USAID
FROM THE AMERICAN PEOPLE

PERSONAL DATA
PROTECTION SERVICE

MINIMUM STANDARDS FOR PERSONAL DATA PROTECTION OFFICERS

TBILISI, 2024

These minimum standards are made possible by the support of the United States Agency for International Development (USAID). The content is the responsibility of the Personal Data Protection Service of Georgia and does not necessarily reflect the views of USAID or the United States Government.

Table of Contents

PURPOSE OF THESE RECOMMENDATIONS

The purpose of these recommendations is to provide minimum standards for selecting and training data protection officers under the Law of Georgia on Personal Data Protection. Together with Normative Acts and recommendations from the Personal Data Protection Service of Georgia, they act as a cornerstone for enhancing data protection practices, safeguarding sensitive information, and ensuring legal compliance with the Law.

These minimum standards provide clear and standardized expectations for organizations when designating or appointing individuals to serve as DPOs. For DPOs, they set the baseline for the knowledge, skills, and character expected of them. These minimum standards are also intended to ensure consistency and quality in the development of DPO training by third parties.

These recommendations were developed with reference to the EU's General Data Protection Regulation and align with European standards of excellence and professionalism. They ensure that DPOs and training programs for DPOs reflect best standards and are relevant and effective. These standards instill confidence among stakeholders that DPOs are effectively serving their organizations to meet the requirements of the Law of Georgia on Personal Data Protection.

METHODOLOGY

These recommendations were drafted to meet the goals and requirements of the Law of Georgia on Personal Data Protection, with due regard given to international best practices and input from interested parties.

Through adoption and implementation of its Law, Georgia joins jurisdictions around the world in recognizing the critical role a DPO plays in how personal data is used by an organization. In addition to the EU Member States by virtue of the GDPR, the role of DPO is also required in Australia, Brazil, Singapore, the United Kingdom, and many other countries.

These recommendations were crafted by examining best practices encouraged by regulators, in particular:

- Article 29 Working Party Guidelines on Data Protection Officers (endorsed by the European Data Protection Board)
- European Data Protection Supervisor's Position Paper on the Role of DPO
- CNIL's Guide on Data Protection Officers
- ICO Guidance on Data Protection Officers

These recommendations looked at how leading international organizations such as Microsoft, Mastercard, and the World Bank view the qualifications and skills necessary for the role of DPO. And these recommendations were informed by best practices promulgated by organizations such as the International Association of Privacy Professionals (IAPP) and the Centre for Information Policy Leadership (CIPL),

These recommendations were also influenced by consultations and conversations with interested parties, who voiced their optimism, wishes and concerns for the role of DPO. These consultations included meetings with representatives from:

- PDPS
- European Commission's International Digital Cooperation Project
- Law and Public Policy Center
- E-Commerce Association
- Grigol Robakidze University
- Institute for Development of Freedom of Information
- Transparency International Georgia
- Bank of Georgia
- National Center for Educational Quality Enhancement
- Public Service Development Agency

INTRODUCTION

The Law of Georgia on Personal Data Protection was enacted "to ensure the protection of fundamental human rights and freedoms, including the right to the inviolability of private and family life, and to privacy and communication, in the processing of personal data."[1] Toward this purpose the Law expects organizations to process data in a lawful manner, with due regard for the rights of data subjects, to implement appropriate technical and organizational measures to ensure processing in accordance with the Law, and to maintain proper documentation to demonstrate compliance with the Law.

The Law obligates public institutions, specific commercial enterprises, and data controllers and processors that process the data of a significant number of data subjects and/or carry out systematic and large-scale monitoring of their behavior, to appoint a data protection officer. The Law sets forth the DPO's primary responsibilities, to whom the DPO is accountable within the organization, and the involvement of the DPO in the organization's decisions regarding data processing.

The DPO is required to have "appropriate knowledge in the field of data protection."[2] To meet this standard, the Personal Data Protection Service of Georgia expects a DPO to possess at the time of their designation or appointment (or to develop shortly thereafter):

- In-depth knowledge of the Law;
- The skills to carry out the specific duties required of a DPO;
- The personal demeanor to promote, facilitate and achieve the organization's compliance with the Law; and
- An understanding of (and at the Organization's discretion responsibility for) the documentation required to demonstrate compliance with the Law.

An effective DPO will also have a basic knowledge of information technology, data security, and artificial intelligence; knowledge of the organization's business, its organizational structure, and industry regulations; and, for public institutions, an understanding of the applicable administrative rules and procedures.

The following non-binding minimum standards are intended to be used as a guideline for selecting and training persons to serve as DPOs.

[1] Law of Georgia on Personal Data Protection, Article 1.
[2] Law of Georgia on Personal Data Protection, Article 33(5).

GENERAL OVERVIEW OF THE LAW OF GEORGIA ON PERSONAL DATA PROTECTION

To strengthen the standards and guarantees for the protection of personal data and privacy, a new Law "On Personal Data Protection" was drafted and adopted by the Parliament of Georgia on 14 June 2023, the main part of which entered into force on 1 March this year. The new Law establishes internationally recognized standards for the protection of personal data, which is a significant step towards harmonization with European legislation. It defines the institutional independence of the Personal Data Protection Service of Georgia as a state authority and introduces several new institutions and legislative innovations.

Harmonization and consolidation of the legal basis for the protection of personal data are obligations assumed by Georgia under the Association Agreement with the European Union and the Association Agenda. For Georgia, as a country in the process of European legal culture and European integration, it is extremely important to harmonize Georgian legislation on personal data protection with EU legislation and, accordingly, to implement new democratic standards at the national level. The values and standards of the GDPR have been incorporated into the new Law. As a result of the implementation of the new Law "On Personal Data Protection", the legal framework for the protection of personal data will be in line with the EU legislation, thus ensuring the effective protection of human rights and freedoms, including privacy, in the processing of personal data and providing the independent data protection supervisory authority with appropriate mechanisms and powers.

The new Law significantly increases the rights of data subjects and extends the guarantees of their protection. Legal novelties concern the rules on data processing for direct marketing purposes. Furthermore, the legislation introduces provisions for audio monitoring, laying down specific legal grounds and requirements.

In line with the GDPR of the European Union, Georgian law establishes the obligation to designate or appoint a personal data protection officer in public institutions and private organizations, defines the concept of an officer and regulates other basic issues related to it.

THE PERSONAL DATA PROTECTION OFFICER

Emerging in 2018 with the entry into force of the General Data Protection Regulation in the European Union, [3] the data protection officer has become a key role in how an organization manages personal data governance. The following summarizes the role of the DPO under the Law of Georgia on Personal Data Protection.

Entities Obligated to Appoint a DPO[4]

Under the Law, a DPO is required for public institutions, insurance organizations, commercial banks, micro-finance organizations, credit bureaus, electronic communication companies, airlines, airports, medical institutions, and organizations that process the data of a significant number of data subjects or carry out systematic and large-scale monitoring of data subjects' behavior. [5] Other organizations have the right to appoint a DPO, at their discretion. Controllers and processors are required to provide the Personal Data Protection Service with information on the identity of and contact details for the DPO.[6]

The Functions of a DPO

The DPO is an essential role for an organization's ability to achieve and maintain compliance with data protection requirements. The DPO informs and advises the organization, monitors its compliance with legal obligations, and acts as a point of contact with the regulatory authority and data subjects.

The overarching role of the DPO is to facilitate and monitor the organization's compliance with the Law. Specifically, the DPO:

- Informs the organization and its employees on matters related to data protection;
- Participates in the development of internal regulations related to data protection;
- Participates in the development and implementation of data protection impact assessments;

[3] Before the adoption of GDPR, the practice of appointing a DPO developed in several EU Member States as a cornerstone of accountability with the belief that appointing a DPO can facilitate compliance and provide a competitive advantage for organizations.
[4] *See* Law of Georgia on Personal Data Protection, Article 33.
[5] Please see, the Normative Act of the President of Personal Data Protection Service "On determining the circle of persons responsible for processing and persons authorized for processing, who do not have the obligation to appoint or designate a personal data protection officer" as of 28/02/2024, https://matsne.gov.ge/ka/document/view/6117102?publication=0.
[6] *See* Law of Georgia on Personal Data Protection, Article 33(8).

- Monitors the organization's compliance with its internal regulations and the Law;

- Analyzes data subject applications and grievances and recommends appropriate responses;

- Represents the organization in its relationship with PDPS, submits information and documentation at its request, and coordinates and monitors PDPS recommendation;

- Provides, at the request of a data subject, information on data processing and data subject rights; and

- Performs other functions to ensure the improvement of the organization's data processing.[7]

General Principles for a DPO

Competence

The Law requires personal data protection officers to have appropriate knowledge in the field of data protection,[8] but does not establish specific qualification requirements. This aligns with the GDPR, which states that a DPO is designated "on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks [of a DPO]."[9] And similar to the Law, the GDPR does not establish a direct requirement for the qualification of DPOs.

European countries subject to GDPR take different approaches on this matter. France and Latvia introduced measures to verify the qualification of a DPO through certification requirement or qualification exam. The UK, Germany and Spain do not explicitly establish certification or licensing requirements.[10]

Regardless of whether certification is mandatory, interested individuals can pursue international online certification courses, such as Apave Certification, IAPP Certification, ITCERTS, EU GDPR Training and Certification.[11]

[7] *See* Law of Georgia on Personal Data Protection, Article 33(1)(a-f).
[8] *See* Law of Georgia on Personal Data Protection, Article 33(5).
[9] European Union General Data Protection Regulation, Article 37(5).
[10] Recommendations on Personal Data Protection Officer, PDPS: https://shorturl.at/qW2dZ
[11] Ibid.

Independence and Impartiality

The Law recognizes the importance of independence, impartiality and conflicts of interest when fulfilling the role of DPO.[12] To achieve this, the Law provides that the DPO is accountable to the highest governance structure within the organization, taking into account the specific circumstances.[13] The role of the DPO may be fulfilled by an organization's employee or may be outsourced to a third party on a contractual basis. The DPO may perform other functions for the organization, and act as DPO for more than one organization, unless there is a conflict of interest.

The importance of independence, impartiality and conflict of interest are also found in the GDPR,[14] and regulators from EU countries have addressed this. For example, enforcement actions clarify that regulators in EU countries find:

- There is a conflict of interest when the DPO is in a position to make substantial decisions regarding data processing activities;

- The autonomy or independence of a DPO may be compromised if the DPO also serves as head of compliance, audit and risk management; and

- Two hierarchical layers between the DPO and executive level management does not give the DPO direct access to the highest level of management, even though the DPO had regular meetings with the board.

Rights and Liability

The Law provides that the DPO has the right to be involved in the organization's important decisions about processing activities, is to be provided with appropriate resources, and to carry out the DPOs duties autonomously.[15]

The DPO is not personally liable for the organization's compliance with the Law. Rather, compliance with the Law is the organization's responsibility.[16] The Law states that the DPO "informs," "participates," "monitors," and "analyzes" the organization's compliance with the Law. The DPO is required to fulfill the duties of the role, subject to the organization's performance and disciplinary standards.

[12] This is again aligned with the GDPR. *See* European Union General Data Protection Regulation, Article 38.
[13] *See* Law of Georgia on Personal Data Protection, Article 33(6).
[14] *See European Union General Data Protection Regulation, Article 38.*
[15] *See* Law of Georgia on Personal Data Protection, Article 33(7).
[16] This is also in line with the GDPR and the European Data Protection Board. *See* Article 29 Working Party Guidelines on Data Protection Officers (endorsed by the European Data Protection Board), Annex (12).

A Note on Risk, Risk Analysis, and Risk Mitigation

Risk, risk analysis, and risk mitigation play an important role in data protection and data privacy. The risk-based approach is an effective tool for ensuring a high level of protection of the rights and freedoms of individuals while advancing an organization's interests and promoting innovation.

The concept of risk is noted throughout the Law. For example, maintaining adequate security measures requires an account of possible threats of violation of the rights of data subjects.[17] A data protection impact assessment is required if there is a high probability of threat of violation of fundamental human rights and freedoms during data processing.[18] Admissible grounds for data processing includes the protection of legitimate interests of the organization unless there is an overriding interest in protecting the rights of a data subject.[19]

Risk analysis requires an assessment of adverse consequences balanced by the benefits of a processing activity. This requires understanding the likelihood and severity of an adverse consequence to data subjects as result of the organization's use of personal data and balancing that risk against the benefits of the processing activity. "Likelihood" means how likely is it that the risk or impact of the risk may materialize. "Severity" means the magnitude of the risk or its impact if it materializes. "Adverse consequences," or harms, to data subjects can be physical, psychological, economic, reputational, discrimination, or autonomy.

If a risk analysis reveals an unacceptable level of risk, mitigation measures include data pseudonymization and data depersonalization. Other risk mitigation measures to consider include: limiting access and data sharing; limiting use by third parties; limiting geographical scope; restricting subsequent processing; enhancing transparency; implementing new or enhanced security measures; training employees; deciding not to process particular types of data; limiting retention periods; ensuring secure and permanent personal data deletion; using systems that allow individuals to access their personal data more easily; taking steps to ensure that individuals are fully aware of how their personal data are used and can contact the organization for assistance; using reputable data processors with written agreements on how data will be processed; using data-sharing agreements that make clear what information will be shared, how it will be shared and who it will be shared with; and numerous other specific compliance and governance controls that address the specific nature of the identified risks.

The DPO plays an important role in assisting the organization in identifying, assessing, and managing risks related to the organization's processing of personal data.

[17] *See* Law of Georgia on Personal Data Protection, Article 27(3).
[18] *See* Law of Georgia on Personal Data Protection, Article 31(1).
[19] *See* Law of Georgia on Personal Data Protection, Article 5(1)(i).

KNOWLEDGE, SKILLS, AND CHARACTER

Knowledge: Understanding the Law of Georgia on Personal Data Protection

A data protection officer is expected to have a thorough and robust understanding of the Law and its application to the organization. Specific training on and study of the following is critical.[20]

Purpose of the Law:	To ensure the protection of fundamental human rights and freedoms, including the right to the inviolability of private and family life, and to privacy and communication, in the processing of personal data.

Scope of the Law:	• The processing of data by automated means within the territory of Georgia
	• The processing of data which form part of a filing system or are processed to form part of a filing system
	• The processing of data by a controller not established in Georgia using technical means available in Georgia (other than technical means used solely for the transit of data)
	• Exceptions:
	  ○ Natural persons for personal or household activities
	  ○ National security
	  ○ State secrets
	  ○ Court proceedings
	  ○ Mass media
	  ○ Academic, artistic, or literary purposes

(Select) Definitions:	• Personal data
	• Special categories of data
	  • Data concerning health
	  • Biometric data
	  • Genetic data
	• Processing of data
	• Automated data processing
	• Filing system
	• Data subject

[20] Robust knowledge of certain chapters of the Law is encouraged but not critical for establishing minimum standards for the role of DPO.

	• Consent of the data subject • Controller • Processor • Video monitoring • Audio monitoring • Direct marketing • Profiling • Data depersonalization • Data pseudonymization • Incident
Principles of Data Processing:	• Lawfulness, fairness, and transparency • Specific, explicit, and legitimate purposes • Necessity and proportionality • Accuracy • Storage limitation • Security • Purpose limitation (and exceptions)

Grounds for Data Processing	• Processing based on consent
	• Processing that is necessary for:
	  ○ Contractual obligation
	  ○ Statutory duty
	  ○ Vital interests of data subject or other persons (e.g., pandemics)
	  ○ Substantial public interest (e.g., crime prevention)
	• Processing when data are publicly available
	• Processing that is provided for by law
	• Processing special categories of data
	• Processing data related to:
	  ○ Minors
	  ○ Deceased persons
	  ○ Biometrics
	• Rules for video monitoring
	• Rules for audio monitoring
	• Rules for direct marketing

Data Subjects' Rights:	• Right to receive information on the processing of data • Right to access and obtain copies of data • Right to rectify, update, and complete data • Right to terminate the processing of data, and erase or destroy data

	• Right to the blocking of data • Right to the transmission of data • Right not to be subject to automated decision-making • Right to withdrawal of consent to processing data • Restrictions on data subjects' rights ○ Right to appeal

Obligations of Controllers and Processors:	• Overarching obligation to protect the rights of data subjects
	• Obligation to inform data subjects about processing
	  ○ When data is collected by controller
	  ○ When data is collected by another party
	  ○ Specific information on data subject consent and withdrawal of consent
	• Obligation to prioritize data masking when creating a new product or service
	• Obligation to implement appropriate technical and organizational measures to:
	  ○ Ensure processing of data in accordance with the Law, and Protect against the risks of data processing to ensure protection of data against loss or unlawful processing, including destruction, deletion, alteration, disclosure or use
	• Obligation to maintain a register of information related to data processing
	• Obligation to notify PDPS and data subjects about (certain) incidents
	• Obligation to carry out data protection impact assessments
	• Obligation to appoint or designate a personal data protection officer
	• Obligation to appoint or designate a special representative
	• Obligation to determine and document in advance responsibilities of each party when there are joint controllers or there is a processor that processes on behalf of a controller
	• Obligations related to the organization's relationship with the PDPS

International Data Transfers:	• Lawful transfers of data to another state and international organization • State and international organizations with adequate safeguards for data transfers, as determined by PDPS

PDPS Main Activities:	• PDPS monitors the lawfulness of data processing in Georgia • Provides consultations on matters related to data protection • Reviews applications (by data subjects) related to data protection • Examines and inspects lawfulness of data processing • Informs and raises awareness of data protection among the public

Administrative Offences and Liabilities:	• PDPS may apply the following for a violation of the Law:
	  ○ Remedy the violation(s)
	  ○ Suspend data processing
	  ○ Terminate data processing
	  ○ Terminate data transfer to another state and international organization
	  ○ Provide written advice and recommendations
	  ○ Impose administrative liability
	• Liabilities for administrative offences are tied to specifics of the offence

Skills: Developing the Credentials of a Data Protection Officer

The DPO role can be separated into several distinct functions: information and awareness, advisory, organizational, cooperative, and compliance. A DPO is expected to have the skills to fulfill these functions.

Information and Awareness Function	• Define and implement an ongoing strategy to communicate within the organization the obligations, responsibilities, and goals under the Law, for example through:
	  ○ Staff information notes and memoranda
	  ○ Training sessions
	  ○ Bespoke outreach to business units
	  ○ Website(s)
	  ○ Data Protection Day events[21]
	• Assist relevant business units in developing, publishing, and maintaining data privacy notices:

[21] *See, e.g.,* https://www.edps.europa.eu/data-protection/our-work/publications/events/european-data-protection-day-0_en.

	○ For all categories of data subjects (e.g., employees and prospective employees, customers and prospective customers, website users) ○ With information for data subjects tailored to how the data is collected[22] ○ And the specific requirements when data processing is based on consent from the data subject
Advisory Function:	• Advise the organization on appropriate privacy-enhancing technologies and organizational measures to mitigate the risks of loss and unlawful processing, for example through: ○ Data classification (public, confidential, restricted) ○ Data pseudonymization ○ Data masking ○ Data de-identification ○ Access restrictions ○ Data minimization ○ Data retention and disposal ○ Physical controls • Advise the organization on notification requirements when an incident occurs, including: ○ Timing of notices ○ Delivery of notices to the PDPS ○ Delivery of notices to data subjects when there is a high probability that an incident will cause significant damage or pose a significant threat to fundamental human rights and freedoms ○ Content of notices ○ Presentation of notices in simple and understandable terms • Advise the organization on carrying out data protection impact assessments (DPIA) ○ A DPIA is obligatory when there is a high probability of threat of violation of fundamental human rights and freedoms ▪ DPIA in advance of a data processing activity ▪ Taking into account the new technologies, categories and volume of data, and the purpose and means of processing ○ A DPIA is mandatory when a controller:

[22] *See* Law of Georgia on Personal Data Protection, Articles 24 and 25.

	▪ Makes decisions in a fully automated manner, including profiling, that have legal, financial, or other significant consequences for data subjects ▪ Processes data of a special category of a large number of data subjects ▪ Carries out systemic and large-scale monitoring of data subjects' behavior in public spaces o The appropriate methodology to use for carrying out DPIAs o The development of documentation that describes the data category, purposes, proportionality, process and grounds of data processing; an assessment of threats of violation of fundamental human rights and freedoms; description of organizational and technical measures taken for data security o What safeguards (including organizational and technical measures) to apply to mitigate any risks to the rights and interests of data subjects o When the PDPS should be consulted o Whether the DPIA has been carried out appropriately o Whether the DPIA's conclusions meet the requirements of the Law • Advise and make recommendations when a data subject submits an application or grievance regarding the organization's data processing
Organizational Function:	• Participate in developing, implementing, and socializing internal policies, procedures, and guidance that: o Identify roles, responsibilities, and reporting structures for data processing within each business unit o Identify individual focal points or champions in each business unit to interact with DPO o Set standards, practices and protocols for the organization so its data processing meets the requirements of the Law • Participate in creating and maintaining a register of data processing information that contains: o Identity and contact details of the controller, special representative, DPO, joint controller, and processor o Objectives of the data processing activities o Data subjects and data categories o Categories of data recipients

	○ Any transfers of data to another state or international organization, with guarantees of data protection and any permits from the PDPS ○ How long data will be stored ○ A general description of the organizational and technical measures taken to ensure data security ○ Information on incidents (if any) • Participate in the engagement and management of processors ○ Conduct vendor assessments to determine processors' ability to meet the requirements of the Law and the organization's protocols ○ Include contractual safeguards to protect the organization • Participate in the development and implementation of incident response procedures to: ○ Assess the risk of the incident ○ Contain the incident ○ Identify and implement remediation measures ○ Report to the PDPS and data subjects ○ Conduct a post-incident investigation and mitigate future risks ○ Maintain an incident register and related documentation ○ Conduct periodic table-top exercises to improve incident response procedures.
Cooperative Function:	• Serve as the contact person for the organization on data protection issues with: ○ The organization's employees and management ○ Data subjects ○ PDPS • Consult with the PDPS when a DPIA indicates that a data processing activity presents a high risk of violation of fundamental human rights and freedoms • Provide data subjects with information on their data processing and their rights when they make an application
Compliance Function:	• Promote a culture that encourages compliance with the Law • Maintain internal policies, procedures and guidance that instruct the organization on how to meet the requirements of the Law

	• Interpret legal requirements and ensure that the organization's policies, procedures and guidance comply with the Law • Seek authority, resources and visibility to promote compliance with the Law • Provide ongoing training and communication on meeting the requirements of the Law • Report internally on status and concerns with the organization meeting the requirements of the Law • Develop incentives and discipline to promote and enforce compliance with the Law • Investigate and remediate actual or suspected non-compliance with the Law • Provide due diligence and oversight of relationships with third parties whose actions can create significant risk of non-compliance with the Law • Monitor and audit the organization's compliance with the Law

Character: Possessing the Personal Qualities of a Data Protection Officer

A DPO is expected to have integrity, a willingness to stay on top of developments in data protection, the ability to solve problems and effectively analyze risk, and to present effective communication skills.

Integrity of Character:	A DPO commits to upholding high level of professional ethics and maintaining confidentiality in handling personal data.
Continuous Learner:	A DPO is willing to stay updated on developments in data protection laws, regulations, and best practices to adapt strategies and processes accordingly.
Problem Solver:	A DPO can analyze complex data protection issues and develop practical solutions that balance legal requirements with organizational goals and values.
Risk Analysis:	A DPO can conduct risk assessments that balance the organization's interests, including the use of personal data, and the risk of harm to data subjects from that use.
Interpersonal Skills:	A DPO can communicate effectively, popularize new ideas, and persuade if there is skepticism or an appearance of conflicting priorities or obligations.

DOCUMENTATION

Documentation plays a key role for organizations to achieve and manage compliance with the Law of Georgia on Personal Data Protection. Organizations are required to maintain a data processing register and documentation on data protection impact assessments, provide information to data subjects, and notify the Personal Data Protection Service and data subjects when there is an incident.

Documentation is an essential tool for the data protection officer because it makes it possible to have an exhaustive knowledge of the organization's processing operations implemented and to plan their management to meet the requirements of the Law. While it is the organization that is required to maintain documentation of its compliance, in practice the DPO plays a primary role in this task. To clarify roles and responsibilities, the DPO's mission statement often stipulates that maintaining documentation is one of their tasks (if that is indeed the case) and obligates the organization to provide the DPO with relevant information in order to meet this responsibility.

Basic guidelines are provided below for a data processing register, data protection impact assessments, privacy notices, and responding to incidents.

Data Processing Register[23]

The data processing register, also known as a record of processing activities, is one of the primary tools for a DPO. The register provides an overview of all personal data processing activities carried out by an organization. The register is a tool for managing, monitoring, and demonstrating compliance with the Law. It also informs the DPO when providing information and advice to the organization about its processing activities.

Controllers, special representatives and processors are required to maintain in writing information on how data is processed. The register for controllers and special representatives must include:

- The name and contact details of the controller, special representative, DPO, joint controller and processor;
- The objectives of the data processing;
- Data subjects and data categories;
- Categories of data recipients;

[23] *See* Law of Georgia on Personal Data Protection, Article 28.

- Transfers of data to another state or international organization, as well as appropriate guarantees of data protection, and any permits from PDPS;

- How long data will be stored;

- Organizational and technical measures to ensure data security; and

- Information on incidents.

The register for processors must include:

- The name and contact details of the processor, DPO, controller, joint controller and special representative;

- The types of data processing carried out for the controller;

- Information on transfers of data to another state or international organization;

- Organizational and technical measures to ensure data security; and

- Information on incidents.

Controllers that process biometric data, or carry out video or audio monitoring, are obligated to determine in writing the purpose and other details of such processing.[24] This information could also be incorporated into the controller's data processing register.

In practice the data processing register often includes additional details, such as recording the grounds for processing, including links to relevant privacy notices, and details on data subject consent.

The register must identify each data processing activity separately. In practice this means the DPO interacts with each business unit to determine its individual data processing activities.

The format of the data processing register is determined by each organization. It must be made available to PDPS upon request.

[24] *See* Law of Georgia on Personal Data Protection, Articles 9, 10 and 11.

Data Protection Impact Assessments (DPIA)[25]

The DPO plays an active role assessing the risks of processing. The data protection impact assessment is the process by which a controller can systematically assess and identify the privacy and data protection impacts of products and services. It enables the organization to identify the impact of a processing activity and take the appropriate actions to prevent or, at the very least, minimize the risk of those impacts.

Considering new technologies, categories and volumes of data, and purposes and means of processing, the Law requires a DPIA when:[26]

- A data processing activity presents a high probability of threat of violation of fundamental human rights and freedoms;
- A controller makes decisions in a fully automated manner, including on the basis of profiling, that have legal financial, or other significant consequences for a data subject;
- A controller processes data of a special category of a large number of data subjects; and
- A controller carries out systematic and large-scale monitoring of data subjects' behavior in public spaces.

During the DPIA process, the controller is required to create written documentation containing:

- A description of the data category, and the purposes, proportionality, process, and grounds of data processing; and
- An assessment of possible threats of violation of fundamental human rights and freedoms; and
- A description of the organizational and technical measures provided for data security.

In practice, controllers have broad range to develop processes and documentation that work best for their needs, with the primary goal of demonstrating that the organization has thoroughly considered all risks (including legal, corporate, civil, and reputational) and taken actions to mitigate those risks. Each risk should be mapped to a specific internal control that ensures

[25] *See* Law of Georgia on Personal Data Protection, Article 31.
[26] *See also* the normative act issued by the President of the PDPS that sets the criteria for determining the circumstances giving rise to the obligation for a data protection impact assessment, and procedures for conducting data protection impact assessments.

mitigation techniques are well documented and understood across the organization. There should be separate assessments for categories of data or specific products or services. Organizations should also include who (an individual or a specific role) is responsible for either the specific control or for carrying out a plan to further mitigate the identified risk.

Based on a review of best practices, the following provide general guidelines for conducting and documenting the DPIA process:

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

- Describe the Processing: How will the organization collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? It is often useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

- Describe the Scope of the Processing: What is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

- Describe the Context of the Processing: What is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

- Describe the Purpose(s) of the Processing: What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

- Identify Consultations: Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organization? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

- Detail Necessity and Proportionality: Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent

function creep? How will you ensure data quality and data minimization? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

- Identify and Assess Risks: Describe the source(s) of risk and the nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. What is the likelihood of risk – remote, possible or probable? What would the severity of harm be – minimal, significant or severe? What is the overall risk – low, medium or high?

- Mitigate Risks: Identify measures to reduce or eliminate risks identified as medium or high risk. What is the effect on mitigation measures – are they eliminated, reduced or accepted? What is the residual risk – low, medium or high? Were mitigation measures approved, and if not, why?

Is There a High Risk of Violation of Fundamental Human Rights and Freedoms?
If the DPIA indicates a high risk of violation of fundamental human rights and freedoms, all necessary measures must be taken to substantially mitigate those risks. Where the threat of violation of fundamental human rights and freedoms cannot be mitigated by organizational and technical measures, the processing is not allowed. Consultation with the PDPS on whether there is a high risk of violation of fundamental human rights and freedoms, and whether mitigation measures are sufficient, is highly recommended.

- Indicate how the DPIA was Administered: Record who approved or rejected risk mitigation measures and integrate actions approved into project plan, with date and responsibility for completion. Record who approved residual risks. Record advice provided during the consultative process. Record the advice provided by the DPO, including mitigation measures and whether processing complies with the Law, and whether that advice was accepted or rejected and by whom.

Privacy Notices[27]

Privacy notices, also called privacy statements, address the requirement of transparency when organizations process personal data.[28] Transparency, an overarching obligation under the Law and intrinsically linked to fairness and accountability, is about engendering trust in the processes that affect data subjects. Privacy notices enable data subjects to understand, and if necessary, challenge those processes.

Privacy notices are a vehicle to provide information and resources to data subjects. The information must be presented to data subjects before or at the beginning of processing, and in simple and understandable language. They may be presented orally or in writing.[29] The Law prescribes the minimum information to present to data subjects, including:

- Name and contact details of the controller and processor (if any);
- Purposes and legal bases of the processing of data;
- Whether providing data is mandatory;
- The controller's legitimate interests (if applicable);
- Name and contact details of the DPO;
- Who will receive the personal data;
- Information on transfers of data;
- How long data will be stored; and
- The rights of the data subjects.

There is an inherent tension between providing enough information to data subjects and presenting that information in a concise, transparent, intelligible manner that is easily accessible. Organizations may use creative methods such as icons, emojis, flow charts, audio and video, and other approaches to balance these considerations.

[27] *See* Law of Georgia on Personal Data Protection, Articles 4, 13, 24, 25, and 32.
[28] *See* Law of Georgia on Personal Data Protection, Article 4.
[29] Information may be provided orally or in writing (including electronically), unless the data subject requests the provision of information in writing. *See* Law of Georgia on Personal Data Protection, Article 24(5). If information is provided orally, it is best practice to maintain a written record of what, when and how information is provided.

To address this in the digital context, layered privacy notices provide links to the various categories of information that must be provided to the data subject. This can help resolve the tension between completeness and understanding by allowing users to navigate directly to the section of the notice they wish to read.

Incidents[30]

The DPO plays a key role in assisting with the prevention of incidents by providing advice and monitoring compliance with the Law. When incidents involving personal data do occur, the DPO is a central member of the incident response team. The DPO is involved with, and often responsible for, maintaining documentation related to incident response procedures and internal registers of incidents, and drafting notifications to PDPS and data subjects.

Commonly known as a data breach, an "incident" is a "breach of security of data leading to the unlawful or accidental damage or loss of data, or the unauthorised disclosure, destruction, alteration of or access to data or the collection/obtaining of data, or other unauthorized processing."[31] Examples of incidents include:

- Access to data by an unauthorized third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Devices containing personal data being lost or stolen;
- Alteration of personal data without permission; and
- Loss of availability of personal data,
- Etc.

Incident response procedures document how an organization identifies, responds to, and mitigates damage from an incident. These procedures are critical as they serve as the manual to follow in a time of crisis. Incident response procedures provide the steps to take once an incident has been identified. For example:

- Step One: Determine whether personal data is involved. If an incident has been identified, check to see whether personal data is affected. Remember that personal data is any

[30] *See* Law of Georgia on Personal Data Protection, Articles 29, 30.
[31] Law of Georgia on Personal Data Protection, Article 3(z_3).

information relating to an identified or identifiable natural person. This means names and addresses, but also could be photographs, comments on social media, other records, and more.

- Step two: Establish what personal data has been breached. Understand the type and amount of personal data that is involved. The data processing register is a good place to start. The type and amount of personal data involved matters, because the way risk is assessed will vary widely depending on the situation. For example, if the breach involves the sensitive personal information of vulnerable people, or financial information that may lead to identity fraud, these are both likely to be high risk situations. You need to handle sensitive personal information with even more care than other types of personal information.

- Step three: Consider who might have the personal data. If the incident involves someone inappropriately accessing the personal data or it being lost or stolen, consider who might have access to the data now. If someone has been sent the personal information in error, accessed it without your authorization or it has been lost or stolen, then you face different levels of risks depending on who is involved. For example, accidentally sending an email internally to the wrong department in your business is lower risk than sending the same email to an unknown person outside your business.

- Step four: Determine how many people might be affected. It is important to learn how many people might be affected by the incident, whether it's single figures or the hundreds of thousands.

- Step five: Consider how seriously the incident will affect people. Determine how the incident might impact affected data subjects, specifically whether it might cause harm. Thinking about the impact the breach will have on people can help decide what to do to try and limit that impact and protect them from potential further harm. For example, query whether the people involved are vulnerable adults or children; will the incident put someone in an unsafe situation; are people at risk of losing money, their job, or their home because of the incident; might the incident impact people's health and wellbeing.

- Step six: Document everything about the incident. Document the details of how the organization responded to the incident. Include how the incident was discovered and controlled, how the risk of harm to data subjects was mitigated, how residual harm was addressed, and actions taken as well as actions considered but not taken. This documentation will be needed to notify the PDPS and data subjects and to include in the data processing register.

- Step seven: Assess the risk of harm to data subjects and other individuals.[32] From the moment an incident is discovered and until it is controlled, risk of harm to individuals needs to be assessed. Information about incidents is rarely linear, so consider the impact of the incident as it unfolds and until it is considered closed.

- A risk assessment determines the probability of causing significant damage and/or creating a significant threat to human rights and freedoms as a result of the incident. Consider who might be affected, how many people might be affected, and the ways it might affect them. As a result of the incident, the probability of causing significant damage to human rights and freedoms and/or creating a significant threat may be low, medium or high.

Considering risk in the context of an incident:		
Low	The incident is not likely to cause significant harm and/or pose a significant threat to basic human rights and freedoms	For example, data subjects will not be affected, or may encounter minor inconveniences (needing to re-login, set a new password, etc.)
Medium	The incident may cause significant harm and/or create a significant threat to basic human rights and freedoms and the absence of such harm/threat are more or less equal.	For example, data subjects may encounter significant inconveniences, which they will weather despite difficulties (extra costs, temporary loss of access to non-essential services, stress, fear, etc.)
High	The incident is likely to cause significant harm and/or pose a significant threat to basic human rights and freedoms	For example, data subjects may encounter significant harm only surmountable with serious difficulties (worsening of health, loss of employment or funds, property damage, etc.) or irreversible harm that prove insurmountable (substantial debt, long-term psychological issues, bodily harm or death, etc.)

[32] *See* the normative act issued by the President of PDPS that identifies the criteria for determining incidents posing a significant threat to fundamental human rights and freedoms, and the procedure for notifying the Personal Data Protection Service of an incident.

- Step eight: Provide notices.[33] Notices are required by a controller if an incident is expected to cause significant damage or pose a significant threat to fundamental human rights and freedoms. A controller must provide notice of the incident to the PDPS no later than 72 hours after identification of the incident that contains detailed information about the incident and measures taken to control it. A controller must provide notice of the incident to affected data subjects immediately after identification of the incident. A processor must notify a controller immediately about an incident.

DPOs should ensure that employees have been informed about the existence of incident response procedures and mechanisms and that they know their role. Incident procedures are ideally routinely tested through table-top exercises. After each incident is controlled, and at the conclusion of table-top exercises, the incident response procedures should be reviewed and updated based on lessons learned.

[33] Note that the President of the PDPS establishes procedures for notifying the PDPS about an incident. *See* Law of Georgia on Personal Data Protection, Articles 29(9) and 30(4).

SUMMARY OF RECOMMENDATIONS

The data protection officer is a cornerstone of an organization's ability to comply – and demonstrate compliance – with the Law of Georgia on Personal Data Protection. The DPO is a subject matter expert on the Law and data protection in general. The DPO guides the organization in recognizing data protection risks and analyzing and mitigating such risks.

The DPO facilitates the organization's compliance with the Law through the implementation of accountability tools such as the data processing register and the data protection impact assessment. The DPO informs and advises the organization, assists with measures taken by the organization to meet the requirements of the Law, and acts as the point of contact with the Personal Data Protection Service and data subjects.

These recommended minimum standards from the PDPS recognize that a competent DPO possesses, at the time of their designation or appointment or possesses shortly thereafter:

- Knowledge: Sufficient knowledge of the Law of Georgia on Personal Data Protection to translate its requirements to advise and assist the organization in processing personal data in compliance with the Law and normative acts of the President of the PDPS, including those that address the:
    - Criteria for determining incidents posing a significant threat to fundamental human rights and freedoms, and the procedure for notifying the Personal Data Protection Service of an incident;
    - Criteria for determining the circumstances giving rise to the obligation for a data protection impact assessment, and procedures for conducting assessments;
    - Category of persons who are not obliged to designate/appoint a personal data protection officer; and
    - Procedure for registering a special representative with the Personal Data Protection Service.
- Skills: The ability to fulfill the distinct functional areas of the DPO role:
    - Information and Awareness Function
    - Advisory Function
    - Organizational Function

- Cooperative Function
- Compliance Function

- Character: Personal qualities, integrity, and skills to uphold the responsibilities of the DPO.

In addition, a DPO has in-depth knowledge on the substance and process for creating and maintaining detailed documentation that facilitates compliance with the Law and allows the organization to demonstrate its compliance with the Law.