Manual on the Protection of Personal Data

Table of content

About the manual

The protection of personal data has a special importance that is not only about protecting and preventing the misuse of personal data. This field is very complex and using the appropriate legal infrastructure, it enables the preservation of personal integrity, the protection of citizens' rights and increases trust in electronic interactions, interactions that are expressed in the contemporary period.

Technological advancement continuously affects that many processes and further development, thus causing many actors to be challenged on a daily basis with dilemmas and opportunities regarding the processing of personal data. All of these are constantly faced with the effort to catch up in the direction of the harmonization and adaptation of the internal rules and local legislation with the best standards.

This manual contains useful and practical information to help understand the main definitions regarding personal data, how these data are processed, subjects, their rights and limitations and the protection mechanisms that citizens have available to protect their personal data. All of these are expressly defined by Law NR.06/L-082 on the Protection of Personal Data, which entered into force in February 2019.

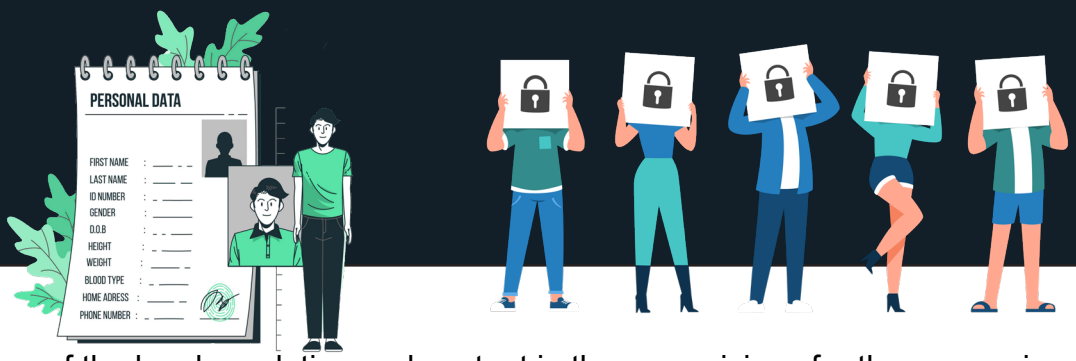
KLI has designed this manual so that it can be easily used by both professionals and lay citizens. The primary aim of the manual is to find use by all actors who process personal data, providing a practical approach to the basic concepts, applicable processes and providing the necessary basis of understanding the protection of personal data. In this way, it is easier to understand the main concepts and to apply the positive legislation related to personal data as easily as possible in practice.

In addition, this manual will serve to raise the awareness of all citizens of the country in relation to the rights and restrictions they have in relation to the protection of personal data and the legal avenues or legal remedies available to them.

1. Definition and importance of personal data

With Law no. 06/L-082 on the Protection of Personal Data, in article 3, par. 1. it expressly determines that any information related to an identified or identifiable natural person is personal data. Whereas, it also stipulates that an identifiable natural person is one who can be identified directly or indirectly, particularly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
The types of personal data may be different, but the main ones defined in the law are: genetic data, biometric data, health data and sensitive personal data.[1]
However, this data covers not only information that directly identifies a person "data subject", but also any element that indirectly identifies the latter.[2]

In the case, Benedik v. Slovenia, the European Court of Human Rights [hereafter: ECtHR] provided an in-depth discussion on the relationship between unique dynamic IP addresses and the notion of privacy. In this aspect, the Court could not ignore the context in which the information was requested in the present case, given that the only purpose of the police for revealing IP addresses was to identify a user. In this situation, these IP addresses were considered as personal data. Despite the fact that this was not identity data, it was identification data. The action of the police to disclose data related to a user of a relevant IP address, without a court order, was in violation of Article 8 (Right to Privacy) of the European Convention on Human Rights [hereinafter: ECHR].[3]
In this way, the name, surname or personal number can be considered as identification data. While, as identifiable data, any data that enables the identification of a person can be used, such as the place of work, physical characteristics, place of residence, education, etc.



The importance of the legal regulation and content in these provisions for the processing of personal data is extremely great. Thus, data protection is not only related to the security of these data, but also the way of processing and securing these data by different actors, in particular in relation to the protection of citizens' rights, ensuring their personal integrity and awareness and increased trust in electronic interactions, based on the technological advances of the time.
On the other hand, a personal data breach consists of *any breach of security measures that results in the destruction, loss, alteration, unauthorized, accidental or unlawful disclosure, or access to personal data transmitted, stored or otherwise processed.*[4]

2. Parties involved in the processing and protection of personal data

The process of processing personal data, according to the law, foresees and includes several different actors, when for each there is also a definition and certain role.

2.1. Data Subject

In the field of personal data processing, the central party is the person to whom the personal data belong. The law names this person as “data subject”.
On the other hand, parties involved in this process are the controllers, processors and recipients of personal data.

2.2. Data Controller

The data controller is *any natural or legal person from the public or private sector that individually or jointly with others determines the purposes and methods of personal data processing.*[5] Depending on the circumstances, the controller must always be careful and implement appropriate technical and organizational measures, as a form of guarantee that data processing is carried out in accordance with the law on personal data protection. Even the controller makes sure that the technical and organizational measures they undertake are reviewed and updated as necessary.[6]

2.3. Data Processor

The data processor is *any natural or legal person, from the public or private sector, who processes personal data for and on behalf of the data controller.*[7]

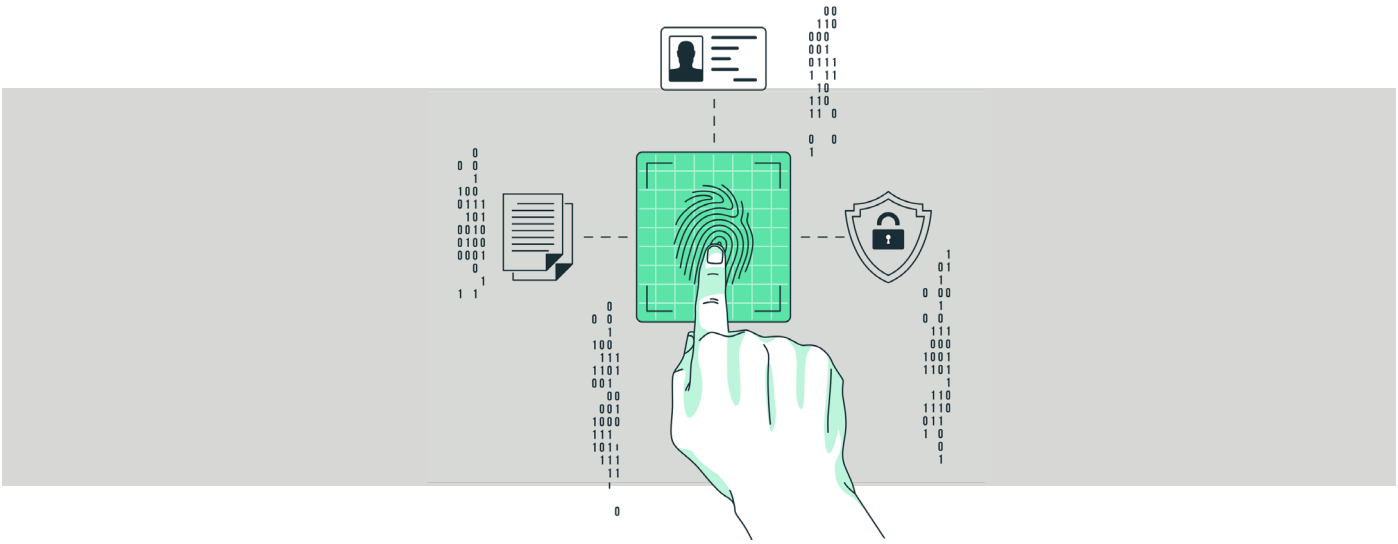
2.4. Data Recipient and Third Party

The data recipient is *any natural or legal person from the public or private sector, to whom personal data is disclosed, whether a third party or not.* Therefore, a data recipient can be a data controller or data processor.[8]
Whereas, the third party is any natural or legal person from the public or private sector that is different from the data subject, the controller, the processor and the persons who, according to the direct authorizations of the controller or processor, are authorized to process personal data.[9] Public authorities that may receive personal data in the context of a special investigation, in accordance with the legislation in force, are not considered recipients.

Hypothetical example:

An online store “Company A” conducts business through the sale of clothing and accessories. This company, when establishing the rules for the sale of products, has decided that the sale of products in the market will be done by “Company B”, while the transport will be done by “Company C”. In order to carry out this process, “Company A” has determined that personal data should be obtained from customers, during the ordering process, such as names, addresses, electronic addresses and payment information, in which case it determines the purposes and means of processing such data, including order fulfillment, customer support and marketing communications. Until now, “Company A” has acted as the controller of personal data.
When selling products, according to the instructions of “Company A”, “Company B” collects personal data from customers. In this case, “Company B” acts as a personal data processor, according to the instructions given by “Company B” as a personal data controller. Company B shares customer data with Company C, including shipping addresses and contact information, to carry out the delivery process.
In this case, Company C acts as the recipient of the personal data.

Thus, Company A, as the data controller, is responsible for the protection of personal data. It must obtain the client’s consent, when necessary, to provide transparent privacy policies and to implement appropriate security measures for data protection. It also has the obligation to respond to customer requests regarding their data, such as access, correction or deletion. Whereas, Company B, as a data processor, has the responsibility to process the data strictly based on the instructions of Company A. Whereas, “Company C”, which did not receive personal data from customers, but accepted them from “Company B” acts as the recipient of personal data, in which case it must provide security and confidentiality regarding the data during the delivery process.
If this entire process was carried out only by “Company A”, then it is considered that this company is both a controller and a processor of personal data.



In case of appointing a processor, the controller takes care to engage only processors who guarantee the implementation of appropriate technical and organizational measures, in order to fulfill the processing requirements, but also at the same time guarantee the protection of the data subject’s rights. On the other hand, the processor cannot engage another processor without specific or general prior written authorization from the controller.[10]

3. How is personal data processed?

In order to determine if an action is considered as processing of personal data, the law clearly foresees that any action or series of actions that are performed on personal data by automatic means or not, such as: collection, registration, organization, structuring, storage, adaptation or alteration, withdrawal, consultation, use, publication by transmission, distribution or provision, amalgamation or combination, restriction, erasure or disposal, is known as processing of personal data.[11]

3.1. Principles of personal data processing

The law of Kosovo on the protection of personal data is built on the basis of several main principles, which create the basis of the processing of personal data, as a key form of proper protection of personal data.
A proper and legal processing of personal data can only be done on the basis of the main princi-

1. The principle of legality, justice and transparency - personal data are processed in an impartial, legal and transparent manner, without violating the dignity of data subjects.

Data processing is considered lawful only if at least one of the following criteria is met:

- giving consent for the processing of personal data by the data subject;
- the necessity of processing personal data for the purpose of fulfilling a contract to which the data subject is a party;
- the necessity of data processing due to any legal obligation;
- the necessity of processing personal data due to the protection of the vital interests of the data subject or other natural persons;
- the necessity of processing personal data for the performance of a task of public interest or the exercise of official authority by the controller;
- the necessity of processing personal data for the purpose of the legitimate interests of the controller or a third party, unless these interests are exceeded by the interests or fundamental freedoms and rights of the subject who requires the protection of personal data, especially if the data subject is a child.[12]

In a number of cases, the ECtHR has found violations of personal data [Article 8 of the ECHR], only due to the lack of a legal basis for the processing of personal data in a fair and legal manner.[13]

In the case of M.D. and others v. Spain, the police drew up a report concerning the judges, who exercised their functions in Catalonia and had signed a document, setting out their legal opinion in favor of the possibility of the Catalan people in exercising the so-called "the right to decide". In this report, the personal data, photographs, professional information and political views of some of them were revealed. The court decided that the right to compile a report by the police was not provided for by law and at the same time it was used by public authorities for a purpose other than the one that justified the collection of personal data. In addition, the Court emphasized that the mere existence of the police report, which was drawn up in relation to individuals whose behavior did not imply any criminal activity, constituted a violation of Article 8 of the ECHR.[14]

2. Principle of purpose limitation – personal data is collected only for specific, clear and legitimate purposes and may not be further processed contrary to these purposes. Further processing for the purpose of archiving in the public interest, for the purpose of scientific or historical research, or for statistical purposes, is not considered inconsistent with the original purpose.

The controller must clearly define which data should be processed and for which purposes they should be processed. In this case, after the processing of personal data, the same cannot be used for other reasons, apart from those previously defined, for which the personal data were processed. The ECHR emphasizes that it is important to limit the use of data to the purpose for which they were recorded.[15]

In the case of Surikov v. Ukraine, the long-term retention of data relating to the party's mental health, together with its dissemination and use for purposes unrelated to the reasons that originally justified the collection, constituted a disproportionate interference with the right to data subject to respect his private life. Given the findings, the Court concludes that there has been a violation of Article 8 of the Convention, in relation to the retention, disclosure and use of the party's mental health data, to decide on the party's application for promotion.[16]

3. The principle of data minimization – personal data must be adequate, relevant and must not exceed the purposes for which they were collected or further processed

Through this principle, the Law determines that when a goal is determined, the achievement of which requires the processing of personal data, only the personal data that are necessary should be obtained. For example, in the case of online sales, the buyer's first and last name, residential address and contact number may be processed. However, their place of work cannot be requested, as this data is not in accordance with the goal that is intended to be achieved, namely the sale of the product. On the other hand, after achieving the goal, in our case the sale of the product, the personal data is not allowed to be used for other purposes. For example, the company that sells products online is not authorized to use customer contacts for marketing. In this regard, protective measures should be taken to maintain anonymity in order not to disclose identifying information. The ECtHR, in the case of Vincent Del Campo v. Spain, found a violation of this principle, after noting that a court decision identified a person not relevant to the process. In such a situation, the Court would have to adopt safeguards to maintain anonymity or remove identifying information in defense of his rights and freedoms, to avoid stigmatization. This could have been achieved by referring to this third person simply by his initials. Therefore, the ECtHR assessed that in this particular case there was a violation of personal data.[17]

4.Principle of accuracy – personal data must be accurate and up-to-date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purpose of the processing, is deleted and rectified without delay.

The ECtHR has had a high number of cases related to the retention of data-by-data authorities, which turned out to be inaccurate or their accuracy was contested by the data subject.[18] In the Rotaru v. Romania case, personal information about the party's life, in particular studies, political activities and criminal record, collected and kept for over 50 years by the state authorities turned out to be inaccurate and defamatory, thus damaging the party's reputation. As a result, the Court concluded that there had been a violation of Article 6 par. 1, 8 and 13 of the ECHR.[19]

5. The principle of storage limitation – personal data may be stored only for as long as is necessary to achieve the purpose for which it was collected or further processed. Upon fulfillment of the purpose of processing, personal data is destroyed, deleted, destroyed, blocked or made anonymous, unless otherwise provided by the relevant Law on State Archives or by any other relevant law.

The issue of the need to limit the duration of personal data storage has been examined by the ECtHR.[20] In the case of S. and Marper v. United Kingdom, the ECtHR found that there is a violation of Article 8 of the Convention in cases of permanent storage (in a national database) of fingerprints and DNA profiles of suspected persons, but not convicted of criminal offences, regardless of the nature of the offense and the age of the suspect. Moreover, the Court assessed that this record keeping is particularly harmful in the case of minors, as was the party in this case, due to their special situation and the importance of their development and integration in society.[21]

6. The principle of inviolability and confidentiality – personal data are processed in a way that guarantees their adequate security, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, using appropriate technical and organizational measures.

In Case Z v. Finland, the Court had to ascertain whether there were sufficient grounds to justify the disclosure of the applicant's identity and HIV status through press coverage of the decision of the Helsinki Court of Appeal. Under the relevant provisions of Finnish law, the Court of Appeal had the power not to disclose in its judgment any name by which the applicant could be identified and to order that the full statement remain confidential for a certain period and instead to a shorter version of the rationale is published. Moreover, it was under these conditions that the Helsinki court published its decision. Therefore, the publication of this information violated the party's right to respect for private and family life guaranteed by Article 8 of the ECHR.[22]

7. The principle of accountability – the controller must be responsible and able to enforce compliance with all the principles set forth in this article.[23]

This principle is also manifested in relation to the sanctions that can be imposed for the illegal control of personal data, which will be discussed in the fifth chapter of this manual.

3.2. Responsible officer

Another important step in the personal data processing process, but also in the general system for the protection of personal data, is directly related to the appointment of the data protection officer. According to the law, the same is appointed based on its own professional skills and especially on the basis of expertise for the protection of personal data, on its own practice and abilities to fulfill this task.[24]

This official can be appointed from among the personnel of the controller or processor, or the same person fulfills the duties on the basis of a service contract. Whatever the way of engagement of the data protection official, the controller or processor is obliged to publish the official's contacts and communicate them to the IPA.[25]

The data protection officer has the duty to inform and advise the controller or processor and the employees, on their obligations in relation to the law and by-laws on data protection. It cooperates with the Information and Privacy Agency and acts as a point of contact with this agency, provides advice on data protection impact assessment and monitors performance, and also consults on any other matter.[26]

4. Rights and limitations

In addition to all the above-mentioned principles and defined procedures, a number of rights are also provided for the data subject. These and other rights defined by the law and other by-laws in force, in addition to guaranteeing security for the data subject, also enable a fair and legal processing of personal data. But in addition to these, for certain purposes, the law has expressly defined the possibilities of their limitations.

4.1. Rights of the subject of personal data

A primary right in this regard is transparent information for the data subject, for which the controller is obliged to take the necessary measures so that the processing of personal data is done in a concise, transparent, understandable and easily accessible format, use clear and clean language, especially for any information directed specifically at a child. The information is provided in writing or by other means, including, where appropriate, electronic means.[27]

Very important for the data subject is especially the right of rectification. In any case, the data subject has the right to have inaccurate personal data corrected without undue delay. Likewise, the data subject has the right to complete personal data, depending on the purpose of the processing. This is also done through an additional declaration.[30]

Likewise, the data subject has the right to access personal data and relevant information, receiving confirmation from the controller whether or not the data related to them is being processed.[28] Whereas, the controller has the obligation to provide the data subject with a copy of the personal data that is subject to processing.[29]

On the other hand, the data subject also has the right to delete his personal data. This right is known as the right to be forgotten. The right to be forgotten includes the right of the data subject to request the controller to delete personal data related to him, in case certain reasons are met, among which the law defines as follows:

- personal data are no longer necessary in relation to the purposes for which they were collected or processed

- the data subject withdraws the consent on which the processing is based and if there is no other legal reason for the processing,

- the data subject opposes the processing in accordance with the law and there are no legitimate reasons for the processing,

- personal data has been processed illegally,

- personal data must be deleted to fulfill a legal obligation to which the controller is subject,

- personal data are collected in connection with the offer of information society services.[31]

Hypothetical example:

1

A media outlet has reported on a court case involving a beating that resulted in light bodily injury. The report in this case was made 3 years ago, when the defendant was found guilty and sentenced to a fine. In this case, the defendant has the right to request from the media that the report in question be deleted or anonymized, due to the fact that a considerable amount of time has passed since that time, the criminal offense for which he was found guilty was not dangerous high and now the public has no interest in this case.

2

A media has reported on a corruption scandal involving some powerful politicians and businessmen. For this case, the media had reported that the same were found guilty by the court and were punished according to the law. This report was made 1 year ago. In this case, the media has the right to reject the request for deletion of this report, based on the fact that the time elapsed since the announcement of the judgment is relatively short, the criminal offenses for which the defendants have been convicted have significant social danger and the public continues to be interested in a scandal of this level.

In line with the rights of the data subject, the right to limit processing and the right to data transfer are also recognized. This first allows that in cases where the processing is limited, these personal data, with the exception of storage, are processed only with the consent of the data subject for the establishment, exercise or defense of legal claims or for the protection of the rights of a person other physical or legal, or for reasons of important public interest.[32] Whereas, in case of exercising the right to data transfer, the data subject has the right to transfer personal data from one controller to another controller. This is done in any case where something like this is technically feasible.[33]

4.2. Limitation of data subject rights

In certain circumstances, legally there are also some possibilities of limiting the rights of the data subject. This has been determined to occur only when such restriction respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure to ensure state and public security and protection, prevention, investigation, detection or prosecution of criminal offences or ethical violations for certain professions, then for the execution of criminal sanctions, the protection of judicial independence and judicial proceedings, the protection of the data subject or the rights and freedoms of others, the execution of claims under civil law, but also other important objectives of the general public interest of the Republic of Kosovo.[34] It should be noted that the restriction in the mentioned cases can only occur as far as is necessary to achieve the purpose for which the restriction is given.[35]

5. Measures and tools for the protection of personal data

5.1. Defense mechanisms

One of the ways to ensure the performance of duties and respect for the rights of the subject of rights is the obligation of the controller and data processor to issue internal acts, through which they must describe the procedures and measures established for the security of personal data and must appoint, in writing, the competent persons who are responsible for implementing the rules according to this law.[36] In addition, the law also stipulates that the agency encourages the drafting of codes of conduct that aim to contribute to the proper implementation of this law, taking into account the specific characteristics of the various processing sectors.[37]

In any case, the party that claims the violation of its personal data and the rights defined by the Law on Protection of Personal Data, has the opportunity to address the Information and Privacy Agency. Thus, every data subject has the right to appeal to the Agency, without prejudice to other

administrative or judicial means. Whereas, the Agency, on the other hand, must keep the complainant informed about the progress and outcome of his complaint.[38]
A data subject who claims the violation of his rights has the right to engage a representative (natural person, body, organization or non-profit association) to exercise his rights in terms of personal data protection, file a complaint on his/her own behalf, go to court or even exercise the right to receive the compensation defined by law.

This authorization must be given in writing and certified by a notary.[39]
Thus, whether directly or through a representative, the data subject has the right to legal remedies both against the Agency and against the controller or processor.
This means that if the Agency, based on its powers, does not handle a complaint, or does not notify the subject within three months regarding the progress or outcome of the complaint, then the data subject has the right to an effective judicial remedy.

At the same time, even with the final decision of the Commissioner of the Agency, the data subject, if he is dissatisfied, has the right to initiate an administrative conflict in court.[40]

In addition to the right to complain to the Agency, a data subject can initiate legal proceedings even when he thinks that his rights have been violated as a result of the processing of his personal data by a processor or controller.[41]

5.2. Compensation

Any person who suffers material or non-material damage due to violations of the law on the protection of personal data, has the right to receive compensation from the controller or processor for the damage suffered. In order to exercise this right, a claim for compensation must be submitted to the court.[42]

5.3. Sanctions

In addition to direct compensation for the data subject, as a person who has suffered direct damage (material or non-material), controllers or data processors may also be obliged to make other payments. These are fines that are imposed by the Agency in case of violations of the provisions of the law during the processing of personal data. The value of the direct violation fine is determined by the Information and Privacy Agency, after taking into account the legal criteria related to the violation committed by the processor or controller, the type of violations and the fact that they are imposed on the legal entity, the responsible person of the legal entity, the responsible person of the body state or individual.[43]

Violations that are defined by law start from the general ones, and being specified in violation of the provisions for contractual processing, for the security of personal data, for direct marketing, for camera surveillance (in official and business buildings, in apartment buildings , in work spaces, etc.), for biometric characteristics (either in the public or private sector), in the registration of entrances/exits from the building, in the interconnection of file systems, in the supervision by the person responsible for the protection of personal data, or other serious and large-scale violations.[44]

The law has determined that the value of the fines that can be imposed for various violations against the legal entity can vary from 4 thousand to 40 thousand euros. For the responsible person of the legal entity, it varies from 200 euros to 4 thousand euros. For the responsible person of the state body, from 200 euros to 8 thousand euros. However, for the individual, it starts from 200 euros and can go up to 2 thousand euros.[45]

Whereas, the imposition of fines or punitive provisions that are determined by the law on the protection of personal data, it should be known that it does not exclude other responsibilities based on the legal provisions in force, in particular the responsibility of data controllers and processors for damages resulting from processing illegal and criminal liability as defined in the Criminal Code of the Republic of Kosovo.[46]

6. Information and Privacy Agency

IPA is a state agency that functions as an independent authority and is responsible for supervising the implementation of the Law on the Protection of Personal Data and other by-laws regarding the protection of personal data and access to documents and public information.[47]



IPA– bases its duties and powers on the Law on Access to Public Documents and the Law on Protection of Personal Data. Whereas, for the purposes of this guide, in the following, only the tasks that are defined in relation to the Law on the Protection of Personal Data will be elaborated in more detail, where:

-supervision of the implementation

-providing advice to public and private bodies regarding data protection;

-informing the public about issues and developments in the field of data protection;

-promotion and protection of fundamental rights for the protection of personal data;

-deciding on the complaints of data subjects;

-providing advice to the Parliament, the Government, institutions and other state bodies regarding legislative and administrative measures related to the protection of personal data;

-inspection related to the implementation of the law;

-periodic review of certifications for work related to personal data, as well as withdrawal of certification in case the criteria are not met;

-providing opinions for public institutions and other bodies.[48]

In addition to the aforementioned duties, depending on the circumstances and the situation that may arise, IPA may also have additional duties and powers.

7. Annex with the forms of submissions for the protection of personal data

For the purpose of the most practical approach, KLI has drawn up and attached five forms of submissions which may be necessary during the procedure of protecting the rights of the data subject according to the law on the protection of personal data.

7.1. Authorization form for representation in personal data protection procedures

In accordance with Article 55 of the Law on the Protection of Personal Data and with the free will of _____ *(name and surname of the authorizing person)* is given:

AUTHORISATION

_____ (*name and surname of the authorizing person)* authorizes _____ *(the name and surname of the natural person who authorizes it/ the name of the organization or legal entity that authorizes it),* from _____ *(place, address),* to be represented in all procedures related to the protection of personal data.
Pursuant to Article 55 of the Law on the Protection of Personal Data, the authorized person has the right to exercise legal remedies on behalf of the authorizer at all stages of the procedure, as well as to exercise the right to receive compensation on behalf of the authorizer, in in accordance with Article 56 of the Law on Personal Data Protection.

The authorization is valid until the end of the case and cannot be used for other matters.

_____,
(place where the authorization is issued)

_____
(date of authorization issues)

Authorizer,
_____
(name and surname)

(signature)

7.2. Complaint form for violation of personal data

INFORMATION AND PRIVACY AGENCY

The applicant of the complaint: _____ *(name and surname),*
_____ *(full address)*

Against: _____ *(name and surname/designation of the personal data processor/controller)*

In accordance with Article 52 of the Law on the Protection of Personal Data, the complainant presents this:

COMPLAINT

Due to violation of provisions _____ *(the type of violation defined in articles 92 - 105 of the Law on Protection of Personal Data)*

Reasoning

(It shows the course of the case and how the violation was committed and by whom this violation was committed, also providing evidence regarding this violation).
Therefore, based on all that was said above, the complainant requests the Information and Privacy Agency, after reviewing all the facts, evidence and, if necessary, the field inspection, to render the following:

DECISION

I. APPROVED in its entirety the complaint from _____ *(name and surname of the complainant)*, from _____ *(place)* with address at _____ *(full address)*.
II. ORDERS _____ *(name and surname/designation of the processor/controller of personal data)* to stop the processing of personal data through _____ _____ *(the manner in which the data is being processed, i.e. the violation of rights related to personal data).*
III. ORDERS _____ *(name and surname/designation of personal data processor/controller)* to destroy all personal data collected through _____ *(the manner in which the data is being processed, i.e. the violation of rights related to personal data).*

_____,
(place where the authorization is issued)

Palintiff,
_____
(name and surname)

_____
(date of authorization issues)

(signature)

7.3 Data deletion request form (right to be forgotten)

_____ *(the name of the institution/body you are addressing)*

In accordance with the Article 16 of the Law on Protection of Personal Data, the com-

REQUEST

For the deletion of personal data, respectively _____ *(personal data that is requested to be deleted)* which are contained in _____*(where the data requested to be deleted are located or published):*

Reasoning

(The information in question is shown, then the conditions that are met in the specific case are elaborated, which are:
- *personal data are no longer necessary in relation to the purposes for which they were collected or processed,*
- *- the data subject withdraws the consent on which the processing is based and if there is no other legal reason for the processing,*
- *- the data subject opposes the processing in accordance with the law and there are no legitimate reasons for the processing,*
- *- personal data have been processed illegally,*
- *- personal data must be deleted to fulfill a legal obligation to which the controller is subject,*
- *- personal data are collected in connection with the offer of information society services.)*

Therefore, based on all that was said above, the complainant requests from _____, that after considering all the facts and evidence, renders the following:

DECISION

I. APPROVED in its entirety the complaint from _____*(name and surname of the complainant),* from_____ *(place)* with address at _____ *(full address).*
II. DELETED the data _____ *(personal data that is requested to be deleted)* which are found at_____ *(the country/registry/page where the personal data that is decided to be deleted is located).*

_____,
(place where the authorization is issued)

_____
(date of authorization issues)

Plaintiff,

_____
(name and surname)

(signature)

7.4. Complaint form against the decision of the Information and Privacy Agency for rejection of the complaint for violation of personal data

Basic Court in Pristina
Department for Administrative Issues

PLAINTIFF: _____ *(Name, Surname, address of plaintiff)*
RESPONDENT: _____ (*Name, Surname, address of respondent)*

In accordance with Article 13, par. 1 of the Law on Administrative Conflicts and Article 53, par. 3 of the Law on Protection of Personal Data, the plaintiff submits this:

LAWSUIT

For administrative conflict
Due to:

- _____ *(List of one or more reasons defined by Article 16 on the Law on Administrative Conflicts)*

(The case is illustrated and the decision rendered by IPA elaborate, which is being contested in this lawsuit.)
(Depending on the reasons which the IPA decision is being contested, treat and elaborate each reason for which the decision is being contested.) For this the facts and evidence that that prove these facts must be presented.

Therefore, based on all that was said above, the plaintiff asks the Court that, after considering all the facts and evidence, render the following:

DECISION

I. APPROVE in its entirety the claim of _____ *(name and surname of the plaintiff),* from _____ *(place)* with address _____ *(full address).*
II. ANNUL IPA decision no. _____, dated _____.
III. ORDERS _____ *(name and surname/designation of personal data processors/controllers) t*o stop the processing of personal data through _____ *(the manner in which the data is being processed, i.e. the violation of rights related to personal data).*
IV. ORDERS _____ *(name and surname/designation of personal data processor/controller) t*o destroy all personal data collected through _____ *(the manner in which the data is being processed, i.e. the violation of rights related to personal data).*

_____,
(place where the authorization is issued)

Plaintiff,

_____
(name and surname)

_____
(date of authorization issues)

(signature)

7.5. Claim form for compensation due to violation of personal data

Basic Court in_____
General Department –Civil Division

PLAINTIFF: _____ *(Name, Surname, address of plaintiff)*
RESPONDENT: _____ (*Name, Surname, address of respondent)*

In accordance with Article 56 of the Law on the Protection of Personal Data, the plaintiff submits this:

LAWSUIT

For compensation of damage due to violation of personal data

(Case to be illustrated and how the violation was committed and by whom this violation was committed, also providing evidence regarding this violation).

(The damage caused to the claimant/data subject is elaborated. For this, the facts and evidence that prove these facts are also presented. In addition to the material damage, which consists in the reduction of property, the respondent has the right to justify the need for compensation for non-material damage, which consists in causing physical pain, mental suffering, etc.).

Therefore, based on all that was said above, the plaintiff asks the Court that, after considering all

DECISION

I. APPROVE in its entirety the claim of _____ *(name and surname of the plaintiff)*, from _____ *(place)* with address _____ *(full address).*
II. OBLIGATES the respondent _____ *(name and surname/ designation of the respondent)* that within 15 days of the entry into force of this decision, to compensate the plaintiff the damage caused concerning the violation of personal data, and that:
a. _____ *(amount requested)* euro in the name of material damage;
b. _____*(amount requested)* euro in the name of non-material damage;
III. OBLIGATES the respondent to immediately compensate the plaintiff after the entry onto force of this decision.

_____,
(place where the authorization is issued)

Plaintiff,

_____
(name and surname)

_____
(date of authorization issues)

(signature)

8. References

Law no. 06/L-082 on the Protection of Personal Data, article 3, par. 1, subpar. 19, 20, 21 and 25.
2. (Benedik v. Slovenia, 2018, par. 107-108).
3. Law no. 06/L-082 on the Protection of Personal Data, article.
4. Ibid, subpar. 18.
5. Ibid, subpar. 11.
6. Ibid, Article 23, par. 1.
7. Ibid, Article 3, par. 1. subpar. 14.
8. Guidelines of the working group for transparency according to Regulation 2016/679, Article 29.
9. Law no. 06/L-082 on the Protection of Personal Data, subpar. 16.
10. Ibid, Article 27, par. 1 and 2.
11. Ibid, Article 3, par. 1.2.
12. Ibid, Article 5, par. 1
13. Taylor-Sabori v. United Kingdom, 2002, para. 17-19, ECtHR; Radu v. Moldova, 2014, para. 31; Mockutė v. Lithuania, 2018, para. 103-104; MD and others v. Spain, 2022, para. 61-64.
14. M.D. and others v. Spain, 2022, para. 61-64, ECtHR.
15. Karabeyoğlu v. Turkey, 2016, para.112-121, STATUS; K.H. and others v. Slovakia, 2009, para. 45-57; Peck v. United Kingdom, 2003, para. 59-62.
16. Surikov v. Ukraine, 2017, para. 83-95, ECtHR.
17. Vicent Del Campo v. Spain, 2018, para. 51, ECtHR.
18. Cemalettin Canlı v. Turkey, 2008, para. 34-37, ECtHR; Rotaru v. Romania, 2000, para. 36.
19. Rotaru v. Romania, 2000, para. 44, ECtHR.
20. S. and Marper v. United Kingdom, 2008, ECtHR; B.B. against France, 2009; Gardel v. France, 2009; M.B. against France, 2009; M.K. against France, 2013; J.P.D. against France, 2014; Peruzzo and Martens v Germany 2013; E. v. Netherlands, 2009; Brunet v. France, 2014).
21. S. and Marper v. United Kingdom, 2008, para. 125-126, ECtHR.
22. Case Z v. Finland, 1997, ECtHR.
23. Law no. 06/L-082 on the Protection of Personal Data, article 4
24. Ibid, Article 37, par. 5.
25. Ibid, Article 37, par. 6 and 7.
26. Ibid, Article 39, par. 1.
27. Ibid, Article 11.
28. Ibid, Article 14, par. 1.
29. Ibid, par. 3.
30. Ibid, Article 15.
31. Ibid, Article 16, par. 1.
32. Ibid, Article 17, par. 2.
33. Ibid, Article 19, par. 2.
34. Ibid, Article 22, par. 1.
35. Ibid, par. 2.
36. Ibid, Article 40, par. 2.
37. Ibid, Article 41, par. 1.
38. Ibid, Article 52, par. 1 and 2.
39. Ibid, Article 55, par. 1 and 2.
40. Ibid, Article 53, par. 1, 2 and 3.
41. Ibid, Article 54.
42. Ibid, Article 56.
43. Ibid, Article 91.
44. Ibid, Articles 92 – 105.
45. Ibid.
46. Ibid, Article 106.
47. Ibid, Article 57, par. 1.
48. Ibid, Article 64.

SUPPORTED BY: