GUIDELINES ON RECORDS OF PERSONAL DATA PROCESSING ACTIVITIES

February 2023

Guidelines on Records of Personal Data Processing Activities

February 2023

This guideline was supported by the OSCE Mission in Kosovo.

Table of Contents

1. Introduction **6**

2. Personal Data Protection Legal Framework **7**

3. Information and Privacy Agency **7**

4. Records of processing activities **8**

4.1. What should records of processing activities contain 10

4.1.1. Name and contact information of the controller and, where applicable, of the common controller, the representative of the controller and the data protection officer ... 11

4.1.1.1. Data controller/processor 12

4.1.1.2. Joint controllers 13

4.1.1.3. Representatives of data controllers 14

4.1.2. The purpose of personal data processing 15

4.1.3. Categories of data subjects and categories of personal data 16

4.1.4. Categories of recipients of personal data 18

4.1.5. Transfer of personal data to a third country or an international organization 18

4.1.6. Personal data retention periods 20

4.1.7. Technical and organizational security measures 23

4.1.8. Lawful basis for personal data processing 24

4.1.8.1 Consent 26

4.1.8.2. Contract 29

4.1.8.3. Legal obligation 30

4.1.8.4. Legitimate interest 30

4.1. 8.5. Vital interest 32

4.1.8.6. Public interest or exercise of official authority 33

5. Contract between the controller and the processor **33**

6. The role of the data protection officer **35**

7. Conclusion **36**

Annex I 37

Record of processing activities for controllers

Annex II 39

Record of processing actvities for processors

Abbreviations

CE	Council of Europe
CRM	Customer Relationship Management
EU	European Union
GDPR	General Data Protection Regulation
IPA	Information and Privacy Agency
LPPD	Law on Protection of Personal Data

1. Introduction

Personal data can be processed only under the conditions set forth by relevant legislation, thus the Law on Protection of Personal Data (hereinafter the LPPD)[1] which defines the principles, criteria, measures, procedures, and the competent authority for supervising personal data processing. Under the LPPD, protection of personal data is guaranteed to every individual regardless of his/her nationality, ethnic or racial origin, religious beliefs, political opinions or other characteristics.

Personal data controllers and/or processors create and keep records of personal data processing activities, which constitute a written documentation of all personal data processing activities carried out by them. These records are documents with inventory and analysis purposes, which should reflect the reality of personal data processing. Records of processing activities allow public institutions and public or private companies to make an inventory of the data processing and to have an overview of what they are doing with the concerned personal data. These records also allow to precisely identify: the actors involved in personal data processing (controllers, processors, representatives, joint controllers), the categories of data processed, the purpose of the processing, who has access and who are the recipients of personal data, for how long will the personal data be retained, as well as the technical and organizational security measures that are implemented during the processing of personal data.

Guidelines on Records of Personal Data Processing Activities aim to provide practical instructions in a clear and user-friendly way for controlling/processing entities in respect of records of processing activities, as well as elucidate principles to be adhered to when processing personal data. These Guidelines are intended to guide public institutions and private companies in creating and maintaining records of personal data processing activities, and set out requirements which must be met where such records are created and maintained. These Guidelines were developed in conformity with the LPPD, the European Union (EU) Regulation for the Protection of Personal Data[2] and the (CE) Convention on data protection[3] with a view to be used by controlling/processing entities as guidance and recommendations on how to transpose legal framework provisions in terms of records of

1 Law No. 06/L-082 on Protection of Personal Data.
2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
3 Council of Europe Convention No. 108 on data protection - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

processing activities.

2. Personal data protection legal framework

Keeping records of personal data processing activities by controlling entities is governed by the LPPD.

The LPPD lays down the principles, legal bases and purposes of personal data processing, security measures, data subject rights and the obligations to keep records of processing activities and to provide information to and request authorization from the Information and Privacy Agency (hereinafter IPA), which must be followed by controlling entities and processors of personal data. The Law on the Protection of Personal Data was drafted in accordance with the EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter GDPR).

Any processing of personal data in the context of the activities carried out by a controller or a processor in Kosovo should be carried out in compliance with the LPPD and its principles.[4]

3. Information and Privacy Agency

The Information and Privacy Agency is an independent authority in charge of supervising the implementation of legislation for protection of personal data and access to public documents and information. IPA is completely independent in fulfilling its duties and exercising its powers and reports to the Assembly of Kosovo.

In respect of personal data protection, pursuant to Article 64 of the LPPD, IPA has the following responsibilities:

- supervises the implementation of the LPPD;
- provides advice to public and private bodies on issues related to data protection;
- informs the public on issues and developments in the area of data protection;
- promotes and supports fundamental rights to personal data protection;
- decides on complaints filed by data subjects;

4 Article 4, Law No. 06/L-082 on Protection of Personal Data.

- advises the Assembly, the Government, other public institutions and bodies on legislative and administrative measures in relation to protection of fundamental rights and freedoms of natural persons in terms of data processing;
- carries out inspections regarding the implementation of the LPPD.

As appropriate, the IPA carries out periodic reviews of certifications issued in accordance with Article 43 of the LPPD and may withdraw the certifications, in case the certification criteria are not met; on its own initiative or upon request, provides opinions on public institutions and other bodies, as well as publishes on any issue related to the protection of personal data. The IPA co-operates with Kosovo institutions, international institutions, and other EU bodies regarding issues that are considered important for the protection of personal data.

The IPA is led by the Commissioner, responsible for representing the institution and organizing and coordinating its activities.

Based on the above, the IPA can supervise controllers and processors both ex officio and upon complaint, conducting inspections and checks with a view to overseeing compliance with the legislation for the protection of personal data.

Oversight of the obligation to keep **records of processing activities** by controllers and processors also falls under. Hence, records of processing activities must be made available, on request, to the IPA at all times.

4. Records of processing activities

The Law on Protection of Personal Data, specifically Article 29 therein, obligates written evidence and overview of the procedures by which personal data are processed. The Records help the controller/processor to be in control over their processing activities and LPPD, and it is in their best interest to male it easier for supervisory authority to do all the intended inspection. By having accurate and complete records, public institutions and public or private companies will be able to prove that they are taking the LPPD seriously by applying a systematic approach to mapping and governing data flows and related processing activities. The record of processing activities is a very useful means to support an analysis of the implications of any processing. The record facilitates the factual assessment of the risk of the processing activities performed by a controller or processor on individuals' rights, and the identification and implementation of appropriate security

measures to safeguard personal data. Records of processing activities must include significant information about data processing, including data categories, the group of data subjects, the purpose of the processing and the data recipients. These records must be made available to the IPA upon request.

The obligation to create and keep records of processing activities is not only imposed to the controller and their representative, but also to the processor and their representatives as set forth in Article29, paragraph 1, of the LPPD. The obligation to keep records does not apply to institutions and companies employing fewer than 250 persons, if the processing is not likely to pose a risk to the rights and freedoms of the data subject, if the processing is done only occasionally or if no special categories of data are processed, as defined in Article 29 of the LPPD. Based on the LPPD, a personal data controller (company or institution) employing over 250 employees is obligated to keep records of processing activities. Notwithstanding the above, a controller or processor must keep records of processing activities if one of the following conditions exists:

- if the processing is likely to result in a high risk to the rights and freedoms of data subjects (for example: introduction of new technologies such as biometric readers, facial recognition, IT services that process personal data);
- if the processing is not occasional or temporary, i.e. the processing is permanent[5] (for example: processing an employee's personal data for the purpose of payment of wages by the employer);
- if processing involves special categories of data (for example: health data, biometric data, genetic data);[6]
- if the processing involves personal data relating to criminal convictions and offences.[7]

Example 1: In order to market its products as successfully as possible and increase sales, the controller, which is a small manufacturer with 20 employees, hires a marketing agency that creates profiles of social network users and uses their personal data for targeted advertising.

5 A great deal of processing is permanent, such as the processing of personal data of employees for the purpose of salary payments, processing of personal data by means of cookies, processing of personal data through video surveillance, processing of personal data in CRM (customer relationship management software) systems, processing of personal data for the purpose e-commerce, direct marketing activities, etc. In all these cases, the processing officer is obliged to keep records of processing activities.

6 Article 8, paragraph 1, Law No. 06/L-082 on Protection of Personal Data.

7 *Ibid*, Article 9.

Although the company has less than 250 employees, the processing entrusted to the processor (marketing agency) may pose risks to the rights and freedoms of data subjects (innovative technology, profiling) and is therefore required to keep records of processing activities. The processor is obligated to keep records of processing activities in this case as well.

Example 2: A medical laboratory has only 10 employees, however it processes the health data of its customers. Since the data processed also includes special categories of personal data, it is obligated to keep records of processing activities.

Based on the above, a controller employing fewer than 250 persons, and where none of the above conditions exist, is not obligated to keep records of processing activities.[8] However, it is recommendable to keep such records as the data contained in these records are a means to verify compliance with the LPPD.

The IPA may carry out inspections and audits to monitor controllers and/or processors' compliance with the obligation to record processing activities.[9]

If a company or institution fails to keep records of processing activities as required under Article 29 of the LPPD, it shall be subject to fines.[10]

4.1. What should records of processing activities contain

Pursuant to Article 29 of the LPPD, records of processing activities should contain the following information:

- name and contact information of the controller and, where applicable, of the joint controller, the representative of the controller and the data protection officer;
- purpose of processing;
- a description data subjects' categories and personal data categories;
- categories of recipients to whom personal data were or shall be disclosed, including recipients in third countries or international organizations;

8 *Ibid,* Article 29, paragraph 4.
9 *Ibid,* Article 68, paragraph 1, subparagraph 1.3.1.
10 Article 92, paragraph 1, sub-paragraph 10, of the LPPD provides that "*The legal person or the person discharging such independent activity shall be punished for a minor offence of twenty thousand (20,000) to forty thousand (40,000) €, if he or she fails to ensure that the filing system catalogue contains the information provided for by Article 29 of this Law*".

- where applicable, transfer of personal data to third countries or to an international organization, including the identification of that third country or international organization, the authorization according to Article 49, paragraph 2, of this Law and in cases of transfers referred to in Article 49, sub-paragraph 1.9, of this Law, documentation of adequate protective measures;[11]
- where possible, the envisaged time limits for erasure of the different categories of data;
- where possible, a general description of technical and organizational security measures referred to in Article 31, paragraph 1, of the LPPD.[12]

In addition, it is recommended to keep records on the legal grounds for personal data processing.

To guide personal data controllers and processors, the IPA has developed a sample form for recording processing activities, which helps controllers and/or processors in keeping records of their processing activities (Annex I and II).

4.1.1. Name and contact information of the controller and, where applicable, of the joint controller, the representative of the controller and the data protection officer;

To start with, the following names and contact information should be entered in the first section of the record of processing activities:

- controllers and processors;

11 Article 49 paragraph 2 of the Law No. 06/L-082 on Protection of Personal Data stipulates that *"The data controller may transfer personal data only upon receipt of the authorization (from the Agency) according to paragraph 1 of Article 49. In his or her request for authorization the data controller shall provide the Agency with all information necessary regarding the required transfer of personal data. This includes in particular the categories of data, the purpose of the transfer and the safeguards in place for the protection of personal data in the other country or international organization."* Article 49 paragraph 1.9 provides that "*the data controller adduces adequate safeguards for the protection of personal data and the fundamental rights and freedoms of individuals as regards the exercise of adduced rights. Such safeguards may result from the provisions of the contract or the general terms of business activities governing the transfer of personal data*".

12 Article 31 of the Law No. 06/L-082 on Protection of Personal Data stipulates that the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate: the pseudonymization and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

- joint controllers, if applicable;
- representatives of the controller;
- personal data protection officer.

4.1.1.1. Data controller/processor

According to the LPPD, **a personal data controller** is any natural or legal person from the public or private sector, which, individually or jointly with others, **determines purposes and means of personal data processing**.[13]

A personal data **processor** is any natural or legal person from the public or private sector which **processes** personal data for and on behalf of the data controller.[14]

As noted above, the controller decides on data processing activities, exercises overall control over personal data being processed and is ultimately responsible for their processing.

Personal data controllers can be natural or legal persons, commercial companies, micro, small and medium sized enterprises, agencies, public authorities, non-governmental organizations, etc. In other words, municipalities, ministries, banks, insurance companies, tourist agencies, department stores (markets), marketing agencies, hospitals, hotels, etc., may be personal data controllers.

Controllers are responsible to ensure that they act in conformity with the GDPR and demonstrate full compliance with all personal data protection principles. They are also responsible to act in accordance with the LPPD in terms of the fulfilment of the requirements by any processor they contract to process the data. Controllers should demonstrate fairness, legality and transparency, accuracy, data minimization, integrity and retention, as well as complete confidentiality of personal data.

Furthermore, pursuant to Article 23 of the LPPD, data controllers shall:

- take into account the purpose, scope, nature, context of any data processing activity;
- take into account the likelihood of a serious risk to the freedoms and rights of natural persons;

13 Article 1, paragraph 11, Law No. 06/L-082 on Protection of Personal Data.
14 *Ibid* Article 1, paragraph 14.

- implement appropriate organizational and technical measures and security measures to demonstrate that data processing activities are performed in accordance with the LPPD;
- review and update these measures as necessary.

The personal data **processor** processes data on behalf of the controller and as per their instructions. They act under the authority of the respective controller. Pursuant to Article 28 of the LPPD, the processor shall not process personal data except as instructed by the controller, unless required to do so by any specific law. Usually, the data processor is a third party outside the institution or company as a controller. The obligations of the processor towards the controller should be determined by way of a **contract for personal data processing** concluded between the controller and the processor. The processor may outsource part of the work to another processor or appoint a common processor **only upon prior written authorization of the data controller**. Processors are not bound by the recording obligations applicable to controllers pursuant to the LPPD, however, the LPPD imposes some direct obligations on processors as well.[15]

In case of personal data breaches, data subjects can lodge compensation claims with both data controllers and data processors. Where a data processor acts in contravention with the lawful instructions of the data controller, it shall be liable for any data breach or damage caused. The same applies to cases where a processor fails to comply with the obligations provided for in the LPPD.[16] Therefore, data processors must always ensure that they comply with the provisions of the LPPD. Claims for compensation shall be lodged before the competent court.[17]

4.1.1.2. Joint controllers

In order for two or more companies or institutions to be considered as joint controllers, their joint participation in determining the purposes and means of processing is necessary. According to the LPPD, joint controllers have a common purpose and jointly agree on the purpose and means of data processing.[18]

Joint participation in determining the purposes and means of processing can be manifested

15 *Ibid* Article 27.
16 *Ibid* Article 56 paragraph 2.
17 *Ibid* Article 56, paragraph 6.
18 *Ibid* Article 25, paragraph 1.

in respect of making joint decisions regarding personal data processing. Moreover, this means that an organization together with another organization decides the "why" and "how" of personal data processing.

An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each controller is inseparable.

Joint controllers must determine among themselves which of them shall take primary responsibility. They share or define their respective responsibilities for compliance with processing obligations in a transparent manner, as well as bear equal liability for any security breaches and any fines that may be imposed on them.

Example: to promote electric cars, a manufacturer joins with several other car manufacturers to jointly develop a commercial website that collects user data, such as IP addresses. Therefore, all car manufacturers involved should agree together what and whose data will be processed, thus defining the common purpose and means.

Controllers who process the same data, but for different purposes, are not considered joint controllers.

4.1.1.3. Representatives of data controllers

Controllers and processors designate in writing a representative in Kosovo where data controllers are not established or do not have branches in Kosovo but process personal data, make use of automatic or other equipment in Kosovo, unless such equipment is used only for purposes of transit through Kosovo.[19]

In these cases, the controller and the processor must designate a natural or legal person established in Kosovo to represent them in terms of their obligations pursuant to the LPPD.

The representative will act on behalf of the controller or processor and may be addressed by the IPA, AIP and data subjects, on all matters related to processing for the purposes of ensuring compliance with the LPPD.

According to the LPPD, the representative must be designated in writing by the data controller or processor to act on their behalf, and its designation does not affect the

19 *Ibid* Article 26, paragraph 1.

responsibility or liability of the controller or of the processor. Such a representative should perform its tasks according to the mandate received from the controller or processor, including communicating with data subjects and co-operating with the IPA with regard to any action taken to ensure compliance with the LPPD.

It should be noted that the designation of a representative is not necessary where the processing:

- is occasional;
- does not involve large scale processing;
- does not involve special categories of data as set out in Article 8 of the LPPD;
- does not result in a risk to the rights and freedoms of natural persons. In addition, this does not apply to a public authority or institution.[20]

It should always be noted that processors and personal data protection officers cannot be designated as representatives of the controller.

4.1.2. The purpose of personal data processing

Before commencing personal data processing, the controller or the processor should determine the purpose of processing at the time of personal data collection. Data may only be processed for **specified, explicit and legitimate** purposes.

The purpose of processing personal data means in the first place that an institution is aware of the reason for which it wants to process certain personal data. Therefore, in these cases, the institution or company needs to asses in the first place why it needs certain data to achieve the purpose for which they are processed.

Personal data is processed for various purposes, such as marketing, service improvement, research, product development, human resource related issues, advertising, property and life safety, etc.

The purpose of personal data processing can be a legal obligation, a contractual obligation or where there is, in specific cases, a legitimate interest pursued by an organization in processing specific personal data.

20 *Ibid* Article 26, paragraph 2.

The purpose is a legal requirement where a specialized law provides for the processing of personal data, such as the Kosovo Labour Law requiring employers to keep records on their employees, therefore, processing of personal data is necessary for compliance with a legal obligation to which the controller is subject. [21]

The purpose is a contractual obligation where, for example, a company that offers the sale of products online may require a customer's personal data to conclude a sales contract, such as customer's first name, last name, phone number, address, etc.

The purpose of processing for certain legitimate interests pursued by an institution or company is applicable where, for example, there were several break-ins in a grocery shop over the course of a year and an employee got injured in the last break-in. The shop subsequently sets up a camera surveillance system to ensure the safety of property and lives, as well as the physical integrity of individuals. However, consideration in this case should be given to whether a test of the legitimate interests in installing a camera surveillance system has been carried out and documented in advance, and whether notification of surveillance (warning sign) containing all elements, such as information about the controller, purpose of processing, data retention period, etc. has been displayed in a visible place.

It should always be noted that personal data must be processed for a specified purpose and that there must be legitimate legal grounds for such processing.

4.1.3. Categories of data subjects and categories of personal data

The LPPD does not specifically define data subjects, rather the legal definition of the data subject is outlined parenthetically in the definition of "personal data", which is defined as any information related to an identified or identifiable natural person ("data subject"). Therefore, a data subject is an **identified or identifiable natural person**.

An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to his/her data.

Data subjects are natural persons whose personal data are processed by a controller/processor. A data subject may be a natural person such as an employee, a person who purchased goods and services, used relevant software, navigated a website, a

21 *Ibid* Article 5, paragraph 1 sub-paragraph 3.

customer, a patient, a person subject to behavioural analysis, etc.

Data subject categorization is a way of classifying data subjects into groups or categories. To categorize data subjects, a controller may group data subjects as follows: shareholders, employees, officers, candidates, customers, students, volunteers, website users, software users, contractors, patients, etc. By means of such a categorization, a controller has a clearer overview of the data it retains.

Legal entities, organizations and companies are not considered data subjects.

The concept of personal data refers to any information relating to a natural person. Personal data includes first and last name, postal address, email address, telephone number, date of birth, personal or identity card number, trade union membership data, IP address, location information, credit/debit card number, health data, biometric data (e.g. fingerprints), images of an individual in a video recording or photo, audio recording, vehicle registration number, and numerous other data.

Personal data revealing information about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation constitute a special category of data, and their processing is generally prohibited under Article 8, paragraph 1 of the LPPD. The processing of such data is in principle prohibited because each of such types of data pose a risk to the individual concerned should they be processed unlawfully.

Moreover, when it comes to increased risk, it also exists in the case of processing personal data of certain categories of data subjects. For example, children, who are regarded vulnerable in any way, merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Personal data can be categorized as follows:

- identifying data: including account number, phone number, name and address, credit card number, employee identification card, etc.;
- data describing the identity: such as first and last name, birthday, address, age, education, nationality, gender, height, citizenship, profession, religion, race, sexual orientation, etc.;
- biometric data: fingerprints, facial features, DNA, signature, voice recordings,

etc.;

- health data: such as health condition, health history, lifestyle, medical tests, medical treatments, etc.;
- financial data: such as assets and properties, salary, family assets, financial transactions, bankruptcies, etc.;
- data on behaviour and character;
- data on media and communication, etc.

4.1.4. Categories of recipients of personal data

According to the LPPD, the recipient of the data can be "a natural or legal person from public of private sector, to which the personal data are disclosed, whether a third party or not."[22] Therefore, a recipient can be a public or private company, public institution, agency, organization, person outside the company or an employee of the company that processes personal data in the course of their tasks and on behalf of and on instructions from the company controlling the data. **For example**, a company which processes its employees' personal data for the purpose of employee records and payroll calculations is required to forward personal data to the Kosovo Tax Administration and the Kosovo Pension Savings Trust. In this case, the recipients of personal data are the Kosovo Tax Administration and the Kosovo Pension Savings Trust.

4.1.5. Transfer of personal data to a third country or an international organization

Personal data is transferred abroad frequently, therefore controllers should ensure an appropriate level of protection of the individual's personal data being transferred.

Transfer of data to other countries or to an international organization means delivering personal data to "recipients" in other countries. At any rate, transfers to third countries and international organizations may only be carried out in full compliance with Chapter XI of the LPPD. A transfer takes place only if the requirements set out in the provisions of the LPPD regarding the transfer of personal data to third countries or international

22 *Ibid* Article 3, paragraph 1, subparagraph 15.

organizations are met by the controller or processor.

Pursuant to Article 44 of the LPPD, the transfer of data is permissible only to countries or international organizations with adequate safeguards in place for protection of personal data, which are listed in a list issued by the IPA with a formal **decision** pursuant to the LPPD[23] which is published in the Official Gazette of Kosovo.[24]

Notwithstanding the above, transfers to countries or international organizations **not** ensuring an adequate level of data protection may take place only in the following cases:

- it is so provided by another law or binding international treaty to which Kosovo is a party;
- the data subject has given his/her consent;
- the transfer is necessary for the performance of a contract between the data subject and the data controller;
- the transfer is necessary for the conclusion or performance of a contract concluded in the data subject's interests between the data controller and a third party;
- the transfer is necessary and legally required on important public interest grounds, to protect the life of the data subject, as well as for the exercise of legal claims;
- the data controller adduces adequate safeguards for the protection of personal data and the fundamental rights and freedoms of individuals as regards the exercise of adduced rights.[25]

According to Article 49 of the LPPD, such transfers by the controller to a third country or an international organization not ensuring an adequate level of data protection may only take place upon receipt of an **authorization by the IPA**. In his or her request for an authorization, the data controller should provide the IPA with all information necessary regarding the transfer, such as: categories of data, the purpose of the transfer and the safeguards in place for the protection of personal data in the other country or international organization.

23 *Ibid* Article 45 and 46.

24 Decision of the Commissioner of the Information and Privacy Agency on the list of countries with an adequate level of personal data protection, available at https://aip.rks-gov.net/download/vendim-lista-e - countries-with-adequate-level-of-personal-data-protection/.

25 Article 49, sub-paragraphs 1.1 - 1.9, Law No. 06/L-082 on Protection of Personal Data.

An example of a transfer of personal data to a company abroad could include instances where a bank operating in Kosovo provides debit or credit cards as part of the services it offers to its customers. To manufacture these cards, the bank contracts a specialized company from abroad. In order to have the service delivered, the bank must transfer the personal data of its customers to the contracted company to personalize the cards. In order to transfer such personal data, the bank should consider the legal requirements set out in Chapter XI of the LPPD.

4.1.6. Personal data retention periods

In order to ensure that personal data are kept for no longer than it is necessary, the controller should make a record of retention periods for different categories of personal data. Wherever possible, the controller should also indicate the criteria because of which the retention period is set.

The LPPD provides that data subject has the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are processed: where a data subject has withdrawn his or her consent objects to the processing of personal data for if based on legitimate interest or for the performance of a task carried out in the public interest; in the exercise of official authority or for direct marketing; where the processing of his or her personal data does not otherwise comply with the LPPD and, when the personal data have been processed to offer information society services to a child.[26]

However, the further retention of the personal data should be lawful where it is necessary:

- exercising the right of freedom of expression and information;
- complying with legal obligation on performance of a task carried out in the public interest or, in the exercise of official authority vested to the controller, on the grounds of public interest in the area of public health;
- establishment, exercise or defence of legal claims.[27]

The LPPD does not set any specific personal data retention limitations or periods. Therefore, the controller, whether an organization, public authority or private company, should be

26 *Ibid* Article 16, paragraph 1.
27 *Ibid* Article 16, paragraph 3.

clear on the time period within which certain personal data need to retained to achieve the purposes for which they are processed, on the basis of the principle of data minimization, the principle of accuracy[28] and local laws.

When it comes to personal data retention and the lawful bases for their processing, it is vital that the controller and/or processor are aware of the special legislation governing the activity in which they engage. More precisely, retention of personal data is often provided for in special laws and secondary laws.

If the subject matter is not specified, the company should be guided by the principle of "**storage limitation.**" This principle stipulates that personal data may be stored insofar as necessary to achieve the purpose for which are further collected or processed, and may be stored for longer periods if these data is processed exclusively for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes. [29]

It is recommended that controllers **establish the policies** which would set forth the period of retaining different categories of data. At the same time, the controllers must take into account that in setting the storage period, they are subject to special legislation, which provide on the storage period of the relevant personal data, and in these cases the controllers must observe the special laws regarding the storage period of data. Controllers must identify each law providing on their requirements of storing relevant data for certain periods. The storage limitation principle basically establishes that personal data may **be stored only insofar as necessary to achieve the purpose of their collection**, which means that personal data must be kept in a form that allows the identification of data subjects not longer than necessary to achieve the purpose for which they are processed.

Regardless of the manner of collecting personal data, when determining data storage periods, controllers must always depart from the purpose of the processing. The controller must set forth the purpose to be achieved and how long the collected data will be needed to achieve that purpose. Should the controllers collect data that law to process requires them, and then they can easily set forth the data storage period, because that is already provided

28 According to the principle of data minimization, data will be processed only to the extent necessary to achieve the specified purpose. Personal data must be adequate, relevant and must not exceed the purposes for which they were collected or further processed. This principle compels companies to limit themselves to the minimum of personal data they require within a processing activity and its purpose. The collected data must be appropriate and proportionate to the purpose for which it is processed. Whereas, according to the principle of accuracy, data must be valid, accurate and up-to-date, and personal data controllers must take measures to rectify or delete inaccurate personal data promptly, taking into account the purposes for which they are processed.

29 Article 4, paragraph 5, Law on No. 06/L-082 Protection of Personal Data.

for by specific legislation on the basis of which they are required to process personal data. **For example,** tax legislation requires that controllers retain data for 6 years, whereas legislation on office work administration requires that state institutions retain personnel files for a period of 50 years.[30] If a special law does not provide for data retention period, then the controller is required to establish its own retention periods, and conduct periodic reviews of the data.

If a controller/processor processes data for the purpose of archiving for public interest, for the purposes of scientific or historical research, or for statistical purposes, then the controller may retain such data for an indefinite period. However, they cannot process such data sets for any other purpose, and are required to implement appropriate technical and organizational measures, as will be explained below (see 4.1.7).

When controllers determine their purpose of processing, they must also establish a data retention period, namely how long will data be retained before it is erased, destroyed, blocked or anonymized based on specific laws defining relevant data retention periods.

The retention period must be proportionate to the purpose. **For example**, if a controller/processor carries out camera surveillance in order to prevent damage to public or private property, a period of no longer than one month is sufficient for the storage of such data. If discovered that the property has suffered damage, then the data proving such damages, which in this case is the camera recording, may be stored for a longer period, as necessary to take legal action. Otherwise, the retention period should be at most one month, as stated above.

Another example relates to establishing retention periods for CVs of natural persons (candidates), collected in the course of an employment procedure in a recruitment company. Assuming that the data retention period (CVs) established by the recruitment company 10 years, the retention period is not proportionate to the purpose of finding employment for a person, in the short or medium term, therefore, if they are kept for too long, they will eventually become outdated or irrelevant, and cannot or should not be used.

30 Ministry of Internal Affairs Regulation (MIA) No. 05/2020 Amending and Supplementing the Regulation (MPA) No. 01/2015 on Unique Marks for Classification of Documents and their Storage Deadlines, available at https://gzk.rks-gov.net/ActDetail.aspx?ActID=34225.

4.1.7. Technical and organizational security measures

The risk to the rights and freedoms of natural persons may result from personal data processing which could lead to physical, material and non-material damage, such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data protected by professional secrecy, etc. In order to protect the rights and freedoms of individuals against the risks arising personal data processing, a series of technical and organizational measures, as provided for in the LPPD, should be undertaken.

To prevent potential personal data breaches, the controller is required to take appropriate technical and organizational measures to ensure an appropriate level of security proportionate to the risks inherent in personal data processing. Personal data breaches includes any breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

For this purpose, the controller should adopt **internal acts**[31] to guide the implementation of appropriate measures, demonstrate compliance with the LPPD and implement measures that guarantee an appropriate data processing security level.

Technical security measures involve safeguards that are taken in physical locations, information technology systems/devices used within the controlling entity or as part of the final products that are used and related to personal data processing. In addition, the controller should indicate technical measures in contracts with third parties which have access to personal data or together with which it participates in data processing. Technical measures, which must be set in place and are foreseen by the LPPD include:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the use of strong passwords on computers, creation of backup copies of data;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of

31 Code of conduct and certification, as provided in Articles 41 and 43, Law No. 06/L-082 on Protection of Personal Data.

technical and organisational measures for ensuring the security of the processing;[32]

- the use of antivirus software, etc.

For example, some issues within the company must be regulated by internal rules:

- personal data protection and information security policy,
- authorizations for personal data processing,
- non-disclosure statements,
- access to select data,
- data retention periods,
- handling requests from data subjects regarding their rights,
- contracts with processors,
- safe use of the Internet and official company equipment, etc.

It is of vital importance to raise awareness among all controllers, especially given the fact that data breaches are for the most part human errors.

4.1.8. Lawful basis for personal data processing

According to the LPPD, controllers should have lawful bases in order to process personal data processing carried out by them (by the controllers themselves or their processors). The legal bases for the processing of personal data are provided by Article 5 of the LPPD, however, when the processing concerns special categories of data or data related to criminal sentences and misdemeanours, Articles 8 and 9 of the LPPD shall apply.

The legal grounds for data collection and processing are mandatory to ensure the legitimacy of personal data processing.

Article 5 of the LPPD stipulates six criteria that constitute the legal basis of the processing. If the controller/processor processes specific categories of data, it must establish one of the exceptions provided for in Article 8 of the LPPD. Processing is lawful only if the personal data is processed on the basis of the consent of the data subject, the necessity to comply with

32 Article 31, paragraph 1, Law No. 06/L-082 on Protection of Personal Data.

a legal obligation to which the controller is subject, or the necessity of performing under a contract to which the data subject is a party, or to undertake actions at the request of the data subject before the stipulation of the contract, the vital interest of the subject, the public and the legitimate interest.

Failure to observe the legal basis of processing may lead to various violations of the LPPD, and in particular, violations of the rights of individuals. Consequently, such violation of legal basis may be sanctioned with a fine of twenty thousand (€20,000) to forty thousand (€40,000).[33]

Based on the above, whenever an organization, company or public authority wishes to collect, store, publish, distribute, delete or dispose of personal data, there must be a legal basis for such processing. Personal data must be processed based on:

- Consent – which means that the data subject has given explicit consent to the controller to process his or her personal data for a specific purpose;
- Contract – processing is necessary for the performance of a contract that the controller has entered into with the data subject, or because the subjects have requested that special steps be taken by the controller prior to entering into a contract;
- Legal obligation – processing is necessary for compliance with the law (not including contractual obligations);
- Vital interest – processing is necessary to protect someone's life;
- Public interest – processing is necessary for the controller to carry out a task in the public interest or in the exercise of official authority, whereby such task or function is clearly laid down by the law.
- Legitimate interest – processing is necessary for the legitimate interests pursued by the controller or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

33 *Ibid* Article 92, paragraph 1, subparagraph 1.

4.1.8.1 Consent

One of the lawful bases for data processing is the consent of the data subject, which is defined as: *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*[34].

Consent is considered valid when:

- ***is freely given*** – meaning that consent will not be valid if the data subject has no other choice and feels compelled to consent or endure negative consequences in case of refusal to consent. Therefore, the data subject should be free in giving/refusing consent without any negative consequences, and be able to withdraw his or her consent anytime;
- ***is specific*** – meaning that consent must be clear and given for each specific purpose, while the data subject has a choice in relation to each of them. The consent request must be clearly specified and must be distinct from general terms and conditions. For each consent request, controllers should provide separate information in relation to the data being processed for each purpose, so that data subjects are made aware and have the possibility of different choices. In this way, data subjects may give specific or separate consent;
- ***is informed*** – meaning that for consent to be considered valid, the subject of personal data must be clearly informed of the purpose for which he or she is giving consent. Though the timing or the moment of obtaining consent has not been explicitly prescribed, the wording of the provisions implies that it must be obtained before data processing begins. In order to comply with this requirement, the controller must inform the data subject about controller's identity, the purpose of each of the processing operations for which consent is sought, what categories of data will be processed, **and the right to withdraw consent at any time.** Withdrawal of consent must be possible in the same way as giving consent. The information provided by the controller must be comprehensible to everyone, not only those who are aware of the legal or economic jargon, but the public. In the event of failure to duly inform the data subject, the controller will be in violation of the LPPD and the IPA shall impose punitive measures or administrative fines as provided in Article 101 of the LPPD.

34 *Ibid* Article 3, paragraph 1, subparagraph 17.

- ***clear affirmative action exists -*** meaning that the data subject must have taken a deliberate action to consent to the processing. Silence or inaction on the part of the data subject cannot be considered as an indication of consent.

Given that some categories of personal data fall into the category of special data, processing this data requires treatment that is more specific. In addition to meeting the above requirements, consent to processing of data under this category must also be *clearly stated*, which means that it must be given **in the form of a written statement.** With regard to processing sensitive categories of personal data, the LPPD provides that consent must be given in writing in some cases. More specifically, Article 8, paragraph 2.4, provides that if *"processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to their members or data subjects who have regular contact with it in connection with its purposes and that the personal data are not disclosed **without the consent** of the data subjects".*

The controller should make sure that the data subject signs a written statement.

For example, by writing the first and last name or pressing a button (selecting a check box) which states "*I, hereby, give consent to the processing...*"

This does not mean that the data subject needs to write a statement in their own words, the controller can provide it for them. However, it is important that the data subject understands and agrees with the statement.

Where personal data processing is based on consent, the controller will bear the burden of proof in the event of a dispute regarding the existence of data subject's consent to data processing. This means that the controller must be able to demonstrate that the data subject has consented to the processing of his/her data and that the prerequisites for the validity of consent have been met.

In some cases, consent may be questioned when:

- there is a risk that data subjects may withdraw their consent at any time, where processing is based on consent solely. Therefore, controllers must rely on consent in cases where no other lawful bases are applicable or when so required by another applicable law (e.g., consent to the use of e-mail for direct marketing is defined by the Law on Electronic Communications);[35]

35 Article 92 paragraph 1, Law No. 04/L-109 on Electronic Communications.

- there is an imbalance of power in the relationship between the data subject and the controller (e.g., an employment relationship), consent may not be valid as it may not be considered as freely given;
- consent is conditioned with the provision of another service. **For example**, a medical clinic requires the patient's consent to process his/her personal data for the purposes of medical treatment. If the subject does not give his/her consent, he/she cannot receive the treatment. This type of consent is incompatible with the LPPD, because it was conditioned with the provision of a service. In this case, the valid lawful basis for processing personal data is not consent, but **legal obligation** under which a physician is required to process the patient's personal data for treatment purposes;
- consent is given in a generic form. Specific consent is required for any processing purpose that based on this lawful basis. Consent should be specific, which means that the processing purpose for which it is given should be sufficiently specified. Therefore, if consent is given in a generic (bundled) way it is not valid;
- processing of personal data is unlawful or in breach of other data protection principles such as the data minimization principle, then obtaining the data subjects' consent does not necessarily make the processing of personal data lawful.

With regard to children's consent, in Kosovo full capacity to act is acquired upon reaching the age of majority (18 years of age) and upon entering into marriage prior to this age (not earlier than 16 years of age).[36] If a child has not reached the age of capacity to act, then his/her will shall be expressed by his/her legal representative (parents, or guardian). Therefore, when it comes to consent by minors, their legal representatives, except in cases where information societies provide services directly to children, give consent to the processing of their personal data. In these cases, if the child is over 16 years old, he/she can give consent on its own. However, institutions or companies have a duty to check the age limit with reasonable measures and, where the child is below the age of sixteen years; make efforts to verify that consent is given by the parent or legal representative.[37]

36 Article 15, Law No. 2004/32 Family Law of Kosovo.
37 Article 7, Law No. 06/L-082 on Protection of Personal Data.

4.1.8.2. Contract

The LPPD provides that processing is lawful where it is **necessary** for the performance of a contract to which the data subject is a contracting party or in order to take steps at the request of the data subject prior to entering into a contract.[38] This means that the controller has a lawful basis for processing, if:

- has entered into a contract with the data subject and needs to process their data for the performance of the contract.
- has not still concluded a contract with the data subject, but the subject is requesting something as a first step from the controller. In order to do what the data subject is requesting, the controller needs to process his/her personal data. For example, if a person wants to be notified by a company about the provision of a service in the location where he/she lives, then the interested person must provide his/her address of residence in order for the company to verify the location. This applies even if no contract is concluded between them in the future.

Processing is **necessary** for the performance or execution of the contract. In these cases, the controller must be able to demonstrate that the subject matter of the contract reached with the data subject cannot be performed, without the specific processing of the personal data in question. **For example**: processing credit card information for payment purposes. When a data subject makes an online purchase, a controller processes their address in order to deliver the goods, therefore the processing of the address is necessary in this particular case. Another example in an employment situation includes the processing of salary information and bank statement details necessary for executing payrolls.

This means that data processing must be necessary, otherwise if a controller is able to conclude or perform a contract by processing less data or using data in a less intrusive way, then contract will not apply as a lawful basis for data processing. This lawful basis usually applies to processing data collected to execute an online sale (e.g., billing, delivery etc.).

38 *Ibid* Article 5, paragraph 1, subparagraph 1.

4.1.8.3. Legal obligation

Article 5, paragraph 1, subparagraph 3, of the LPPD provides that processing is considered lawful if it is necessary for compliance with a legal obligation to which the controller is subjected. According to this Article, where personal data processing is laid down by law and sub-legal acts, the content of such processing constitutes a **legal obligation** to which the controller is subjected and as such processing is considered lawful because there is an adequate legal basis. In other words, specific laws may require controllers to process relevant personal data. Controllers should be able to identify the obligation in question by reference to specific legal provisions or administrative instructions. It should also be noted that the processing of relevant data must be necessary.

For example: An employer needs to process personal data to comply with its legal obligation to disclose employee salary details to the Tax Administration of Kosovo, which through tax legislation requires that companies as controllers and/or processors retain records for a duration six years, therefore companies have a legal obligation to process data.

It is also important to note that if personal data is processed based on legal obligation,[39] the individual has no right to erasure, right to data portability, or right to object.

4.1.8.4. Legitimate interest

Article 5, paragraph 1, sub-paragraph 6 of the LPPD provides that the processing is considered lawful: "*if processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"

This lawful basis concerns the legitimate interests pursued by the controller or by a third party. In theory, it applies where a controller uses personal data in ways data subjects would expect. In general, legitimate interest applies where processing is not required by law, and where there is a minor risk that the processing may violate the privacy of the data subject, and the data subject would reasonably expect that his/her data will be used in that way.

Legitimate interests is different to the other lawful bases as they it is not centred on a particular purpose. **For example**, entering into a contract with the data subject, complying

39 *Ibid* Article 16, paragraph 3.2.

with a legal obligation, protecting a vital interest, or carrying out a public duty, it is not that the data subject has specifically consented to.

Legitimate interests are more flexible and may in principle apply to any type of processing for any reasonable purpose. If a controller chooses to rely on legitimate interests, it takes assumes additional responsibility for protecting the rights and interests of data subjects.

When it comes to this lawful basis, the controller should:

- identify the legitimate interest. They can the interests of the controller or a third party. They may involve commercial interests, individual interests, or wider societal benefits,
- demonstrate that the processing is necessary to achieve the specified purpose, and
- balance it against the interests, rights, and freedoms of the data subject. If subjects would not reasonably expect the processing, or it would cause them unwarranted harm, their interests are likely to override the legitimate interests of the controller.

As noted above, where legitimate interest is used as the lawful basis for processing, the organization should perform a balancing test, namely: is this processing activity **necessary** for the organization to operate? Do the interests of the data subject override the legitimate interest? If the answer to any of these questions is "no", then the institution or company cannot use legitimate interest as its lawful basis for processing.

Processing is necessary for the purposes of the legitimate interests pursued by the controller or third party, except where there is a compelling reason to protect the individual's personal data which overrides those legitimate interests, in particular when the data subject is a child.

According to the GDPR, the processing of customer or employee personal data necessary for the purposes of fraud prevention, network and information security, reporting possible criminal acts or threats to public security and the transmission of relevant personal data to a competent authority constitutes a legitimate interest of the data controller concerned.[40]

For example, a public institution, public or private company is considering how to store job applications. The data in question can be stored for a set period as provided by the legislation and regulations on employment in the event of complaints by candidates on

40 Recital 47, GDPR.

grounds of discrimination. However, the organization decides to store the data for a longer period because it foresees scenarios where a candidate, who was found not suitable for the position he/she initially applied for, may be suitable for another position in the future. In this case, the public institution, public or private company has the right to retain or save personal data on legitimate interest for a specific period, but not indefinitely.

Such legitimate interests also arise where, for example, there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client of the controller. These situations could include customer-service provider relationships where the customer can reasonably expect their data to be processed.

Legitimate interest **does not apply to public authorities** that process personal data to carry out their tasks.

4.1.8.5. Vital interests

The processing of personal data is considered lawful where it is necessary to protect the vital interests of the data subject or of another natural person. The processing of personal data based on the vital interest of another natural person should take place in principle only where the processing cannot be manifestly based on another legal basis.

Furthermore, some types of processing may serve both grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

For example, if a serious accident occurs and the victim is admitted to a hospital with life-threatening injuries and incapable of giving consent to the processing. The hospital will want to find out more about the victim's medical history, such as allergies that can be provoked by specific medicines, in order to protect the victim's life, therefore, the applicable lawful basis for the controller is that processing is necessary to protect the vital interests of the data subject.

However, it should be noted that if the victim is capable of giving consent, then the controller cannot rely on vital interests for health data or other special category data, even if he/she refuses consent.

4.1.8.6. Public interest or exercise of official authority

The LPPD, respectively Article 5, paragraph 1, subparagraph 5, defined the public interest as a basis for lawful processing:

"Personal data processing shall be lawful if processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller", (e.g., VAT obligations and other taxes). This lawful basis can be relied on when personal data are processed for the purpose of exercising official authority, which means that they are processed only by public, central and local level institutions. Exceptionally, it can also apply to any institution that exercises an official or public function. The task performed in the public interest must have a basis in legal provisions. The processing must be deemed absolutely necessary or indispensable. If the task can reasonably be performed in a way that is less intrusive to the rights of the data subject, this lawful basis does not apply. Again, it is important that any decision to rely on this basis is fully documented, in order to help demonstrate compliance with the LPPD.

For example, data may be processed by government institutions and law enforcement authorities if this activity is intented to protect the public interest. For example, in the course of law enforcement there may be a need to access data in order to prevent criminal activity, or processing in the public interest may include processing personal data for scientific or historical research or compiling statistics.

5. Contracts between controllers and processors

Any personal data processing carried out by a processor on behalf of a controller should be governed by a **contract** concluded between the controller and the processor.[41] The contract normally sets out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data involved and the categories of data subjects, as well as the rights and obligations of the controller and the processor. The contract is important so that both parties understand their responsibilities and liabilities. The LPDP sets out the elements that need to be specified in a data processing contract.

According to the LPPD, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Law and ensure the protection of

41 Article 27, Law No. 06/L-082 on Protection of Personal Data.

the rights of the data subject.

The contract should also contain special terms or clauses related to:

- processing only on the controller's documented instructions;
- duty of confidentiality on part of the processor and persons authorized for such processing;
- adequate security measures;
- engagement of sub-processors;
- data subjects' rights;
- assisting the controller with adequate technical and organizational measures;
- end-of-contract provisions, what happens to personal data at the end of contract;
- auditing and inspection.

The processor may hire/engage another processor (sub-processor) to process personal data for a controller, with a contract in place between the parties. The contract should set out the same terms as stated above. However, it should be noted that, in order to conclude a contract with a sub-processor, the processor would need prior written authorization from the controller.

For example: A supermarket (controller) has a large number of employees and has decided to sign a contract with a company that provides accounting services (processor), which will calculate the employees' salaries. The supermarket determines dates of payroll disbursement, informs the accounting company when a new employment contract is concluded or a contract terminates, when an employee is to receive a raise or incentive, and provides the accounting company with all necessary personal data of employees for the purpose of payroll and its execution. The accounting company stores employee data (only those necessary for fulfilling the contractual obligation) in its databases and has taken all appropriate technical and organizational measures to protect personal data. The processor must guarantee to the controller the protection and confidentiality of the processing of personal data.

6. The role of the data protection officer

The LPPD, respectively chapter X, defines the method of designation, the role and tasks of the personal data protection officer. The personal data protection officer is tasked with informing and advising the controller and/or processor and the employees with respect to their obligations to protect personal data, and cooperate with the IPA (as a focal point for IPA) for all issues related to the processing of personal data.

According to the LPPD, his/her designation by the controller and/or processor is mandatory in cases where:

- the processing is conducted by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;
- the core activities of the controller or processor of processing on a large scale of special categories of personal data.

Designation of a personal data protection officer is not incumbent on the size of an institution or of a company. The data protection officer can be appointed on a voluntary basis even where it is not mandatory, but the same requirements of the position and tasks apply had the appointment been mandatory. He/she may be a staff member of the controller or processor, or an external associate who will fulfil the tasks based on a service contract.

Upon designation, the institution or company shall publish the contact details of the data protection officer and communicate them to the IPA. The obligation to publish contact details does not necessarily require to include the data protection officer's name, email and official contact number are sufficient.

The personal data protection officer is bound by secrecy or confidentiality concerning the performance of his or her tasks. He/she may perform other tasks and duties. Controllers or processors ensure that any other such tasks and duties do not result in a conflict of interest.

In any case, it is necessary that the data protection officers be sufficiently resourced to be able to perform their tasks in a qualitative manner (financial support, time, human resources, professional development, etc.).

Personal data protection officer must be independent and, in this sense, cannot receive instructions for performance of his/her duties, cannot be dismissed or penalized for performing his/her tasks, and reports to the higher management level.

The personal data protection officer should be familiar with the law and regulations for the protection of personal data, and the personal data processing processes in the institution or company.

7. Conclusion

Keeping records of personal data processing activities, aside from being an obligation provided by Article 29 of the LPPD, is also an internal control tool and a way to demonstrate compliance of the controller and/or processor with the LPPD.

Keeping the high-quality records of processing activities demonstrate that the public institution (the public and private companies) in addition to complying with the LPPD, have considered the processing of personal data as some form of auditing of the activities that it carries out, establishing by this the control over all processes related to personal data, which eventually reduces the risk of personal data breaches.

According to the LPPD, data controllers are not obliged to submit the aforementioned processed personal data to the IPA, but they keep records of processing activities in written form, including electronic form, and are obliged to make them available at the request of the oversight authority (IPA).

It is recommended to keep records in processing activities even if you are not required to keep them pursuant to the LPPD, because records of processing activities are one of the documents with which you can prove compliance with the LPPD.

Keeping a record of processing activities is not a one-off exercise, rather the information you document should reflect the current situation as regards the processing of personal data. Thus, you should treat the record as a living document that you update as and when necessary. This means you should make regular reviews of the information you process to ensure that your documentation remains accurate and up to date.

Annex I
Record of processing activities for controllers

Controller					
Name and contact Information		Personal Data Protection Officer (where applicable)		Representative (where applicable)	
Name		Name		Name	
Last Name		Last Name		Last Name	
Email		Email		Email	
Phone		Phone		Phone	

Article 29 Processing activity records										
Business Activity	Purpose of Processing Operation	Name and contact Information of joint controller (where applicable)	Categories of data subjects	Personal data categories	Special categories of personal data	Categories of recipients	Link to Processing Agreeement	Name of a third country or an international organization to which the personal data is transferred (where applicable)	Security measures for exceptional transfers of personal data to third countries or international organizations (where possible)	Retention period (where possible)

Personal Data Protection Policy							Personal data breaches		
A general description of technical and organizational security measures (where possible)	Article 5 Legal basis of personal data processing	Article 8 Conditions of Processing of special categories of personal data	Legitimate Interest of processing (if applicable)	Link to registration of assessment of legitimate interests (if applicable)	Data subject rights	Existence of automated decision-making, including profiling (if applicable)	Source of personal data (if applicable)	Has a personal data breach occurred?	Link to personal data breach registration

Annex II
Record of processing activities for processors

Processor					
Name and contact Information		Personal Data Protection Officer (where applicable)		Representative (where applicable)	
Name		Name		Name	
Last Name		Last Name		Last Name	
Email		Email		Email	
Phone		Phone		Phone	

Article 29 Processing activity records						
Link to Processing Agreement	Name and contact Information of controller	Name and contact Information of controllers' representative (where applicable)	Categories of processing	Name of a third country or an international organization to which the personal data is transferred (where applicable)	Security measures for exceptional transfers of personal data to third countries or international organizations (where possible)	A general description of technical and organizational security measures (where possible)