 12.

[5] See EDPS (European Data Protection Supervisor). 2014. Guidelines on data protection in EU financial services regulation (Brussels). Available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Thematic%20Guidelines/14-11-25_Financial_Guidelines_EN.pdf [22 May 2018].

[6] Office of the United Nations High Commissioner for Human Rights. 2011. Guiding Principles on Business and Human Rights (New York, United Nations). A/HRC/17/31, endorsed by the Human Rights Council in resolution 17/4, on 16 June 2011. Available at: http://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_en.pdf [9 May 2018].

This issue brief has been prepared by Magdalena Sepúlveda Carmona, based on M. Sepúlveda Carmona (2018) Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection. Extension of Social Protection ESS Working Paper No. 59 (Geneva, International Labour Organization).

The editor of the series is Isabel Ortiz, Director of the Social Protection Department, International Labour Organization (ILO). For more information, contact: ortizi@ilo.org.

International Labour Office, 4, route des Morillons, 1211 Genève 22, Switzerland

Visit our websites:
- www.social-protection.org
- www.ilo.org.