FOL

Hypothetical personal data breach scenarios and relevant rights protection guidelines

Sweden
Sverige

HUMAN RIGHTS HOUSE

CDF

Hypothetical personal data breach scenarios and relevant rights protection guidelines

This document is part of the “Human Rightivism” project, conducted under the “Data Guardians: Strengthening Privacy Policies and Awareness in Public Institutions” initiative, led by Lëvizja FOL. The project is implemented by the Community Development Fund (CDF) with the support of the Embassy of Sweden in Pristina.

This document was created in collaboration with the Information and Privacy Agency.

YEAR OF PUBLICATION:
2024

PUBLISHED BY:
FOL Movement

WEBSITE:
www.levizjafol.org

ADDRESS:
Andrea Gropa no. 35 Prishtina 10000, Republic of Kosovo

Table of contents

Introduction

Privacy and protection of personal data are fundamental human rights that play an important role in everyday life, especially in an increasingly interconnected and digitized society. Breach of privacy and unauthorized processing of personal data are major concerns that affect all citizens, both in the public and private sectors.

The document "Personal Data Breach and Protection Scenarios," was drafted by FOL Movement within the framework of the Project "Data Guardians: Strengthening Privacy Policies and Awareness in Public Institutions", through Human Rightivism supported by the Embassy of Sweden in Kosovo through Community Development Fund - CDF. This document aims to provide a clear and comprehensive overview of everyday situations where privacy and personal data may be violated, as well as help citizens understand their legal rights and steps they can take to protect them. The law cited in this document is Law No. 06/L-082 on Protection of Personal Data.

Each scenario reflects real challenges that Kosovo citizens may face regarding privacy and processing of personal data, including legal obligations of relevant institutions and actions that citizens can take to ensure the protection of their rights.

This document was developed incorporating input from Focus Group meetings and suggestions from professionals in this field, with the aim of being a practical and educational guideline for all those seeking to better understand their personal data protection rights.

We believe that this material serves as a valuable resource for raising awareness and improving privacy protection practices in Kosovo.

SCENARIO 1:

Lack of confidentiality in sharing health diagnoses

The law requires that any information about your health be kept confidential and that no one has access to it without your consent!


Diagnoza

SCENARIO 1:

Lack of confidentiality in sharing health diagnoses

Arjeta, a 48-year-old woman, goes to a clinic in Prishtina for a routine check-up. While she waits in the hallway, a nurse begins to ask her personal questions about her medical history, including past surgeries and illnesses, in the presence of patients and other staff who are not directly serving/helping her.

These open questions make Arjeta feel exposed and uncomfortable, as sensitive details of her health are discussed publicly, with no respect for her privacy.

Also, later, when results came out, the document with her diagnosis was left on an open table for anyone nearby to access.

This scenario raises questions about the violation of privacy and respect for personal data within health care settings in Kosovo, where confidential information is often shared without due discretion.

What were the obligations of the respective institution in this particular case?

Legal basis: Law, Article 3, paragraph 1.25, Article 5, paragraph 1.1, Article 8, paragraph 2.1.

- **The institution should have the appropriate infrastructure that allows data protection:**

  The institution may determine the methods that are applicable to ensure that personal data are protected (special rooms for receiving data, specific forms, other forms determined by the controller itself, etc.), as long as these methods ensure data protection and compliance with the law.

- **Register of processing activities:** The institution must maintain a register of data processing activities, as defined by law.

  Legal basis: Law, Article 29.

- **Drafting of internal acts for processing:** The health institution in question must have internal acts in which aspects related to procedures and measures established for the security of personal data should be regulated.

  Legal basis Law, Article 40.

- Establishment of a data protection office and specialized/certified training of officials in compliance with Articles 37-40 and 43 of the Law.

What could Arjeta do in the described scenario?

Pursuant to the Law on Protection of Personal Data, Arjeta may take the following actions:

Request for access to personal data: Pursuant to **Article 14,** Arjeta has the right to request access to her personal data to find out who had access to it, and whether there has been unauthorized data processing.

Request for deletion of processed data without her consent: Pursuant to **Article 16,** if the document with her diagnosis has been made accessible to others without her consent, she has the right to request for deletion of the data.

Complaint to the Information and Privacy Agency: Pursuant to **Article 52,** Arjeta may file a complaint with the Agency to request an investigation into the breach of confidentiality and take measures to protect her personal data.

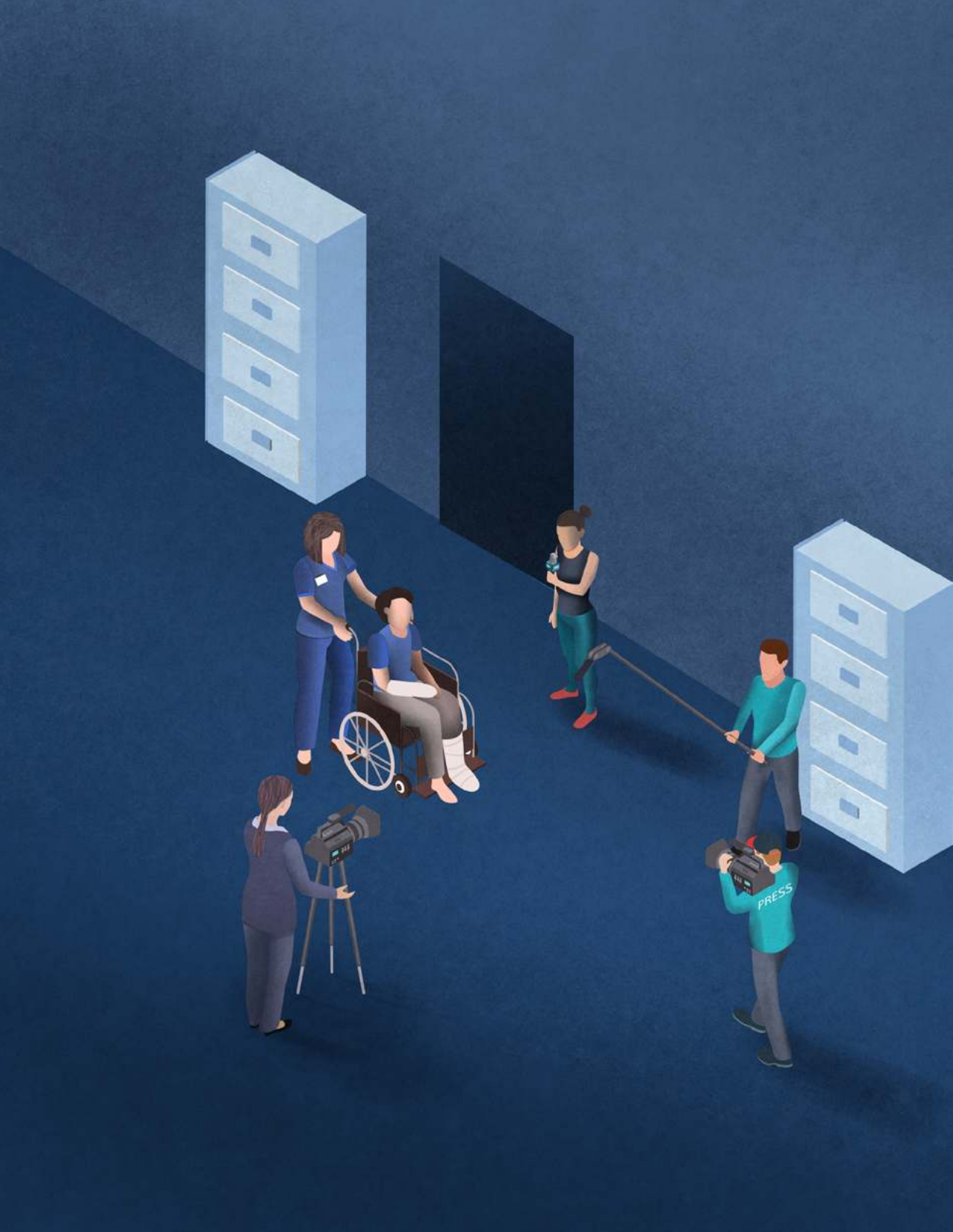
Request for correction or restriction of processing: Pursuant to **Article 17,** if Arjeta believes that her data has been processed in an unauthorized manner, she may request the correction or restriction of processing of her data.

Claim for compensation of damages: Pursuant to Article 56 of the law, Arjeta can file a claim for compensation for material and non-material damages, for violations of her rights.

SCENARIO 2:

Photographing and videotaping patients

Patient privacy is not an option – it is a fundamental right!!


PRESS

SCENARIO 2:

Photographing and videotaping patients

After a car accident, Faton, a 33-year-old man is receiving treatment at a hospital in Peja. While he is in the hallway awaiting treatment, a local TV station comes to cover a story from the emergency room. The reporter film Faton without his consent, capturing his injuries and his fragile condition. The footage is then broadcast on the evening news, showing Faton's condition to all who watched the news. The next day, Faton learned from numerous phone calls he received that all of his family and friends were shocked by the images they had seen, causing him to experience great emotional distress due to the exposure of his condition without his consent. This violation of privacy causes concern for Faton and his family, highlighting the importance of legal and ethical standards when it comes to media reporting in healthcare settings in Kosovo.

What were the specific obligations of the Journalists in this particular case?

- **Following the steps to obtain permission for recording inside clinics:** There is specific policy to request permission for recordings within clinics. Journalists must ensure that these procedures have been followed.

- **Code of ethics:** Journalists and self-regulatory bodies of journalism must ensure compliance with the law on the protection of personal data and the code of ethics of journalism.

It is recommended: that the relevant institutions of this field establish and promote the guiding criteria for determining public interest, as well as guide journalists on the need to obtain consent for cases where such sensitive personal data are in question.

What could Faton do in the described scenario?

Pursuant to the **Law on Protection of Personal Data**, Faton can take the following actions:

Data deletion request: Pursuant to **Article 16**, Faton has the right to request deletion of his footage from the media that broadcasted it without his consent.

Request for restriction of processing: Pursuant to **Article 17,** he may request the restriction of the processing of his personal data until he is assured that these have been processed on a legal basis.

Complaint to the Information and Privacy Agency: Pursuant to **Article 52,** Faton may file a complaint with the Agency to request an investigation into the violation of his privacy and to take measures to ensure that his data is protected.

Claim for compensation: Pursuant to **Article 56,** Faton has the right to file a claim for compensation for material and non-material damages, due to the violation of his rights and the impact that the broadcast of the footage has had on his work and personal life.

SCENARIO 3:

Publication of patient data for treatment abroad

Respecting patients' dignity
and privacy is an obligation,
not a choice!


NDIHMO
DIAGNOZA

SCENARIO 3:

Publication of patient data for treatment abroad

Donjeta, a 6-year-old girl from Gjilan, has a serious kidney problem and needs urgent treatment abroad. To raise funds, Donjeta's family felt they had no other choice but seek help from a media outlet and a charity organization. To prove the girl's illness to these parties, Donjeta's family shared the details of her diagnosis with the media outlet and the organization in question. After that, these parties made a public post calling for fundings for Donjeta's treatment, the post also included details about her medical diagnosis and the type of illness Donjeta was suffering from. The post reached hundreds of thousands of people, some of whom mocked her family for their poverty and social background.

Pursuant to the Law on Protection of Personal Data, Donjeta's family can take the following actions:

- **Request for deletion of personal data:** Pursuant to **Article 16,** Donjeta's family can request the deletion of posts of any sensitive data about their daughter's health condition, which has been published without adequate protection.

- **Complaint to the Information and Privacy Agency:** Pursuant to **Article 52,** if data was shared without their consent, the family can file a complaint for investigation and action against the entities that published this data without protection.

- **Request for restriction of processing:** Pursuant to **Article 17,** they can request that the media and charity organization restrict further processing of their daughter's data.

- **Claim for compensation of damages:** Pursuant to **Article 56**, the family may file a claim for compensation for material and non-material damages, due to the violation of Donjeta's rights and the damage that may have been caused to the family as a result of the exposure of their daughter's sensitive details.

What were the obligations of the institutions involved:

- The institution/organization is responsible for assessing and protecting the data even if Donjeta's parents were not clear regarding the type of consent for processing.

- General research of the current state of privacy policies for media and organizations should be conducted.

SCENARIO 4:

Requests for genetic data from health insurance companies

Sharing sensitive data requires clear consent and strong reasoning!


REFUZUAR
REFUZUAR
DNA TEST

SCENARIO 4:

Requests for genetic data from health insurance companies

Arben, a 52-year-old insured with a local health insurance company, submits a claim for reimbursement for cancer treatment. The insurance company requests his detailed medical tests, including genetic data, which were conducted to assess his risk for inherited diseases. Although Arben feels embarrassed about sharing this sensitive information, he fears that his claim will be rejected if he does not comply with the requirements. This scenario illustrates the coercive practices that can occur in health insurance processes in Kosovo, where personal data is often requested without consent or sufficient justification.

What are the recommended actions for Arben?

- **Refusal to process genetic data without explicit consent:** Arben has the right to **refuse the processing of his genetic data**, if they are not necessary for the fulfillment of the claim for reimbursement, based on **Article 8** of the law, which stipulates that genetic data and sensitive data shall be processed only with explicit consent, and in very specific cases. The insurance company must have a **clear legal justification** for requesting such data, and Arben has the right to request clarification **on the rational and purpose** of obtaining such data.

- **Request for transparency and access to information:** Pursuant to **Article 14,** Arben may **request access to personal data** processed by the insurance company.

  He is entitled to know:

  ➔ Why is his genetic data being requested;
  ➔ How will that data be processed and how long will it be stored;
  ➔ Who will have access to his data.

- **Request for restriction of processing:** Pursuant to **Article 17**, Arben is entitled to r**equest restriction of the processing** of his personal data until it is ensured that the insurance company is acting in accordance with the law and only requests the data necessary to fulfill the claim for reimbursement.

- **Request for deletion of unnecessary data:** In case the genetic data is collected without clear reason or without his consent, **pursuant to article 16,** Arben has the right to **request for deletion of unnecessary data**. This includes requiring sensitive data to be immediately deleted from the insurance company's system if it has been collected without a legal basis.

- **Submitting a complaint to the Agency:** If Arben feels that his data is being processed unlawfully or without his explicit consent, pursuant to **Article 52,** he has the right to **file a complaint with the Information and Privacy Agency.** The Agency may investigate the case and take measures to protect his rights.

- **Claim for compensation:** Pursuant to **Article 56,** if the insurance company processes his data without justification or causes damage to Arben through unlawful processing of his data, he has the right to **claim compensation** for the violation of his rights.

SCENARIO 5:

Placement of surveillance cameras by public and private institutions

Respect for privacy and the protection of personal data are inalienable rights of every worker in the workplace!

SCENARIO 5:

Placement of surveillance cameras by public and private institutions

Blerina works as an administrative assistant in a state office in Prizren. Recently, cameras were installed throughout the workplace, including shared areas and shared break rooms (kitchen used for lunch). The constant surveillance makes Blerina and her colleagues feel uncomfortable, as they are being watched even during their breaks. Workers were not informed about the cameras or the purpose of the recordings, raising serious concerns about privacy in the workplace and the rights of workers in the public sector in Kosovo.

Obligations of the institution in this particular case:

Pursuant to the Law on Protection of Personal Data, the public or private institution when installing and managing the surveillance camera, they have the following specific obligations:

1. **Internal decision on the installation of cameras:** The institution is obliged to issue an internal decision, which must contain reasons for the installation of camera surveillance systems and the appointment of the person responsible for their administration. The decision must be in compliance with **Article 76,** which requires that surveillance be carried out only if necessary for the safety of people and property, and these images cannot be used for other purposes unless required by a specific law.

2. **Notice of placement of cameras:** The institution must clearly and visibly notify employees of the existence of cameras and their purpose, as defined by **Article 75, paragraph 2 and Article 78, paragraph 4**. The notification must be clear and visible to all parties involved, in order to respect the rights of data entities.

3. **Restriction of surveillance:** Pursuant to **Article 78, paragraph 3,** camera surveillance is prohibited in private spaces, such as changing rooms, kitchens, sanitary areas, or any other space where employees expect to have privacy. Surveillance should be allowed only in spaces where a security risk is present.

4. **Data storage and protection:** Pursuant to **Article 76, paragraph 7,** the institution must set a maximum period for the retention of recordings, which may not exceed one month, unless there are legitimate reasons for extending this period. Pursuant to **Article 75, paragraph 4,** the data must be protected from unauthorized access or use.

What could Blerina do in this particular case?

Pursuant to the **Law on Protection of Personal Data**, Blerina may take the following actions to protect its privacy:

1. **Request for information and transparency:** Blerina has the right to request from the institution for clear information on the purpose of the installation of cameras, locations where they are installed and the data retention period. This request is supported by **Article 14** of the Law.

2. **Request to terminate data processing in private spaces:** Pursuant to **Article 78, paragraph 3,** if cameras are installed in shared spaces such as the kitchen or break rooms, Blerina has the right to request the termination of data processing in these private spaces.

3. **Complaint to the Information and Privacy Agency:** Pursuant to **Article 52,** if the institution does not act in accordance with her requests, Blerina has the right to file a complaint for investigation with the Information and Privacy Agency.

4. **Request for deletion of personal data:** Pursuant to **Article 16** of the Law, Blerina may request that her data be deleted if it has been processed in an unauthorized manner or in areas where there should be no surveillance.

5. **Claim for compensation of damages:** Pursuant to **Article 56,** if Blerina suffers material or non-material damage due to the illegal installation of cameras and surveillance of her privacy, she has the right to seek compensation for the damages caused.

These actions comply with legal provisions and help Blerina protect her privacy and her rights in the workplace.

SCENARIO 6:

Data processing by public and private telecommunications institutions

Every piece of information has value - protect it like a treasure!


XXX - XXX
I Nderuari z.Besim
Oferta deri XXX....
Blej TANI...

SCENARIO 6:

Data processing by public and private telecommunications institutions

Besim, a 40-year-old man from Mitrovica, begins receiving personalized promotional offers via SMS based on his call history and web browsing history. He never agreed to his data being used in this way and feels that his privacy has been violated. After an investigation, Besim discovers that his telecommunications provider has shared his personal data with third-party marketing companies without his consent, a practice that highlights the lack of data protection measures in the telecommunications sector in Kosovo.

Obligations of the telecommunications service provider in this case:

Pursuant to **Article 73 of the Law on Protection of Personal Data,** the telecommunications institution has specific obligations regarding processing and sharing of personal data for direct marketing purposes. These obligations include:

1. Use of data only with explicit consent: Pursuant to **Article 73, paragraph 1,** the telecommunications institution may only use personal data collected from public sources or collected within the framework of lawful activities for direct marketing purposes. **Prior consent** is required for other data, especially sensitive data, which may only be processed with **explicit written consent**.

2. Informing the data entity about its rights: Pursuant to **Article 73, paragraph 3,** in the event of direct marketing, the institution has the obligation to inform data entities, such as Besim, of their rights in accordance with the provisions of the law, including the right to object to the processing of personal data for marketing.

3. Disclosure of data to third parties for marketing purposes: Pursuant to **Article 73, paragraph 4**, before sharing personal data with third parties for marketing purposes, the institution is obliged to obtain **explicit written consent** from Besim. Furthermore, the institution must inform him of all information intended to be shared and with whom.

4. **Restriction of Data Processing:** Pursuant to **Article 73, paragraph 2**, the institution may only process basic data for direct marketing, such as name, address, telephone number, and e-mail, and only if Besim has given his prior consent for these data processing.

What could Besim do in this particular case?

Pursuant to the Law on Protection of Personal Data, Besim may take the following actions to protect its personal data and privacy:

1. **Request for termination of data processing for direct marketing:** Besim may request that the processing of his data for marketing purposes be terminated, if that is taking place without his explicit consent, pursuant to **Article 20** of the Law, he is allowed to object to such data processing for direct marketing.

2. **Request for deletion of personal data:** Pursuant to **Article 16** of the Law, if Besim has not given his consent to the data processing for marketing purposes, he may request that his data be deleted from all registers of companies that have received them without his authorization.

3. R**equest for transparency and access to data:** Pursuant to **Article 14** of the Law, Besim may request clear information from the telecommunications institution on how his data has been processed, sources of collection of this data, and with which third parties they have been shared with.

4. **Request for written consent:** Pursuant to **Article 73, paragraph 4,** if the institution has shared his data with third parties for marketing, Besim has the right to request that all further sharing of data be made only after obtaining his written consent.

5. **Complaint to the Information and Privacy Agency:** Pursuant to **Article 52,** Besim may file a complaint with the Information and Privacy Agency if he believes that his data has been used unlawfully without his consent.

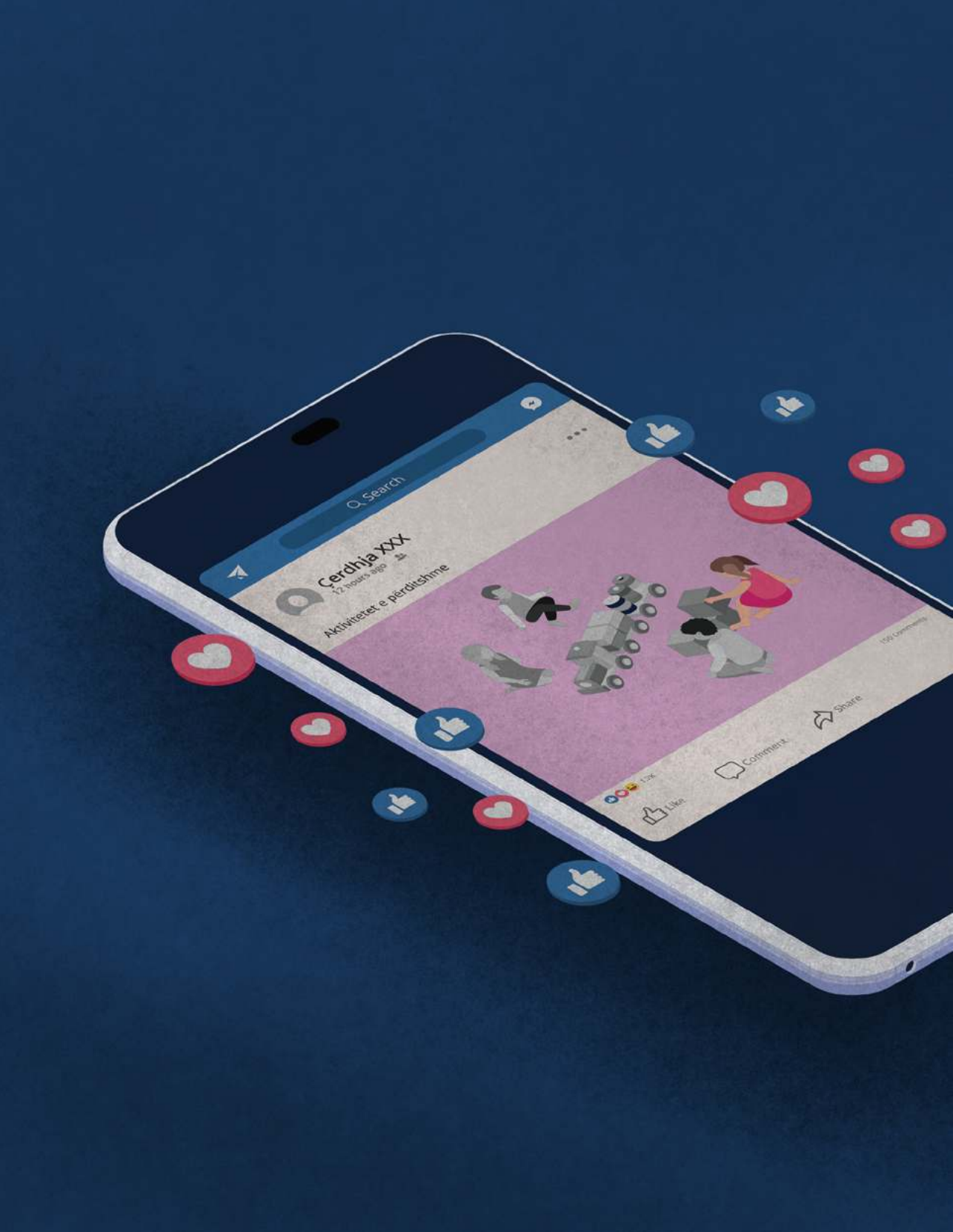
6. **Claim for compensation of damages**: Pursuant to **Article 56** of the Law, if Besim has suffered material or non-material damage as a result of the unauthorized use of his data, he has the right to claim compensation for the damages caused.

These actions will help Besim protect his privacy rights and ensure that his personal data is not used unlawfully by telecommunications institutions and third parties involved in marketing.

SCENARIO 7:

Use of cameras and data processing in pre-school institutions

Child's privacy is a fundamental right. Let's ensure that their data is protected and that they grow up in a safe environment!


Search
Çerdhja xxx
12 hours ago
Aktivitetet e përditshme
Like
Comment
Share

SCENARIO 7:

Use of cameras and data processing in pre-school institutions

Drita, a 3-year-old girl, has been sent by her parents to a daycare center in Ferizaj, where surveillance cameras have been installed in classrooms and playground areas. The daycare center often posts videos and photos of the children on its Facebook page to show daily activities. Drita's parents were never asked for consent and were shocked to see their daughter's images online, available for anyone to see. The scenario demonstrates the growing privacy concerns surrounding the use of surveillance in educational settings in Kosovo, especially when children are involved.

Obligations of the Daycare center in this particular case:

Based on the **Law on Protection of Personal Data**, and in particular the provisions on camera surveillance and the protection of child's data, the daycare center has these specific obligations regarding the use of cameras and processing of child's personal data:

1. **Placement of camera notifications**: Daycare center is obliged to post visible and clear notices regarding the use of cameras, as defined by **Article 75, paragraph 2.** The notice must be clear and visible, informing parents and visitors of the existence of cameras and the purpose of the surveillance.

2. **Requesting consent from parents**: Pursuant to **Article 7 and Article 73 of the Law,** since camera surveillance occurs in spaces where children are involved, the daycare center must obtain the **explicit written consent from child's parents or legal guardians.** Without their consent, processing visual data for purposes such as publishing on social networks is illegal.

3. **Restricted use of cameras:** Pursuant to **Article 76,** cameras may only be installed in areas where it is necessary for the safety of people and property, such as entrances and hallways. Installing cameras in children's classrooms or playground areas must be avoided in order to protect child's privacy.

4. **Data storage**: Pursuant to **Article 75, paragraph 4 and Article 76, paragraph 6,** camera footage must be retained only for as long as is necessary for the intended purposes and must be protected from unauthorized access and use. Retention of data for more than one month is permitted only if there is a legitimate purpose.

5. **Informing parents and daycare workers about their rights:** The daycare center must inform parents of their rights regarding the processing of child's personal data, including the right to access, rectify, erase and restrict processing, pursuant to **Article 14,** and the daycare center employees, pursuant to **Article 78, paragraph 4.**

What could Drita's parents do in this particular case?

Based on the parents may take the following actions to protect their daughter's privacy:

1. **Request for information and clarification on the use of cameras:** Parents have the right to request from daycare center to inform them about the purpose and placement of cameras, as well as how their children's data is processed and stored. This action is supported by **Article 75 and Article 14** of the Law.

2. **Objection to data processing for undesired purposes:** Parents may object to the processing of their child's data for publication on social networks or for marketing purposes, pursuant to **Article 20,** which allows data entities to refuse data processing for specific purposes.

3. **Request for deletion of personal data:** Pursuant to **Article 16** of the Law, if videos or photos of a child are published without their consent, parents have the right to request for immediate deletion of materials from all platforms where they were published.

4. **Complaint to the Information and Privacy Agency:** Pursuant to **Article 52,** parents may file a complaint with the Information and Privacy Agency if they feel that their daughter's data has been processed unlawfully, requesting that data protection measures be taken.

5. **Claim for compensation for damages:** Pursuant to **Article 56** of the Law, if parents believe that their daughter has suffered material or non-material damage due to unauthorized publication of her data, they may seek **compensation for the damages caused.**

These actions ensure that the daycare center respects parents' and child's rights, and the protection of personal data, including transparency and security of footage.

SCENARIO 8:

Use of cameras and data processing in educational institutions

In educational institutions, students must be educated with skills, and not exposed to risks!

SCENARIO 8:

Use of cameras and data processing in educational institutions

Ardit, a 16-year-old high school student in Gjakova, was filmed by a surveillance camera installed in his classroom. The footage is stored on the school's server, but security measures are weak and some staff members have unrestricted access to it. One day, a teacher accidentally shared in a Viber Staff Group a video clip, where Ardit was in the exam in biology class, thus exposing him without his consent. Ardit has a condition that makes it difficult for him to express himself, especially in stressful situations. The video circulated in the Viber group also circulates outside of it and was posted by third parties on Facebook and Instagram. Ardit is experiencing this situation severely and is requesting to change the school.

Obligations of the school in this case:

Based on the **Law on Protection of Personal Data**, as well as the specific provisions on the use of cameras in the education sector, the school has the following obligations regarding camera surveillance and the processing of students' personal data:

1. **Internal decision on the installation of cameras:** Pursuant to **Article 76,** paragraph 2, the school is obliged to issue an internal decision on the installation of cameras, which must include the clear purpose of using the cameras and the person responsible for their administration.

2. **Notice of use of cameras:** Students, parents and school staff must be clearly informed in a written form about the existence of cameras and their purpose, according to **Article 75, paragraph 2 and Article 78, paragraph 4.** Notices must be visible in all areas where there are cameras.

3. **Data storage and security:** Data collected through cameras must be stored securely and protected from unauthorized access. **In this case, unrestricted access by some staff members** to the stored data is in contradiction to **Article 75, paragraph 4,** which requires that the data be protected from unauthorized use. Pursuant to **Article 76, paragraph 7,** the retention of data must be limited to the period that is necessary for the purpose of the data processing.

4. **Restriction of data processing:** The school should limit the processing of images for security purposes only and their distribution must not occur without student's or parents' explicit consent, especially in situations where publication of images causes harm. Cessation of unauthorized distribution is required by **Article 73, paragraph 4**.

5. **Student or parent consent:** Pursuant to **Article 7,** consent for processing of personal data for students under 16 years of age must be given by parents or guardians. In this case, Ardit is over 16 years of age and he should be the one to give consent for processing and use of his images in any form, in particular for further publication.

6. **Staff training:** The school is obliged to inform and train staff about **their responsibilities** regarding the protection of students' personal data and the appropriate use of cameras.

What could Ardit or his family do in this particular case?

Pursuant to the **Law on Protection of Personal Data**, Ardit and his parents may take the following actions to protect his rights:

1. **Request for information on the use of cameras:** Pursuant to **Article 14,** Ardit and his parents have the right to request information on the **purpose and placement of cameras**, as well as security measures that the school has taken to store the data. They can also request access to the data collected about Ardit.

2. **Request for deletion of data:** Pursuant to **Article 16** of the Law, Ardit has the right to request immediate deletion of his personal data that has been processed and distributed without his consent, especially images that have been distributed on Viber and social networks.

3. **Objection to data processing:** Pursuant to **Article 20** of the Law, Ardit may object to the further processing of his personal data and request the termination of unauthorized classroom surveillance or the restriction of data processing.

4. **Complaint to the Information and Privacy Agency:** Pursuant to **Article 52,** if the school does not meet the requirements for personal data protection, Ardit and his parents may file a **complaint with the Information and Privacy Agency,** requesting that the necessary measures be taken to protect his data.

5. **Claim for compensation for damages:** Pursuant to **Article 56** of the Law, if the distribution of the footage has caused psychological and emotional damage to Ardit, he or his parents have the right to seek **compensation for material and non-material damages.**

Improvements to school protective measures:

1. **The installation of cameras must be limited to areas where security is needed,** such as entrances or hallways, and not in classrooms where students are exposed to continuous filming, pursuant to **Article 78, paragraph 2.**

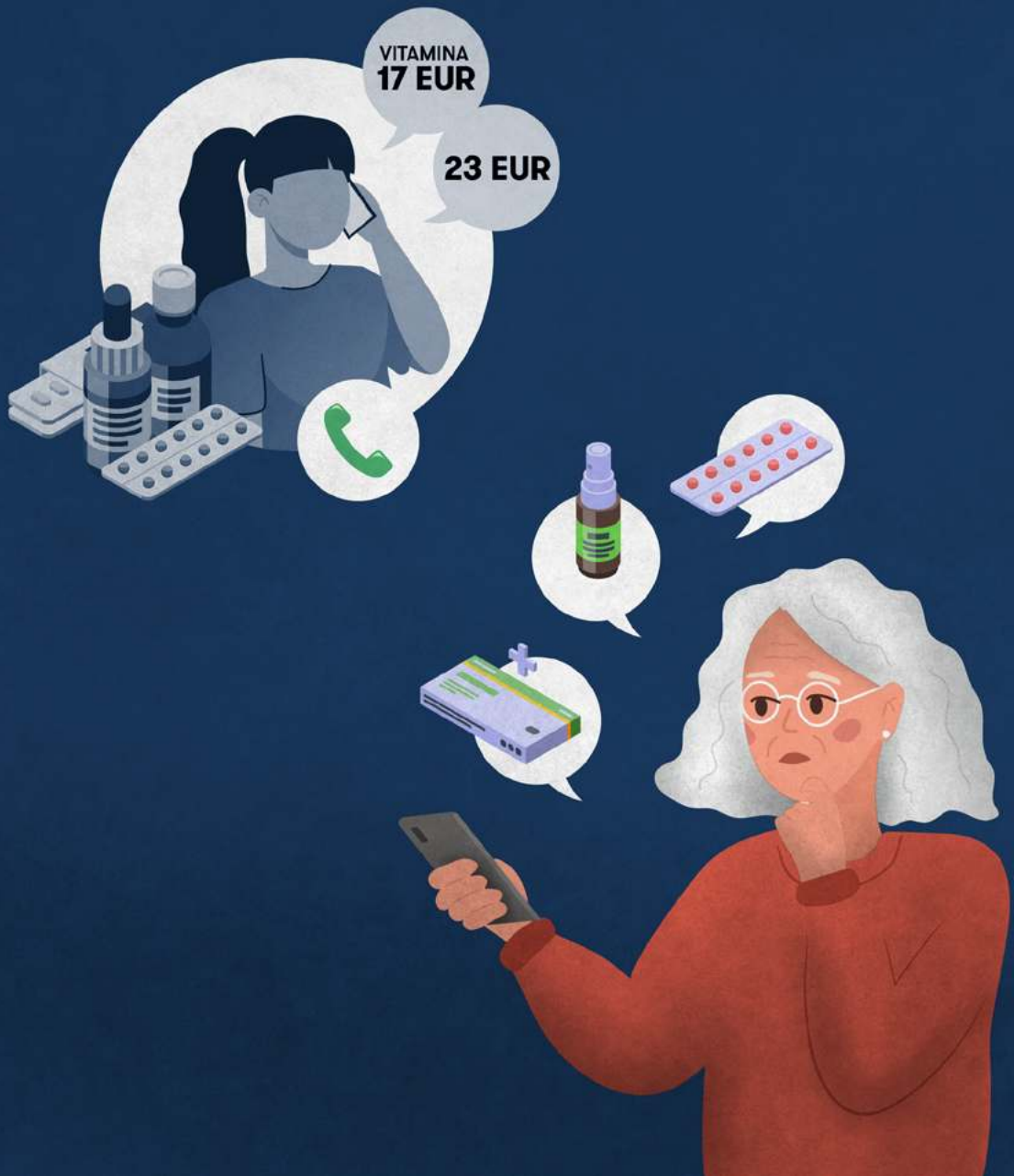
2. **Server security systems must be improved,** and access to records must be limited and monitored, ensuring that only authorized personnel have access to the data collected, pursuant to **Article 75, paragraph 4.**

These measures will help ensure the protection of Arditi's rights and ensure that data processing is lawful and in accordance with privacy protection standards.

SCENARIO 9:

Direct marketing - SMS and non-stop phone calls

Every personal information is part of our identity - its protection is an obligation for every company and institution!


VITAMINA
17 EUR
23 EUR

SCENARIO 9:

Direct marketing - SMS and non-stop phone calls

Valbona, a 66-year-old pensioner from Prishtina, begins receiving incessant calls and SMS messages from a new pharmaceutical company promoting certain medical products. She is surprised because she has never given her contact details to this company. Moreover, she is surprised because the offers Valbona receives are precisely for the treatment of the disease and health concerns that she has recently identified. It turns out that her data has been sold by a third-party marketing agency without her knowledge, causing concern and highlighting the intrusive nature of direct marketing practices in Kosovo, which often occur without sufficient consumer protections.

Obligations of the pharmaceutical company and the marketing agency in this particular case:

Pursuant to the **Law on Protection of Personal Data,** and in particular the provisions on direct marketing, the pharmaceutical company and the marketing agency have several specific obligations to protect Valbona's personal data and to ensure that their practices comply with the law:

1. **Seeking clear and informed consent:** Pursuant to **Article 73 of the Law,** the pharmaceutical company and the marketing agency are obliged to obtain Valbona's **clear and informed consent** for processing and use of her personal data for direct marketing purposes. The consent must clearly include which data will be used and for what purpose, as well as inform Valbona of her rights.

2. **Use of personal data for marketing:** Pursuant to **Article 73, paragraph 2,** data controllers may only use personal data that have been lawfully obtained for direct marketing purposes, such as name, address and telephone number. Any use of sensitive health information requires **explicit written consent** from Valbona.

3. **Data sharing without consent is prohibited:** Pursuant to **Article 73, paragraph 4,** the marketing agency shall not share Valbona's personal data with other companies without her prior explicit consent. This provision requires that any data disclosure be made only after obtaining consent and clear notification to the data entity.

4. **Security measures for data protection:** Pursuant to **Article 31** of the Law, the pharmaceutical company and the marketing agency must ensure that Valbona's data are protected from unauthorized access or unauthorized distribution, by taking **technical and organizational measures** to guarantee the security of the data. These measures include the encryption and pseudonymization of personal data, as well as protection against any unauthorized loss or destruction.

5. **Rights information:** Valbona must be informed of her rights to object to direct marketing, pursuant to **Article 73, paragraph 3,** which includes the right to refuse processing of data for marketing purposes and to request that it no longer be contacted via phone calls or SMS.

What could Valbona do in this particular case?

Pursuant to the **Law on Protection of Personal Data,** Valbona may take the following actions to protect its rights:

1. **Request for deletion of personal data:** Pursuant to **Article 16 of the Law,** Valbona has the right to **request deletion of her personal data** that has been processed without her consent and to prohibit the pharmaceutical company and the marketing agency from further processing her data.

2. **Objection to direct marketing:** Pursuant to **Article 20 and Article 74**, Valbona may object to processing of her data for **direct marketing** purposes and request to no longer be contacted by the pharmaceutical company or marketing agency.

3. **Request for information and transparency:** Pursuant to **Article 14,** Valbona may request information on **how its data is processed and shared with third parties.** It has the right to know how its data was obtained and who has access to it.

4. **Complaint to the Information and Privacy Agency:** Pursuant to **Article 52** of the Law, if Valbona believes that her data has been processed unlawfully, she has the right to file a complaint with the **Information and Privacy Agency.** The Agency may investigate the matter and take the necessary measures to protect her data.

5. **Claim for compensation of damages:** Pursuant to **Article 56** of the Law, if Valbona believes that it has suffered material or non-material damage due to unauthorized distribution of her data, it may seek **compensation for the damages caused.**

Additional measures to be taken by the pharmaceutical company:

1. **Seeking and verifying the consent of data entities:** The company must ensure that it obtains Valbona's **prior consent** for the use of her personal data for marketing purposes, as defined in **Article 73, paragraph 1.**

2. **Data storage and protection:** The Company must **implement appropriate technical and organizational measures** to protect Valbona's data from unauthorized access and distribution, as required by **Article 31.**

3. **Transparency and information:** Pursuant to **Article 14 and Article 73, paragraph 3,** the company must ensure that Valbona is **fully informed** about how her personal data will be processed, and about her rights to object data processing for marketing purposes.

These measures will ensure that Valbona's personal data is processed lawfully and in accordance with privacy protection standards.

SCENARIO 10:

Transfer of personal data by banks

The right to privacy
is a cornerstone of a
democratic society – it is
everyone's responsibility to
protect it at all costs!


CREDIT CARD
1234 5678 9012 3456
Agon Banka

SCENARIO 10:

Transfer of personal data by banks

Agon, a 27-year-old IT professional, opens a new bank account at a well-known bank in Prishtina. The bank informs him that his personal and financial data will be stored by a third-party service provider abroad. Without Agon's explicit consent, his data is then transferred to another company as part of a new service agreement. Meanwhile, the company where his data was stored abroad, due to weak policies of that country, sold the data of 100,000 persons, including Agon's data, to a third party. The third party then understands Agon's financial situation and cancels a deal that was being negotiated for the sale and purchase of some shares, because, understanding Agon's financial situation, the third party demanded a price many times higher than the one for which the negotiation had begun.

Agon feels his privacy has been violated, as his sensitive information is being transferred between multiple companies without proper notice, highlighting the lack of transparency in how banks in Kosovo handle personal data.

Obligations of the bank and the third party in this particular case:

Pursuant to the **Law on Protection of Personal Data,** the bank and third-party service providers abroad have several key obligations to ensure that Agon's personal data is handled with sufficient transparency and security:

1. **Notification and solicitation of explicit consent:** Pursuant to **Articles 14 and 49** of the Law, the bank must inform Agon in a clear and transparent manner about the transfer of personal data to a service provider abroad. This must include the **purpose and manner of processing** the data and Agon's consent must be obtained for this transfer, unless the transfer is mandatory under a law or international treaty.

2. **Level of protection in the third country: Articles 44** and **45** state that transfer of personal data abroad may only take place if the receiving country ensures **an adequate level of protection** of personal data, as determined by the **Information and Privacy Agency.** The Bank is obliged to verify that the receiving country or organization provides **security equal to or higher** than the standards in Kosovo.

3. **Provision of technical and organizational measures:** Pursuant to **Article 31,** the Bank and the data processor abroad are obliged to implement **appropriate technical and organizational measures** to protect Agon's personal data. This includes **pseudonymization and encryption** of the data, as well as the ability to restore their availability in the event of an incident.

4. **Contractual agreement with the external data processor:** Pursuant to **Article 47, paragraph 1,** the Bank must have a **clear contractual agreement** with the data processor abroad, which includes details on the security of the data and guarantees for their processing. This agreement must contain details on the protection of the data and the limitation of their use for purposes other than those for which they were transferred.

5. **Notification of any data leaks:** Pursuant to **Article 33** of the Law, in the event of a data leak by a third party abroad, the bank is obliged to notify the **Information and Privacy Agency within 72 hours** and to inform customers, including Agon, of the nature of the leak. The bank is responsible for ensuring that the processor abroad complies with these obligations.

6. **List of countries with an adequate level of protection:** Pursuant to **Article 46,** the Agency must maintain a **list of countries or international organizations** that ensure an adequate level of data protection. The Bank is responsible for ensuring that the transfer of Agon's data is made only to a country that appears on this list, or if not, to obtain authorization from the Agency for the transfer of data to a third country with insufficient protection.

What could Agon do in this particular case?

Pursuant to the **Law on Protection of Personal Data**, Agoni may take the following actions to protect its rights and demand transparency regarding the processing of its data:

1. **Request for information on data transfer:** Pursuant to **Article 14,** Agon has the right to request **clear and complete information** from the bank on the reasons for the transfer of his personal data abroad, including the safeguards taken by the processor abroad.

2. **Objection to further data processing:** Pursuant to **Article 20,** Agon may **object to further processing** of his personal data by the company abroad, if this processing is done without his consent or is in contradiction to the purpose for which the data was collected at the initial stage.

3. **Request for deletion of personal data:** Pursuant to **Article 16** of the Law, Agon has the right to request for **deletion of his personal data** from the processor abroad and from any third party that has gained access to this data, especially in the event of misuse of his data for other purposes.

4. **Complaint to the Information and Privacy Agency:** Pursuant to **Article 52,** if Agon believes that his data has been transferred and processed unlawfully, he has the right to file a **complaint with the Information and Privacy Agency,** which may investigate the case and decide on the necessary measures.

5. **Claim for compensation of damages:** Pursuant to **Article 56,** if Agon has suffered material or non-material damage as a result of the unauthorized transfer of his data, he has the right to **claim compensation for the damages caused.**

Additional measures to be taken by the bank and processor abroad:

1. **Agency authorization for the transfer:** Pursuant to **Article 49,** if the foreign country or organization does not appear on the list of countries with **adequate data protection,** the bank must obtain an **authorization from the Information and Privacy Agency** to carry out the transfer.

2. **Customer notification:** Pursuant to **Article 45**, the Bank must notify Agon of any **further interference** in the processing of its data by the third party abroad, including sharing of data with other parties.

3. **Data protection measures:** Pursuant to Article 31, the Bank and the processor abroad must implement **adequate technical and organizational measures,** including **encryption and pseudonymization** of data, to ensure that Agon's data is secure and protected from any unauthorized access.

Këto masa dhe veprime do të sigurojnë që transferimi i të dhënave të Agonit të kryhet në përputhje me ligjin dhe të mbrojë të drejtat e tij për privatësi dhe siguri të të dhënave personale.

This document is part of the “Human Rightivism” project, conducted under the “Data Guardians: Strengthening Privacy Policies and Awareness in Public Institutions” initiative, led by Lëvizja FOL. The project is implemented by the Community Development Fund (CDF) with the support of the Embassy of Sweden in Pristina.