ICMPD
International Centre for Migration Policy Development

ENIGMMA
Putting the pieces together to respond effectively to migration challenges

This project is funded by the European Union

Summary of the Report of a Baseline Study on Personal Data Protection in the Area of Migration Management in Georgia

The baseline study was carried out by the Innovations and Reforms Centre (IRC) in the framework of an EU funded project Enhancing Georgia's Migration Management (ENIGMMA) implemented by the International Centre for Migration Policy Development (ICMPD)

OFFICE OF THE PERSONAL DATA PROTECTION INSPECTOR

IRC
Innovations and Reforms Center

Table of Contents

1. Introduction 4

2. Scope and methodology of the study 5

2.1 Scope 5

2.2 Methodology 6

3. Main observations of the study 7

Part 1 Assessment of the Personal Data Protection Law with regard to international documents related to personal data protection 8

1.1 The Scope of the Law of Georgia on Personal Data Protection 8

1.2 The principles of data processing 9

1.3 The legal basis of data processing 10

1.4 The implementation of the principle of fair processing 11

1.5 Data security 13

1.6 Compliance 13

1.7 Control of data processing by an independent authority 14

1.8 Recommendations for changes to the PDP Law concerning topics found to be of direct relevance in the context of migration management 14

Part 2 Assessment of the migration management sectoral legislation with regard to the requirements of the Personal Data Protection Law and the Convention 16

2.1 The Law of Georgia on The Procedures for Registering Citizens of Georgia and Aliens Residing in Georgia, for Issuing Identity (Residence) Cards and Passports of a Citizen of Georgia (ID Law) 16

2.2 The Law of Georgia on the Legal Status of Aliens and Stateless Persons 18

2.3 The Organic Law of Georgia on Georgian Citizenship 19

2.4 The Law of Georgia on Refugee and Humanitarian Status 20

2.5 The Law of Georgia on Consular Activities 21

2.6 The Law of Georgia on ‘Repatriation of Persons Forcefully Sent into Exile from Georgian SSR by the Former USSR in the 1940s’ 21

2.7 The Law of Georgia on the State Border 22

2.8 Agreement between the European Union and Georgia on the readmission of persons residing without authorisation 23

Part 3 Personal data protection practices in migration management related processes 23

3.1 The LEPL Public Service Development Agency (PSDA) 24

3.1.1 Overview 24
3.1.2 Observations 24
3.1.3 Recommendations 26
3.2 The Ministry of Foreign Affairs (MFA) 27
3.2.1 Overview 27
3.2.2 Observations 27
3.2.3 Recommendations 30
3.3 The Ministry of Internal Affairs (MIA) 30
3.3.1 Overview 30
3.3.2 Observations 31
3.3.3 Recommendations 33
3.4 The Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia (MRA) 33
3.4.1 Overview 33
3.4.2 Observations 33
3.4.3 Recommendations 35
4. Annex: Position of the Public Services Development Agency (PSDA) on the Summary of the Report of a Baseline Study on Personal Data Protection in the Area of Migration Management in Georgia 37

1. Introduction

Personal data protection has recently started to gain wider interest and attention from different stakeholders, however, it still remains at an early stage of development in Georgia. In 2006, Georgia joined the 1981 Council of Europe (CoE) Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.[1] However, it was not until 1 May 2012 that the Law of Georgia on Personal Data Protection[2] entered into force. This was followed by the appointment of a Personal Data Protection Inspector in 2013.

Notwithstanding the number of shortcomings this Law has, we can say that, in general, it is in compliance with the modern European standards. However, at the same time it is worth noting that the Law entered into force at a time and in an environment that were rather unfavourable to its implementation, with:

- virtually no demand for protection of personal data, due to low public awareness about the existence of data protection rights and their importance;
- the inexistence of public servants and lawyers with an in-depth understanding of the issues;
- well-established public sector e-governance and massive databases built without regard for the rules of public sector data processing;
- a lack of manager readiness to allocate necessary resources to personal data protection;
- an absence of privacy activists/advocates; and
- the Inspector's Office being in its early stages of establishment.

Migration management and data protection in this context becomes particularly important, taking into consideration the volume of nationals, as well as foreigners and stateless persons, who are involved in the process. At the same time, taking into consideration the complexity of migration management and the several ministries which have it in the framework of their competences, personal data protection related issues become of further importance.

At the end of 2013, with regard to personal data protection in migration management, there were several concerns to point out: none of the Ministries had in place a policy or guidelines for personal data protection (at the end of 2013 only the Ministry of Internal Affairs said they had been developing a policy document, which was expected to be approved within a short timeframe).

[1] CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 (1981).
[2] Law of Georgia on Personal Data Protection (2011).

Taking into account that the Law on Personal Data Protection is rather general, that there is a lack of expertise on personal data protection in public institutions, and that the Office of the Personal Data Protection Inspector is newly established and its resources are rather limited, this report aims at delivering an assessment of the current state of data protection in Georgian migration management, identifying further room for improvement and providing recommendations for action.

2. Scope and methodology of the study

2.1 Scope

The IRC was commissioned by ICMPD to prepare a baseline study on personal data protection in migration management in Georgia. The main objective of this study was to examine and analyse the impact of the Personal Data Protection Law on the situation in the field of migration management in Georgia, providing a static (the situation in 2014) and a dynamic (the situation in 2014 and before) analysis, in order to examine how far the legal acts and procedures in the field of migration management are in line with the Personal Data Protection Law and the Council of Europe 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, and to identify possible gaps and need for further improvement.

The study was requested to cover all aspects of migration management, including the legal acts and practical procedures, and the following processes and institutions:

Organisation	Process
Public Service Development Agency (Legal Entity of Public Law under the Ministry of Justice)	
	1. Issuance of residence permits 2. Granting stateless person status 3. Issuance of ID cards 4. Issuance of passports 5. Procedures related to the citizenship of Georgia 6. Deferring an alien's stay in Georgia
Patrol Police and Migration Department, Ministry of Internal Affairs	
	7. Removal of aliens from Georgia 8. Issuance of visas at border crossings 9. Border Control (Database of the Border Crossing) 10. Readmission management 11. Exposure of illegal migration, arrest and placement of illegal migrants[3]

[3] Only processes 9 and 10 were assessed, as information concerning the remaining processes at the MIA was not made available.

Consular Department of the Ministry of Foreign Affairs	
	12. Issuance of visas 13. Issuance of return documents to citizens of Georgia 14. Consular registration
Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia	
	15. Issuance of the Status of Refugee and granting asylum 16. Determination of the Repatriate Status 17. Management of the Reintegration Process

The study covered the period from the adoption of the Personal Data Protection Law up until the end of December 2014. However, some responses to the questionnaires sent to institutions were returned to the IRC in the first quarter of 2015, and some facts may be inclusive of developments up until the end of the first quarter of 2015.

The following assumptions were applied during the undertaking of the study:

- Only officially obtained information and responses were considered relevant to assessing the baseline situation with regard to personal data protection; unofficially obtained information was an impetus to request further clarification/information, but was not used as a basis for forming an opinion.
- Institutions participating in the study view it as an opportunity to see the holistic picture of data protection in their respective institutions and that the information provided contains a high degree of precision.
- Confidential documents would not be disclosed by the respective institutions, but their existence/content would, however, be accepted by the study based on the responses made by the respective institutions, without additional verification.
- The assessment and recommendations made in this report are intended to support the improvement of the state of data protection in migration management. However, they should not be taken as legal advice.

2.2 Methodology

Qualitative research methods were applied while carrying out the study. The key task of the study was to identify and understand the existence of certain data protection related documents/procedures, their content and their application in practice; this required descriptive tools as well as more in-depth content understanding. In the framework of the qualitative study, an array of instruments were used, including desk research,

questionnaires, interviews, expert consultation, group discussions, and direct observation.

3. Main observations of the study

The discussions and findings of the study are provided herein. The structure of the findings is as follows:

Part I	Assessment of the Personal Data Protection Law with regard to international documents related to personal data protection
Part II	Assessment of the migration management sectoral legislation with regard to the requirements of the Personal Data Protection Law and CoE Convention No. 108
Part III	Personal data protection practices in migration management related processes

Part 1 Assessment of the Personal Data Protection Law with regard to international documents related to personal data protection

The purpose of this part is to compare the Law of Georgia on Personal Data Protection (hereafter the PDP Law) to standards of data protection prescribed by supranational or international legal instruments. This chapter provides an overview as to what extent the PDP Law satisfies internationally established data protection standards in areas relevant to migration management.

The following legal instruments have been regarded as benchmarks in this chapter:

- international agreements, which Georgia is a party to;
- EU documents regulating personal data protection; and
- privacy protection related international recommendations.

The key benchmark for this analysis is the Council of Europe Convention 108 (hereafter referred to as the Convention[4]), with Georgia being a contracting party.[5] The Convention sets out the minimum standards with regard to personal data protection; however, the states party to it can adopt higher standards.

1.1 The Scope of the Law of Georgia on Personal Data Protection

Georgia adopted the first PDP Law in 2011,[6] which regulates processing of personal data through automatic and semi-automatic means, as well as data processing through non-automatic means, if it is part of a filing system.[7] In its Article 3, the PDP Law initially excluded several areas from its applicability, among them areas closely related to police work. The Convention allows in its Article 3 para. 2 item (a) for exemptions from the applicability of domestic legislation on data protection.

Through the amendments made in 2014,[8] the scope of the PDP Law was extended. With regard to migration management, of particular importance is the extension of the Law – with certain exemptions – to the processing of data for the purpose of fighting crime. As a result, the PDP Law now also covers "automatic processing of data, assigned the status of state secret, in order to prevent crime and carry out investigation,

[4] CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108 (1981).
[5] The Parliament of Georgia ratified Convention 108 on 28 October 2005.
[6] Law of Georgia on Personal Data Protection, available at: https://matsne.gov.ge/ka/document/view/1561437.
[7] A "filing system" is a "structured set of data where information is arranged and thus accessible according to specific criteria" (Art. 2 (n) of the Georgian PDP Law).
[8] Law of Georgia No. 2636 and No. 2639 of 1 August 2014 available at: https://matsne.gov.ge/ka/document/view/2457307 and https://matsne.gov.ge/ka/document/view/2455851 respectively.

operational and investigative work and purposes of protecting public order."[9] The general application of the PDP Law on data processing for the purpose of operational and investigative work of police authorities is a positive development and the Georgian legal situation now meets the recommendations made by CoE R (87) 15.

1.2 The principles of data processing

The essence of European personal data protection law is condensed into the data protection principles of Article 5 of the Convention:

"Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;
b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
d. accurate and, where necessary, kept up to date;
e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

The same principles are laid down in Article 6 of the EU Data Protection Directive and also in part II of the OECD Guidelines on Privacy Protection, although with a partly different formulation.

Article 4 of the PDP Law contains data protection principles aligned with the principles set out in Art. 5 of the Convention (and Art. 6 of the EU Directive). The first principle, that personal data "must be processed fairly and lawfully", is provided in paragraph (a) of Art. 5 of the Convention and Art. 4 (a) of the PDP Law. Paragraph b of Art. 5 of the Convention and paragraph (b) of Art. 4 of the PDP Law introduces the so-called "purpose limitation principle" which is another cornerstone of European data protection law.[10]

Additional principles under the Convention and the other listed documents on data protection include: (1) the limitation of the categories of processed data to what is absolutely necessary and (2) the obligation to keep data accurate and, where necessary, up to date. These principles are repeated in Article 4 (c) and (d) of the Georgian PDP Law.

[9] Only Art. 6 shall not be applicable "where the issue is directly and specifically regulated under the Criminal Procedure Code of Georgia or under the Law of Georgia on Operational - Investigative Work or other special laws" (Art. 3 para. 6 of the PDP Law).
[10] Art. 5 (e) of Convention 108 and Art. 4 (e) of the Georgian PDP Law.

1.3 The legal basis of data processing

The principle that all processing of personal data must be lawful demands that every case of processing must be founded on a reason foreseen by law. For data controllers in the public sector, this reason is usually an obligation or, at least, permission by law is required. Whereas the Convention leaves it to domestic law to define when processing of personal data shall be lawful, the EU Directive undertook for the first time in European law to define the cases of lawful processing.[11] It therefore makes sense to draw comparison to the rules of the Directive. The PDP Law has taken account of these articles of the EU Directive; with some notable differences, however.

The PDP Law discerns between "ordinary" and "special category" ("sensitive") personal data; the circle of sensitive data is, however, wider than in the EU Directive. Articles 7 and 8 of the Directive can, nevertheless, be compared to Articles 5 and 6 of the PDP Law respectively.

Among the public institutions participating in the Baseline Study, no significant problems were spotted concerning the existence of a legal basis for processing non-sensitive data. Such processing can be founded on either Art. 5 (c) (legal obligation of the controller), Art. 5 (e) (protection of substantial public interest), or Art. 5 (h) (necessity to provide a service to the data subject).

The challenges encountered centred on finding a legal basis for processing "special category data": cases were identified where processing was evidently necessary, however, no provision was found in Article 6 of the PDP Law. There is a lack of a provision similar to paragraph 4 of Article 8, which states that additional cases of processing sensitive data may be foreseen by law for the sake of substantial public interests and under condition that the necessary safeguards for the protection of the data subjects are provided. Although one could maintain that the PDP Law can be altered and enhanced by any later adopted legal provision, this does not fully satisfy the underlying problem: a separate article dealing with the legal basis for processing sensitive data actually *limits* the lawful processing of sensitive data and thus *prevents indiscriminate creation of additional cases of processing sensitive data by legislation*; this function cannot be performed by Art. 6 of the PDP Law.

As migration management is related to maintaining public order, part of the activities in this area may be "police activities". Therefore, the CoE Recommendation (87) 15, which demonstrates how the general principles of Convention 108 shall be implemented in police work, is relevant.[12] It introduces the notion that any data collection which does not

[11] Articles 7 and 8 of the EU Directive must be considered to be examples of good practice.
[12] CoE Recommendation No. R (87) 15 available at: https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2196553&SecMode=1&DocId=694350&Usage=2.

serve the prevention of real danger or the suppression of a specific criminal offence should be the exemption from the rule and would need special justification ("special legislation"). As a consequence, Article 5 (c) and (e) of the PDP Law must be understood as limited in this very specific sense.

Communication of data to other bodies[13] should, according to the Recommendation, be allowed only on grounds of clear authorisation or if it is indispensable for the legal task of the recipient, whilst being limited by the principle of compatibility with the original purpose of collection. These limits may be put aside if the communication of data is undoubtedly in the interest of the data subject.[14] Such questions are not dealt with in the PDP Law, but rather in the sectoral legislation and by-laws. Article 18 of the PDP Law deserves special mention in this context as it obliges the data controller (and – if relevant – the data processor) to document every case of data transfer or access to the files of a controller with the purpose of being immediately able to give information about data disclosures to the data subject (and the Inspector) upon request.

1.4 The implementation of the principle of fair processing

The principle of fair processing is closely related to what is called by the OECD Guidelines the "openness principle" and also the "individual participation principle"; this means that transparency about processing personal data shall be achieved vis-à-vis the data subject but also, to a certain extent, vis-à-vis the general public. Even though there may be some differences between the OECD Guidelines and especially the Directive concerning information obligations of the data controller, the Guidelines' "principle of openness" is contained in the principle of fair processing according to the Convention and the Directive.

To what extent the Georgian legislation complies with the Convention, and also with the good practice for transparency as foreseen under present EU law, is discussed below.

The Explanatory Report to the Convention explains[15] that the safeguards to be established by domestic law according to Article 8 of the Convention include four main elements:

- knowledge about the existence of an automated data file;
- knowledge about the contents of information, if any, stored about data subjects in a file;
- rectification of erroneous or inappropriate information; and
- a remedy if any of the previous elements are not respected.

[13] CoE Recommendation No. R (87) 15, principle 5.2.
[14] See principle 5.2.ii.
[15] See point 50 of the Explanatory Report.

The PDP Law provides for the duty of the controller to present "filing system catalogues"[16] to the Inspector who publishes them in an electronically accessible register, thus fulfilling the requirements for publicity under Art. 8 (a) of the Convention and of the OECD Guidelines' "ready availability".

The controller must inform the data subject at the time of collecting data about the main features of his planned processing operations (Art. 15, PDP Law). The PDP Law, on this point, evidently follows the example of the Directive; however, a difference exists in who shall fulfil this duty. Under the PDP Law, both the data controller and the data processor have this duty, which seems an unnecessary duplication and not advantageous for the clarity of roles and obligations.

One more significant difference to the Directive is that when the data are collected from the third parties, according to the PDP Law information has to be given only "upon request". It is true that the Explanatory Report to the Convention mentions it as an example,[17] but this is not in the best interest of the data subject, as the collection of data from the third parties constitutes a higher risk and therefore would need higher transparency than collecting data directly from the data subject. Exemption from the duty is provided for in the case that "the data subject already has the information"[18] – this complies with Art. 10 of the Directive.

"Individual participation" is secured by the provisions of Chapter IV of the PDP Law through the access rights named in the Convention (Art. 8 (b) and (c)) and in the Directive (Art. 12). Principle 6 of Recommendation (97) 15 is met as the data subject's access rights exist also in the context of processing data for police purposes. Chapter IV of the PDP Law also contains provisions on the possible limitations of the rights of the data subjects. These provisions seem to be in line with Art. 9 of the Convention and Art. 13 of the Directive.

Finally, it has to be stated that also Article 8 (d) of the Convention concerning an effective remedy against refusal to rectify or delete is taken care of by Art. 26 of the PDP Law.

Special regulation is foreseen in the PDP Law on personal data obtained through covert investigative actions: a special commission, established by the Parliament, is entrusted with the task of evaluating whether and when such information shall be deleted (Art. 26[19]). What is not foreseen in this context is the duty to inform the data subject after the termination of covert investigations; paragraph 3 of Art. 9 of the Explanatory Report to

[16] Art. 19 and Art. 20 of the PDP Law.
[17] See point 51 of the Explanatory Report.
[18] Art. 15 (2) the PDP Law.
[19] This (second) Art. 26 was created by the Law of Georgia No. 2636 of 1 August 2014 available at: https://matsne.gov.ge/ka/document/view/2457307.

Recommendation (87) 15 mentions it as an example of good practice.[20] However, the PDP Law tries to establish special data protection safeguards through an oversight by the data protection supervisory authority (Art. 35 of the PDP Law): court permission shall be accompanied by permission from the Inspector.[21] Whether such direct involvement of the supervisory authority in the process of granting permission to operate covert investigative work is the best solution is sometimes queried.[22]

1.5 Data security

Data security is dealt with by the OECD Guidelines under the "security safeguards principle". The obligation of the data controller to guarantee data security by adequate technical and organisational means is set down in the Convention (Art. 7) as well as in the Directive (Art. 17).

The PDP Law deals with the duty to adduce data security in Art. 17, naming the data controller as the person to whom this duty belongs. Art. 17 specifically obliges the controller to document "all operations performed in relation to the data in his file" (para. 2) and to analyse risks concerning operations (para. 3). Paragraph 4 of Art. 17 obliges the employees of data controllers and of data processors to use data exclusively according to order and to keep data confidential, even after they have left their position.

The relationship between data controller and data processor(s) is regulated in Art. 16 of the PDP Law: it explicitly maintains that the data processor must limit his processing operations to what has been determined by the data controller. This article also refers to data security at the processor, but does not clearly foresee a genuine original legal obligation of data processors to guarantee data security. However, as Art. 16 of the PDP Law mentions the possibility that a processor does not act on grounds of a contract but is appointed by law, it must be concluded that the duty to provide appropriate data security is inherent in the legal concept of a "data processor". The last paragraph of Art. 17 promises further legislation on data security, which seems an adequate reaction to the importance of information security in an online world.

1.6 Compliance

The accountability of the data controller for being compliant with the existing data protection legal framework calls for special instruments to improve and secure compliance. One of these instruments, as first mentioned in the Directive, is an "internal

[20] CoE Recommendation No. R (87) 15, principle 2.2, Explanatory Report para. 44.
[21] The Authority of the Inspector includes: "a) checking lawfulness of data processing through electronic means of control; b) when carrying out covert surveillance, to issue permission on covert investigative work through the means of two-stage electronic system; c) checking (inspecting) lawfulness of data processing by data processor/authorised person."
[22] Article 1.3., paragraph 25, Explanatory Memorandum to Recommendation No. R (87) 15, https://wcd.coe.int/ViewDoc.jsp?Ref=ExpRec(87)15&Language=lanEnglish&Ver=original&Site=COE&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383.

data protection officer".[23] Experience shows that such an officer must have "influence" over what is going on in the institution. However, the final responsibility to the outside world rests with top management.

The PDP Law does not foresee the mandatory appointment of an internal data protection officer and does not elaborate on the position and special tasks of such a function.

For promoting compliance, special attention must be given to the issue of adequate procedures elaborated and documented. The explorations done in the course of the Baseline Study showed several attempts to create special regulations, usually in the form of by-laws; however, having a general legal instrument on what should be done on the level of internal guidelines might facilitate achieving internal structures favourable to data protection. The special legislation promised in Art. 17 (5) of the PDP Law might be an opportunity to extend more technical data security to a more comprehensive organisational data protection security.

1.7 Control of data processing by an independent authority

One of the important special features of effective personal data protection according to European standards is the supervision of data controllers (and processors) by an independent authority.

The Georgian PDP Law complies with this requirement; in Chapter V, the Law establishes the office of a Personal Data Protection Inspector with competences and powers to monitor the lawfulness of personal data processing. Since the amendments of 2014, the PDP Law is fully applicable to police work; even the processing of "state secret data" for the purpose of fighting crime underlies the PDP Law and thus supervision by the PDP Inspector. One of the important special requirements under the CoE Recommendation (87) 15[24] is thus fulfilled.

1.8 Recommendations for changes to the PDP Law concerning topics found to be of direct relevance in the context of migration management

1. Art. 3 of the PDP Law on the scope of applicability shows a degree of complexity, caused by several amendments, which makes understanding most difficult for the average citizen; thus, it is recommended to reformulate it in the interest of transparency of legislation.

[23] A "personal data protection official" according to Art. 18 (2) of the EU Data Protection Directive.
[24] Principle 1.1.

2. As the PDP Law does not have a higher status than any other Georgian law, the limitations foreseen in Article 6 are not effective. They are also insufficient when processing sensitive data is not allowed under Art. 6, although evidently and reasonably necessary. It is recommended to give further thought to the question of if and how the evident purpose of Art. 6, in order to limit indiscriminate creation of additional cases of processing sensitive data by law, could be realised under the Georgian legal system.

3. It is highly recommended to discuss whether and how the Law could be more explicit on the total of the conditions for lawful disclosure of data to third parties.

4. As concerns the obligation to inform the data subject at the time of collecting data, it should be deliberated to amend the Law in order to reach the standard of the Directive also in cases where data are collected from third parties. Moreover, it should be clarified that the duty to inform the data subjects rests with the controller and does not involve the processor.

5. It should be explicitly stated in the PDP Law that the obligation to safeguard adequate data security is a legal obligation for everyone who processes personal data, regardless of whether he is a controller or a processor and regardless of what is foreseen in the contract between them.

6. The mandatory appointment of an internal data protection officer should be foreseen in the PDP Law for institutions with a significant volume of data processing.

7. More detailed legal provisions on organisational measures for safeguarding compliance with the data protection legal framework should be created; an obligation for the public sector to have the necessary by-laws containing such measures in place could be foreseen.

Part 2 Assessment of the migration management sectoral legislation with regard to the requirements of the Personal Data Protection Law and the Convention

The legal history of Georgia as an independent state starts in the 1990s. Even though the majority of the laws which are applicable today were adopted a bit later, many of them represent revised versions of the initial laws adopted in the 1990s. Regardless of the fact that provisions on privacy rights existed in the Constitution of Georgia of 1995, a separate, special law on data protection was only introduced in 2011; to which the sectoral legislation did not pay attention to.

Revised versions of the majority of the existing legal acts on migration issues were adopted in the period 2012-14. Regardless of the fact that the new edition of the sectoral legislation was adopted mainly after the adoption of the PDP Law, it remains generally "indifferent" towards personal data protection.

This chapter analyses migration management related sectoral legislation to determine:

- whether it complies or is in direct contradiction with the principles and provisions prescribed by the Convention and the PDP Law; and
- whether it provides rules, which do not directly refer or relate to provisions of the said legal instruments but, nevertheless (a) support the realisation of the provisions prescribed by the Convention and the PDP Law by filling in the gaps and regulating the issues not precisely regulated by the PDP Law, or (b) worsen the data protection standards.

Changes which have occurred within the sectoral legislation have not been initiated to introduce personal data protection standards and ensure their compliance. Therefore, this report will review the present formulation of the laws and by-laws (the original versions before the changes will only be referred to if this is important for purposes of comparison or clarifying developments).

2.1 The Law of Georgia on The Procedures for Registering Citizens of Georgia and Aliens Residing in Georgia, for Issuing Identity (Residence) Cards and Passports of a Citizen of Georgia[25] (ID Law)

The Issuance of ID documents is the basic source of forming the population registry. Historically, in Georgia, the population registry was formed on the basis of information gathered on issued identification documents and the population registry began to function *de facto.* Consequently, relevant articles were added to the existing law on ID

[25] Adopted on 27 June 1996.

documents; for example: according to paragraph 4, Article 20 of the ID Law, the Public Service Development Agency (PSDA) is authorised to issue personal data contained in the identity documents to third parties under certain circumstances. Accordingly, the ID Law regulates not only the issuing of ID documents, but also serves as the act on the population registry to some extent. When analysing and assessing this Law in the light of Convention 108 and of the PDP Law, these particularities should be taken into account.

When assessing the ID Law in the light of data protection standards, the following key issues emerge:

a) There is the need to provide more specifics concerning special category data to guide employees in fulfilling their work in compliance to the data protection standards; for instance, when issuing ID (residence) cards under Art. 14, paragraph 10 of the ID Law. This article provides for the possibility of issuing ID (residence) cards without an electronic data carrier, although healthcare information may be processed. The processing of special category data, such as healthcare data, is permissible under Art. 6 of the PDP Law, on the grounds "to protect the vital interests of the data subject". On some occasions, however, one can challenge whether specific actions represent such vital interests.

b) Matters related to the consent during the disclosure of information contained in the PSDA database are of concern. According to the paragraph 4, Article 20 of the ID Law, the consent shall be considered issued if from consent or other circumstances of the activity undertaken by the institution requesting the information about the data subject it can be concluded that the data subject agrees to the disclosure of his/her personal data. However, in certain cases the subject might not be able to predict whether his/her data will be checked against the database of the PSDA; *thus this provision contradicts the legal definition of 'consent' as provided by the PDP Law*. The clarification to this norm stated that this article serves mainly for answering requests from banks and similar institutions to verify identity and residence data of clients or prospective clients. In this special relationship, the legal basis can be Article 5 h) of the PDP Law: "Data processing is necessary to deal with the application of a data subject." Even if this provision should in a given case indeed be applicable, it seems evident that – in the context of the extent of the database such as the unified population registry – the ID Law needs more detailed provisions about the categories of data which may be disclosed to such third parties.

c) The ID Law does not specify the provisions contained in the Convention and in the PDP Law and it therefore does not support their implementation. For example, Article 7 of the Convention and Article 17 of the PDP Law regulate data security. They contain a general obligation for the data controller to take the necessary organisational-technical measures to safeguard data security and the PDP Law states that these measures shall be defined, evidently in more detail, by the Georgian (sectoral) legislation. However, the reviewed normative acts do not provide any information about the measures to be undertaken in respect to data security in the given context. Therefore, it remains unclear how the general accountability of the register authority for guaranteeing data security will be fulfilled.

Conclusion: Several provisions of the ID Law and the relevant by-laws are rather vague on essential data protection issues. The range of the personal data to be processed in the population registry and to be disclosed to third parties is not predictable. The legal basis for processing special category data (health data) in exceptional cases is questionable.

2.2 The Law of Georgia on the Legal Status of Aliens and Stateless Persons

The Law of Georgia on the Legal Status of Aliens and Stateless Persons (hereinafter the Law on Aliens) was adopted on 5 March 2014. According to the Article 1 of the Law on Aliens, one of its goals is to establish the legal guarantees for aliens and stateless persons in Georgia according to the universally recognised principles of human rights and freedoms that involve the right of privacy and personal data protection. In addition, compliant to paragraph 1 of the Article 67 of the Law, “Personal data of aliens shall be processed under the legislation of Georgia.”

Chapter III of the Law refers to issuing visas and provides detailed regulation on the general conditions for issuing visas, as well as specific procedures. Paragraph 3, Article 8 of the Law on Aliens proclaims that if needed, a visa issuing authority may require additional documents or invite a visa applicant for an interview to verify their application. *This is a clearly positive approach*, since on the one hand it does not prescribe a strict approach on obtaining additional information during the visa issuance process, while on the other hand naming the legitimate goals for the fulfilment restricts the data processor to which the right to collect additional information is granted.

Regarding residence permits, the matter is somewhat different, as the PSDA, which is authorised for instance to issue residence permits, is entitled to request additional documents and is prescribed to use an application form. However, *no restriction is*

provided against the application form requesting the processing of more information than needed for obtaining the residence permit. To align it with the requirements of the PDP Law, it would be highly recommendable to formulate paragraph 1, Article 13 of the residence decree as follows: "the agency shall be authorised to request additional documentation at any stage of the case consideration, if the documents are necessary to prove facts and circumstances which are essential for the decision of the case."

The processing of sensitive data (special category data) is another important issue. According to subparagraph 'f' of paragraph 1 of the Article 18 of the Law on Aliens, an alien may be denied a residence permit in Georgia if "he/she has such infectious or other diseases, the nature, severity, or duration of which may pose a threat to the population of Georgia." What is missing is a body competent to announce that there is a situation in a third country which calls for the presentation of special certificates of health status; this should also comprise a timeframe for such special measures.

Conclusion: In some cases, the provision of the Law or the by-laws is vague and the volume of the data to be processed is unpredictable.

2.3 The Organic Law of Georgia on Georgian Citizenship

The Organic Law of Georgia on the Citizenship of Georgia (hereinafter the Organic Law) was adopted on 30 April 2014. The Law defines the basic principles of Georgian citizenship, establishes the legal status of Georgian citizens and the grounds for acquiring and terminating Georgian citizenship.

The parties involved in citizenship issues are the PSDA, the administration of the President of Georgia, the Ministry of Internal Affairs (MIA) and the Intelligence Service of Georgia. It should be noted that the Organic Law only mentions the PSDA and the Administration of the President. Presidential Decree No. 237 on 'Approving the provisions for considering and deciding the issue of Georgian citizenship' issued on 10 June 2014 (hereinafter the Presidential Decree) includes the MIA and the Intelligence Service. The Presidential Decree defines the bodies responsible for data processing and the parties involved in the procedure. Which data should be processed and what can be accessed by officials inside the organisation, or what part of the data can be transferred to various agencies, is at the discretion of the organisation itself. Frequently, these issues are completely regulated by the individual act, or the practice. The Law does not define the scope of regulation on this issue.

The Presidential Decree determines the list of documents to be submitted for reviewing issues of Georgian citizenship. Application forms differ between procedures and are

rather flexible. Mandatory fields only involve general data and the additional information can be submitted in the form of attached documents. For example, if information on the business activities of the person is important for resolving the specific case, the documents will be annexed to the application form. This approach is the result of the legal amendment entered in 2014, which should be assessed as a positive development since it *supports the processing of the data proportionate to its purpose*.

Conclusion: The regime prescribed by the Organic Law does not differ from the PDP Law, although the sectoral law also does not specify the issues of personal data protection. It should be noted that sometimes the parties involved in the process, their role and, in some cases, also the categories of the processed data are not clear or predictable.

2.4 The Law of Georgia on Refugee and Humanitarian Status

The Law of Georgia on Refugee and Humanitarian Status (hereinafter the Refugee Law), which was adopted on 6 December 2011, does not particularly point out issues of personal data protection, it also does not determine the regime differently from the one prescribed by the Constitution and the PDP Law. According to subparagraph 'e', paragraph 2, Article 18 of the Refugee Law, the asylum-seeker is obliged to undergo a compulsory medical examination in a healthcare institution. Implementation of the procedure leads to the conclusion that the processing of special category data concerning health status is undertaken for public healthcare protection based on subparagraph 'c', paragraph 2, of Article 6 of the PDP Law. *However, with regard to this sensitive data, it would be recommendable to provide more specific provisions and clearly define the cases, the amount of data and the procedure for processing the special category data.*

Decisions on granting refugee status and asylum are made by the Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia (MRA). The Refugee Decree defines the relevant structural units of the Ministry and their competences. The MIA, the Ministry of Justice of Georgia, the Ministry of Corrections of Georgia, the Ministry of Foreign Affairs (MFA), the Ministry of Labour, Health and Social Issues, the Ministry of Education and Science, and local self-government bodies are also involved in the process. The Law prescribes the scope of the competences of each body in detail, which is by all accounts a *positive factor*.

Conclusion: The Refugee Law does not foresee any rules different from the PDP Law; nor does it specify the principles and provisions of data protection. It does not contain clear and strict provisions regarding the processing of sensitive data.

2.5 The Law of Georgia on Consular Activities

The Law of Georgia on Consular Activities (hereinafter the Law on Consular Activities) was adopted on 12 June 2012. The Law is general and limited to setting out the principles and list of basic or delegated consular functions.

Article 20 of the Law on Consular Activities refers to issuing certificates for persons returning to Georgia. Decree No. 426 by the Georgian Government on 'Approving the provision concerning the Certificate for Return to Georgia' issued on 30 June 2014 (hereinafter the Decree on Return Certificates) prescribes the grounds, conditions and timeframes for issuing a return certificate, and contains the list of documents to be submitted. According to paragraph 4, Article 9 of the Decree on Return Certificates, special category data can be processed if the return certificate is issued to a person who is unable to express his/her will because of severe illness and absence of a representative. In this case, an additional certificate proving the inability of the person to express his/her willshall be provided. The vital interest of the data subject is the legal basis for lawfully processing this data.

Art. 21 of the Law on Consular Activities deals with the consular registration rules; however, it delegates the right to regulate the procedure for consular registration to an order of the Minister. Order No. 241 on 'Approving the Procedure for Consular Registration and De-registration' issued by the MFA on 10 October 2011 (hereinafter the Consular Registration Order) defines the procedure for consular registration and de-registration and the list of the documents to be submitted, defining the volume of the information to be processed.

Conclusion: The Law on Consular Registration and the Decree on Return Certificates seem not to be in contradiction to the regulations promulgated in the PDP Law.

2.6 The Law of Georgia on 'Repatriation of Persons Forcefully Sent into Exile from Georgian SSR by the Former USSR in the 1940s'

The Law of Georgia on 'Repatriation of Persons Forcefully Sent into Exile from Georgian SSR by the Former USSR in the 1940s' (hereinafter the Repatriation Law) was adopted on 11 July 2007. It provides legal tools for the return of persons forcefully expelled from the Georgian SSR in the 1940s and their descendants in Georgia. The

Repatriation Law specifies the procedure for submitting the application to obtain repatriation and the list of required documents.

Article 6 of this Law determines the procedure for considering the application and authorises the MRA to transfer documents to other agencies for further review if needed. However, no further explanation of "*if needed*" is provided, nor a list of the agencies that might be involved.

Order No. 276 on 'Determining the additional requirements for consideration of the assignment of the repatriated status' (hereinafter referred to as the Repatriation Order) issued by the Government of Georgia on 17 December 2007 approves the application form for the repatriation status seeker. The application form requests information on education, work experience, etc. Since Article 4 of the Repatriation Law does not prescribe the processing of this type of data, it is unclear as to what is the purpose of collecting information on education or work experience.

The Repatriation Order also envisages processing of information concerning religious and ethnic belonging. Article 6 of the PDP Law defines the grounds for processing the special category data; however, *none of them are in compliance with the processing of the sensitive data as prescribed by the Repatriation Order*.

Conclusion: The amount of data to be processed under the Repatriation Law is not predictable in certain cases. The data processing is not always proportionate to the purpose. Grounds prescribed by the PDP Law for processing the special category data on religious and ethnic belonging are not available.

2.7 The Law of Georgia on the State Border

The Law of Georgia on State Border of Georgia (hereinafter the Law on State Border) was adopted on 17 July 1998 and regulates the status of the State border, and provides general rules for border crossing and regulations on establishing and maintaining the State Border regime. According to the Article 33 of the Law on State Border, the MIA shall be authorised to control the State Border of Georgia. However, various institutions from the executive branch are also involved in the process. On the one hand, the Law does not define who – inside the organisation itself – shall have access to the data processed during the border control process. Whilst on the other hand, the scope of competences of the bodies involved in the process is also not defined. Besides, according to subparagraph 'b', Article 4 of the Joint Decree No. N985-N1187 issued by the Minister of Finance of Georgia and the Minister of Internal Affairs of Georgia on 'Approving the procedure of making relevant records in the travel documents on

crossing the State Border of Georgia and reflecting the information in the automated database operated by the Ministry of Internal Affairs of Georgia', as of 31 December 2010, the authorised officers at the border checkpoints have been "obtaining information about a person". However, there is no indication as to the type of information allowed to be obtained, the source of obtaining the information, etc.

Conclusion: This Law does not prescribe regulations different or contradictory to those of the PDP Law; nor does it specify the data protection issues. A lack of specifics renders processing of personal data unpredictable.

2.8 Agreement between the European Union and Georgia on the readmission of persons residing without authorisation

The Agreement between the European Union and Georgia on the Readmission of Persons Residing without Authorisation (hereinafter the Readmission Agreement) entered into force in 2011. Article 16 of the Readmission Agreement covers the personal data protection issues. The article defines the principles of data processing. However, Joint Order No.185-No.35-No.63-No.22 on 'Approving the procedure for implementing the Readmission Agreement' issued by the Minister of Internal Affairs of Georgia, the Minister of Justice of Georgia, the Minister of Foreign Affairs of Georgia, and the Minister of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia on 12 March 2012 (hereinafter the Readmission Order) regulates the organisational and procedural issues of the readmission process, without any indication concerning data protection. According to subparagraph 'b', paragraph 1, Article 5 of the Readmission Order, for the readmission application a photo and the fingerprints of the person are examined – which means that special category data are processed.

Conclusion: The Readmission Agreement clearly outlines the issues of personal data protection, while the by-laws foresee the processing of sensitive data on grounds which have no equivalent in Article 6.

Part 3 Personal data protection practices in migration management related processes

Personal data protection was studied in migration management related processes in four government institutions:

- the LEPL Public Service Development Agency (PSDA);
- the Ministry of Foreign Affairs (MFA);

- the Ministry of Internal Affairs (MIA); and
- the Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia (MRA).

The discussions which follow provide general observations and recommendations.

3.1 The LEPL Public Service Development Agency (PSDA)

3.1.1 Overview

The PSDA is one of the most important organisations in the migration management process, particularly in the context of personal data protection, as it uses a variety of categories of data in large volumes, among other sensitive and biometric data. The circle of data subjects is rather wide and covers every citizen of Georgia, as well as stateless persons and aliens residing in Georgia.

As a result of the study, one can say that generally, concerning its organisational development, the PSDA is rather ready/has a certain degree of maturity in personal data protection related matters in the Georgian context; this is also true for the level of human resource development. The PSDA has an internal data protection officer responsible for compliance. The physical and IT infrastructure is good, which justifies hopes that there are good preconditions present in the will of the PSDA top management that the gaps related to personal data protection which were identified in the course of the study can be closed.

3.1.2 Observations

Legal grounds for processing data

For all processes studied at the PSDA, legal grounds for processing non-sensitive personal data *do exist* and are mainly founded on Article 5, Point c of the PDP Law, “data processing is necessary for a data controller to perform obligations prescribed by national legislation”. However, there seems to be a need to critically assess whether processing all currently processed data is absolutely necessary.

Concerns do exist with regard to the special category data. From the point of view of data protection, which is governed by a general ‘need-to-know principle’, any data disclosure which reveals more than is absolutely necessary for performing a legal task is unlawful. Concerns mainly cover:

- The PSDA receives access to more information through electronic services (e-services) than needed for the decision-making; for instance, the entire information on border crossings and criminal convictions of applicants stored in the MIA database can be viewed by the caseworker, even though only a

limited amount of such information is needed. *This can be considered a deficiency of the e-services*.

- The processing of some special category data is evidently absolutely necessary for the PSDA to perform its duties, however, this is not always founded in Article 6 of the PDP Law; processing of data on the criminal history of an applicant, for instance, is indeed carried out, but is not covered by any of the cases mentioned in Article 6.
- The PSDA caseworker receives access to information on a person, who might not be an applicant but whom may have similar data to an applicant, in order to exclude potential errors in entering an applicant's data into the system. This need may be justified to exclude such errors, however, it raises questions from the data protection standpoint and requires critical assessment with respect to the principle of proportionality.

Obligation to inform the data subjects

Article 15 of the PDP Law orders the data controller (as well as data processors) to provide the data subject with certain information.

The PSDA notes that this obligation is fulfilled upon providing an applicant information on the confirmation of submission of documents[26] and provides this information on the website. However, the text on confirmation of submission does not comply with the requirements of the Article 15 and information is not provided on the website. Therefore, it is highly recommended to revise the relevant text and communicate it to the applicants.

Obligation to register any disclosure of data

Article 18 of the PDP Law provides for an obligation of the data controller and the data processors eventually involved to register all acts of disclosure of personal data. This provision is of high practical importance in terms of the realisation of the rights of a data subject and represents a significant instrument for monitoring the legality of the processing (disclosure) of data.

The PSDA stores information concerning disclosure and it is possible with some effort to search for the source of the information (by accessing archives, government programmes/software, electronic databases, etc.). However, the effort required to do this may be substantial as there is no simple, data protection-oriented mechanism of registering disclosure, thus making it difficult to reach the objective of this provision.

[26] The so-called "სამახსოვრო ბარათი".

Obligation to have filing systems catalogues and to notify the PDP Inspector of them

Pursuant to the Article 19 of the PDP Law, a data controller is obliged to keep a catalogue of his filing systems and to register the information on data processing in each filing system; the same time changes need to be updated. The PSDA has provided such catalogues to the PDP Inspector upon request, however, no updates have been made to it since the initial submission. This fact may raise some questions, as since the submission of catalogues, new Laws (e.g. the Law of Georgia on the Legal Status of Aliens and Stateless Persons) have entered into force, which might have entailed changes to the filing system catalogue.

Obligation to provide data security

Article 17 of the PDP Law obliges the data controllers as well as processors to "apply organisational and technical measures to ensure the protection of data against accidental or unlawful destruction, alteration, disclosure, access or any other form of unlawful use and accidental or unlawful loss." The same Article 17 provides that "the measures applied for data security shall be adequate to the risks related to the processing of data".

The PSDA has not yet carried out identification of threats and risk assessment in migration management, it is therefore rather questionable whether measures to mitigate potential risks are in place.

It is worth noting, that up until the period of the study, the PSDA had no registered incidents related to personal data protection, nor any cases of someone being liable for a personal data protection related administrative violation.

3.1.3 Recommendations

In order to improve the data processing practices and better align migration management related processes to the Georgian Personal Data Protection Law, it is recommended that the PSDA takes action in the following areas:

- Analysis of threats and specific risks in data processing[27] with regard to data protection.
- Creation of an effective system of informing data subjects at the time of data collection.

[27] The project team had a desire to carry out a PIA on at least one of the processes. However, this requires a high degree of cooperation from the PSDA, which was difficult to obtain at the given moment.

- Development of a more efficient mechanism for registering the disclosure of data to third parties, so that any such disclosure is easily traceable.
- Development of a database structure for e-services enabling the splitting of data records into smaller entities, so that only needed data are accessible by a specific type of user.
- Exploration of possible legislative changes to ensure that the processing of special category data stays within the framework of the PDP Law.
- Definition of who is entitled to receive which type of data from the population registry.
- Clarification of the access to identity data for institutions requiring identity confirmation by special legal regulation.
- Analysis of procedures related to information security, equipment management and other areas in the context of personal data protection.
- Making participation of the data protection officer mandatory in certain processes, for instance, when defining the scope of access to data by persons in specific positions.
- Developing an internal audit methodology in order to check how effective the policy documents and instructions are with regard to data protection.

3.2 The Ministry of Foreign Affairs (MFA)

3.2.1 Overview

The MFA is one of the key institutions participating in the migration management process through processes such as issuing visas, return documents and consular registration. In the course of these activities, the MFA processes non-sensitive, as well as special category and biometric data of Georgian citizens, and aliens.

The MFA has certain principles of the PDP Law enacted into practice, particularly with regard to the legal grounds for data processing, informing the data subjects; however, awareness and expertise in the Ministry concerning the data protection principles is rather low. The MFA does not have a person responsible for personal data protection at the organisational level, which even though not mandatory by the PDP Law, could be of help in the absence of organisational expertise in this area.

3.2.2 Observations

Legal Grounds for the processing of data

For all processes studied at the MFA, legal grounds for processing non-sensitive personal data *do exist* and are mainly founded on Article 5, Point b and c of the PDP Law, “data processing is enshrined in law” and “data processing is necessary for a data

controller to perform obligations prescribed by national legislation" respectively. However, there seems to be a need to critically assess whether processing all currently processed data is absolutely necessary.

Concerning special category data, the MFA processes biometric data in the form of a photo, to issue the return certificate, for instance. However, as this is an identity document in accordance with Article 9 (2), which allows the processing of biometric data "to issue an identity document under procedures established by Law, or to identify a person crossing the state border", consular authorities can be considered to have sufficient legal grounds to process these biometric data.

Concerns do exist, however, in relation to other special category data; for instance, the processing of some special category data is evidently absolutely necessary for the MFA to perform its duties but is not, however, always founded in the Article 6 of the PDP Law (for example, processing of data on the criminal history of an applicant is indeed necessary, but is not covered by any of the cases mentioned in Article 6).

The MFA sets a good practice on the *access to data* collected in the course of dealing with visa applications. Access to a visa application and attached documentation is only given to a consul and his/her assistant involved in the decision-making, and the application is opened by a consul only when an applicant comes to the interview. From the viewpoint of personal data protection, this fact deserves positive mention, as the described practice minimises the risk of unauthorised access and disclosure of the data subject's personal data.

Obligation of the data controller to inform the data subjects

According to the Article 15 of the PDP Law, data controllers are obliged to notify a data subject about processing data related to him/her.

The MFA has some good practices on informing the data subject of his/her data being processed. For instance, when filing the form for the return document, the data subject confirms that he/she is notified/informed about the following:

- Personal data indicated in the electronic application (inter alia, biometric data), and information presented by myself, as a representative, in case of necessity can be transferred and processed by relevant state bodies for the purposes of making decision on the given application.
- Data, which I present about myself or a person which I represent, will be further checked with relevant bodies.
- The processing of data presented by myself in the electronic application is covered by the Georgian legislation on personal data protection.

- For the purposes of considering an electronic application, assembling relevant information and presenting my photo (collection of fingerprints if necessary) is a mandatory procedure to make a decision on the application.

Even though this text is not included in the Order of the Minister No. 51 dated 28.02.2012, it is used in practice and serves the purpose, which is a positive development. What is missing, just as in other processes handled by the MFA, data subjects are not informed about their rights to access their data and to request correction, update, addition, blocking, erasure and destruction under certain circumstances.

Obligation to provide data security

Data controllers as well as processors are obliged to undertake organisational and technical measures which ensure that data are safeguarded against accidental or illegal destruction, alteration, revelation, access, and any other illegal use and accidental or illegal loss.

The MFA has not yet carried out identification of threats and risk assessment in migration management; therefore, it is rather questionable whether measures to mitigate potential risks are in place.

Obligation to register any disclosures of data

Article 18 of the PDP Law provides for an obligation of the data controller and the data processors eventually involved to register all acts of disclosure of personal data. This provision is of high practical importance in terms of the realisation of the rights of a data subject and represents a significant instrument for monitoring the legality of the processing (disclosure) of data.

The PSDA stores information concerning disclosure and it is possible with some effort to search for the source of the information (by accessing archives, government program/software, electronic data base, etc.). However, the effort required to do this may be substantial as there is no simple, data protection-oriented mechanism of registering disclosure, thus making it difficult to reach the objective of this provision.

Obligation to have filing system catalogues and to notify the Personal Data Protection Inspector of them

Pursuant to the Article 19 of the PDP Law, a data controller is obliged to keep a catalogue of his filing systems and to register the information on data processing in

each filing system; the same time changes need to be updated. The MFA has provided such catalogues to the PDP Inspector upon request.

3.2.3 Recommendations

In order to improve the data processing practices and better align migration management related processes to the Georgian Personal Data Protection Law, it is recommended that the MFA take action in the following areas:

- Analysing threats related to specific processes and developing risk-oriented specific actions.
- Creating the position of personal data protection officer within the MFA, whose task it is to promote fulfilling the requirements of the Law.
- Creating the position of information security officer who should contribute to ensuring that the requirements of the Law on Information Security are fulfilled, which would also enhance data security, being an essential part of data protection.
- Clarifying the roles of employees within the organisation, as well as their responsibilities with regard to personal data protection.
- Developing internal documents or guidelines which regulate the use, management and return of organisational assets which are used for processing data.
- Developing an access control policy and defining user access revision procedures.
- Defining procedures for identifying technical weaknesses and recording information security related incidents.
- Developing an effective mechanism for documenting the disclosure of data to third parties, so that any disclosure is easily traceable and access requests from data subjects can be speedily answered.

3.3 The Ministry of Internal Affairs (MIA)

3.3.1 Overview

The MIA is one of the most important institutions in the migration management process, particularly in the context of personal data protection. The MIA processes a variety of categories of data, in large volumes, among other sensitive and biometric data. The circle of data subjects is rather wide and covers citizens of Georgia, as well as stateless persons and aliens.

During the past two years, and particularly in 2014, certain enhanced activities towards implementing the PDP Law have been observed at the MIA. Certain legal and organisational activties were implemented in this period; several by-laws, specifically concerning personal data protection matters, were issued.

Generally, concerning its organisational development, the MIA has a certain degree of maturity in the Georgian context. At the same time, a certain degree of readiness of its management towards implementing the PDP Law in practice can be observed. However, the existing IT systems and workflow procedures were developed prior to the PDP Law entering into force and without regarding its principles, adherence to which requires more effort from the MIA.

3.3.2 Observations[28]

In the processes studied at the MIA, legal grounds for processing non-sensitive personal data *do exist* and are mainly founded on Article 5, Point b and c of the PDP Law, "data processing is enshrined in law" and "data processing is necessary for a data controller to perform obligations prescribed by national legislation" respectively. However, there seems to be a need to critically assess whether processing all currently processed data is absolutely necessary.

Concerns exist in relation to other special category data, for instance: the processing of some special category data is evidently absolutely necessary for the MIA to perform its duties, however, this is not always founded in the Article 6 of the PDP Law; processing of data on health conditions or wanted persons is indeed necessary, but is not covered by any of the cases mentioned in Article 6. Regarding the processing of biometric data, namely fingerprints in certain cases (during readmission) at the border crossing, this is founded on the Article 9 of the PDP Law, and thus happens within the legal grounds.

Additional concerns also exist regarding the fact that access to the database may be given to different State bodies and agencies to fulfil their official duties. Even though such access is permissible by the Law, in some cases the e-services are structured in such a way that public bodies obtain access which goes beyond their needs to fulfil official duties; for instance, a PSDA caseworker can view the entire border crossing history of a person when issuing residence permit, even though he/she requires only a limited amount of information.

Obligation to Inform the Data Subjects

According to Article 15 of the PDP, data controllers (or processors, if applicable) shall provide the data subject, at the time of collecting data from him/her, with some information.

At the border crossing points, even though the border control officers do not inform the data subject or explain their rights related to data protection, some written material

[28] Due to the deficiency in information provided by the MIA in the course of the study, observations only cover readmission management and border crossing.

containing some information on data processing is made available and visible to data subjects.

International data transfers

Personal data are transferred to other states only in the cases of readmission based on the mandatory requirement of the Readmission Agreement and thus can be considered as lawful.

Obligation to provide data security

Data controllers as well as processors are obliged to undertake organisational and technical measures which ensure that data are safeguarded against accidental or illegal destruction, alteration, revelation, access, and any other illegal use and accidental or illegal loss.

Information concerning any measures related to risk assessment and data security in the course of the study was not made available to the study and, therefore, cannot be assessed. However, there is an order from the MIA Patrol Police Department Director about Approval of the Standard Procedures of the Border Crossing Points, which might have a positive influence on data security. Nevertheless, as this document was not available during the study and no information as to whether a prior risk assessment was carried out is known, compliance with the Article 17 of the PDP Law cannot be discussed.

Obligation to register any disclosure of data

Article 18 of the PDP Law provides for an obligation of the data controller and the data processors eventually involved to register all acts of disclosure of personal data. This provision is of high practical importance in terms of the realisation of the rights of a data subject and represents a significant instrument for monitoring the legality of the processing (disclosure) of data.

Decree No. 790 (as of 15.10.2014) of the Minister of Internal Affairs of Georgia 'On settlement of the organisational issues related with the issuance of some information existing in the system of the Ministry of Internal Affairs of Georgia' determines standards of issuing data to other institutions. However, this Decree does not contain a section obliging data processors to keep special record of data disclosure, allowing easy searching of each act of disclosure, but rather a manual search in different systems.

It is worth noting that up until the period of the study, the MIA had no registered incidents related to personal data protection in migration management processes, nor

any cases of someone being liable for a personal data protection related administrative violation.

3.3.3 Recommendations

In order to improve the data processing practices and better align migration management related processes to the Georgian Personal Data Protection Law, it is recommended that the MIA take action in the following areas:

- Analysing threats and specific risks in data processing in the context of data protection.
- Creation of an effective system of informing data subjects at the time of data collection.
- Developing an effective mechanism to register the disclosure of data to third parties, so that any such disclosure is easily traceable.
- Development of a database structure for the e-services, which will allow the creation of more discerning categories of access rights so that only needed data are accessible by a specific user.
- Analysing the procedures related to information security, equipment management and other topics in the context of personal data protection.
- Making participation of the data protection officer mandatory in certain processes, for instance, when defining the scope of access to data by persons in specific positions.
- Developing an internal audit methodology in order to check how effective the policy documents and instructions are with regard to data protection.

3.4 The Ministry of Internally Displaced Persons from the Occupied Territories, Accommodation and Refugees of Georgia (MRA)

3.4.1 Overview

The MRA is the responsible controller of complex data processing activities concerning large amounts of data, a considerable part of which is special category data.

The MRA has approved the policy of personal data protection; however, as the MRA lacks expertise in the field of data protection, its implementation will require substantial effort. The MRA does not have an internal personal data protection officer to fulfil the requirements of the PDP Law, which gains even more importance in the absence of organisational expertise on data protection matters.

3.4.2 Observations

Legal grounds for the processing of data

In the processes studied at the MRA, legal grounds for processing non-sensitive personal data *do exist* and are mainly founded on Article 5, Point b and c of the PDP Law, “data processing is enshrined in law” and “data processing is necessary for a data controller to perform obligations prescribed by national legislation” respectively. However, there seems to be a need to critically assess whether processing all currently processed data is absolutely necessary.

The MRA, in some cases, also processes the following special category data: race or ethnicity, political views, religious or philosophical beliefs, health status, sex life, conviction records, custody history and wanted status. As concerns compatibility with Article 6 of the PDP Law, a legal ground for processing will be found only in the minority of cases, for instance, when processing is done for “public health protection” (Art. 6 (c)). For other cases of processing special category data, a legal basis must be sought in the relevant sectoral legislation. Even though the sectoral legislation does not extend to this matter, this information is submitted by an applicant on his/her own initiative and according to his/her interests. It can be said that the processing of such sensitive data is in the vital interests of the data subject and can be considered as reasonable under the Article 6 of the PDP Law.

However, concerns do exist in relation to other special category data; for instance, the processing of some special category data is evidently absolutely necessary for the MRA to perform its duties, but is not always founded in the Article 6 of the PDP Law.

As for the system of personal data movement inside the MRA, the “need-to-know” principle must be taken into consideration. When granting refugee or humanitarian status, the personal data of a person is available to persons who are not involved in the case management process and do not need the personal data in order to exercise their authorities.

Obligation to inform the data subjects

According to Article 15 of the PDP Law, data controllers (or processors, if applicable) shall provide the data subject, at the time of collecting data from him/her, with some information.

According to the MRA, the data subject is informed about his/her rights in all the processes, however, no specific text has been provided to allow judgment on this matter. However, based on information obtained through direct observation and interviewing data subjects, it seems that the data subject is not provided with the information envisaged under the Article 15.

Obligation to provide data security

Data controllers as well as processors are obliged to undertake organisational and technical measures which ensure that data are safeguarded against accidental or illegal destruction, alteration, revelation, access, and any other illegal use and accidental or illegal loss.

The MRA has not yet carried out identification of threats and risk assessment in migration management; therefore, it is rather questionable whether measures to mitigate potential risks are in place.

Obligation to register any disclosure of data

Article 18 of the PDP Law provides for an obligation of the data controller and the data processors eventually involved to register all acts of disclosure of personal data. This provision is of high practical importance in terms of the realisation of the rights of a data subject and represents a significant instrument for monitoring the legality of the processing (disclosure) of data.

While transferring the data, the Ministry does not ensure the registration of the following information: disclosed data, data receiver, time and legal grounds of disclosure; thus fulfilling the obligations of a controller under Article 18 would call for separate documentation of disclosures, otherwise the right of the data subject to get information on the disclosure of his/her data cannot be exercised in practice.

The MRA does not register appeals concerning personal data protection; up until the period of the study, there have been no recorded instances of administrative liability for the violation of personal data protection rules.

3.4.3 Recommendations

In order to improve the data processing practices and better align migration management related processes to the Georgian Personal Data Protection Law, it is recommended that the MRA take action in the following areas:

- Preparing guidelines and instructions concerning specific processes and divisions.
- Developing guidelines which regulate the use, management and return of assets which are used for data processing.
- Training and awareness raising of employees on issues related to information security and data protection.
- Defining persons responsible for personal data protection.
- Defining procedures for identifying technical weaknesses and recording information security related incidents.
- Amending document flow process when reviewing refugee status.
- Defining rules for work in protected areas.

- Ensuring that data subjects are informed on the processing of their data.
- Ensuring the registration of disclosure of personal data: which data, to whom, when and on what legal grounds.
- Analysing threats and specific risks in data processing; carrying out risk assessment and its possible impact on the right to data protection of the data subjects and determining actions to mitigate these risks.

4. Annex: Position of the Public Services Development Agency (PSDA) on the Summary of the Report of a Baseline Study on Personal Data Protection in the Area of Migration Management in Georgia

- On the issue of receiving excessive information about border crossing, we would like to comment that, in general, receiving the information derives from the law. Any foreigner who addresses the agency about any issue is required to stay on Georgia's territory legally. There is no possibility to determine, whether a person is legally staying on Georgia's territory on Schengen principle, unless it is calculated based on information taken from database on border crossing.

- It is stated in the report that, employee of the agency takes information about a person who might not be an applicant, but has similar data with the applicant. In this case, first of all, it is important to determine which procedures we are talking about; these comparisons take place in different procedures, in different circumstances, also in database of Ministry of Internal Affairs. It should be mentioned, that these issues are already discussed in terms of compliance with Personal Data Protection Standards and appropriate decisions are being made. Data processing in this form is necessary, because in Georgia and many other countries this is the only method to reveal fraud or determine information about wanted person in the field of issuing identity documents. In reality, in Georgia, taking in consideration that it is not long since electronic databases were developed and in the recent past personal data fraud was very popular, using this method is even necessary to avoid issuing documents with inaccurate data. At the same time, there is no probability of tempting employees, because the system is processing data in the same unique method. Therefore, employee cannot use this method in case of their own wish, there is no such possibility at all in the system interfaces. At the same time, the agency took into consideration requirements of PDP law about processing data rationally and only in case of need while developing this method and introduced a method that processes only very similar data. Therefore, the agency cannot agree with the recommendation on additional procession of the data without determining the need. Additionally, specific details of this method were not discussed during the study.

- We receive information about criminal record of a person fully. Though grounds of refusal for residence permit is having criminal record only for the last five years, in other cases, according to article 16, section a and b of Organic Law of Georgia on Citizenship of Georgia - ordinary rule of granting Georgian citizenship; simplified procedure for granting Georgian citizenship; granting Georgian citizenship in exeptional cases; recovering Georgian citizenship; granting Georgian citizenship in special cases, the application is rejected if: a)

the applicant has committed international crime or crime against peace and humanity. b. The applicant was taking part in grave crime against person, state or society. Therefore, the agency needs full information about criminal record of an applicant who wants to naturalize. The same information is needed for examining application for emigration permit from Georgia.

- According to the report, recording information about revealing personal data is not in full compliance with the aim of article 18 of the law. In general law on Personal Data Protection obliges organizations to have registries, in order to have easy access to information. The agency has these means. As for the comment that the procedure is too complicated and there is no easy access to information, it cannot be accepted. The agency owes searching mechanisms (during working process and while getting information from the database). Though the mechanism is complicated (data can be produced by means of analysis and is not readily available for users), this can be seen as positive phenomenon, to avoid unauthorized access and abuse of power by the employees. At the same time, the law does not oblige organizations to create separate registry, where only these data would be stored.

- Policy of PSDA on computer and peripheral equipment mobility reflects business processes and provides mobility of equipment. Recommendation in the report is not clear for us, we did not fully understand what should and should not be included in the order. It would have been better to point at specific gap. There are other individual acts, which regulate safety and destruction of data, so there is a probability that relevant regulations are indicated there.
- Report also states that the data subject is not provided sufficient information about data processing and text given on memory card is not in compliance with article 15. It should be noted that issuing information about processing personal data is made by application and not using the memory card. By signing the application the applicant confirms that he/she is informed.

- Filing system catalogues are currently updated and the PDP Inspector Office is already informed about that.

- It is noted in the report that, it is not necessary for PDP officer to be involved in decision making process about employee's access to information recourses and the officer does not authenticate decisions and projects affecting data protection. There are certain principles in the agency about this issue. According to these principles, officer is monitoring orders. In case of direct access, the agency considers it incorrect to involve the officer, because the officer should not be involved in specific cases – all the employees are equally obliged to obey the law. In general the system works in a way that persons responsible for risks are accessing the risks themselves and they know that they will be responsible if they make a wrong judgment. It is also stated in the report, that in the process of

planning or implementing any new project, service or information system/computer program, as well as modifications, regulations of the law on Personal Data Protection should be taken into consideration. Risks connected to PDP should be identified in advance and appropriate technical or organizational risks should be identified and appropriate measures taken. But there are no instruments to facilitate this approach, for example involvement of PDP officer in these processes. The agency considers that taking in consideration the law does not mean that the officer should directly participate in the processes. The employees who rule the processes can take these issues into consideration themselves. It is also indicated that involvement of officer should be necessary so that he/she had a real power. It can unambiguously be stated from the agency's side, that the role of PDP officer cannot be measured by an obligation to be involved in particular processes, when he/she has lot of other obligations in a large organization such as PSDA.

In the end of the report, there are recommendations provided by IRC, which the agency welcomes, but has its position on few issues:

1. First recommendation: We would like to inform you that information security system ISO 27001 is being implemented in the agency. The agency is under obligation to implement this system according to the law on Information Security as the agency is subject of critical information. The standard in itself involves registration of all information actives and determination of their critical levels, analyzing risks and developing their protection mechanisms. For now the agency plans to use this system for main business projects of civil registry department. Two business process analyses have already been finalized.
2. Third recommendation: agency's position is stated in the above paragraph.
3. Fourth recommendation: concerning creating new structures of databases and electronic services, (which will enable separation of data in a way that their receipt and issuance will be provided according to the real need) we would like to inform you that, this system is already created for external users and is in the process of implementation now.
4. The agency executes it obligations and processes the data in accordance with the law. Different departments are continuously working in order to achieve this goal.
5. Sixth recommendation: The agency considers that it is not justifiable to include who possesses what data in legal acts. The data is processed and processes are controlled without this process in accordance with the principles of law on Personal Data Protection.
6. According to the law on "Prevention of Legalising Unlawful Income," In order to identify a client, person who is doing monitoring has a right to access identification documents' electronic databases of PSDA in accordance with the

law. Number of transactions are under monitoring of commercial banks, the law includes its exact list. According to this regulation, in order for the bank to process personal data of a person in cases written down in law on “Prevention of Legalising Unlawful Income” and in accordance with article 5 section g of the law on Personal Data Protection, it is necessary that the few circumstances were present. It is possible to add article 5 section g as one of the bases for data processing while drafting contracts with the banks, but in this case articles of law on Prevention of Legalising Unlawful Income will also be included and during processing the bank will be obliged to provide documents to justify spesific legislative bases for each case. As for creating appropriate legislative basis, the agency is not authorized to give recommendations to institutions from private sector on which legislation should be used, while processing data or how to arrange business projects. While contracting the banks, the agency, takes into consideration obligations under law on PDP fully and checks whether the banks have violated obligations under the contract during monitoring of the contracts. The agency is not competent to determine working directions of organizations and give recommendations.

7. Eighth recommendation: the agency’s position on recommendation number 8 is widely discussed in the above paragraph; accordingly, we will not repeat it here.

8. Ninth recommendation: the agency’s position on recommendation number 9 is also widely discussed in the above paragraphs; accordingly we will not repeat it here.

9. Every year working plan on territorial and structural units is approved by internal audit of the agency. Document also involves spheres and directions which are monitored, more precisely business processes and scopes of audit. One of the directions of this document is to study and evaluate lawfulness of personal data processing.