FREE DATA

Practices on collecting and processing personal data from the private sector

An EU funded project
managed by the European
Union Office in Kosovo

Disclaimer

This publication has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of LENS and can in no way be taken to reect the views of the European Union.

The views expressed in this publication are not necessarily those of the Friedrich-Ebert-Stiftung (FES).

List of Abbreviations

LPPD - The Law on Personal Data Protection

NAPPD – National Agency for Personal Data Protection

ICT – Information and Communication Technology

EU – European Union

RAECP – Regulatory Authority of Electronic and Postal Communications

LEC – Law on Electronic Communications

KOS-CERT – National Computer Security Unit in the RAECP

MIA – Ministry of Internal Affairs

LSEC – Law on Interception of Electronic Communication

CBK – Central Bank of Kosovo

KIA- Kosovo Intelligence Agency

"...you would think by now we would have learned the way these things work, which is this:
1) everything that's already in the world when you're born is just normal;
2) anything that gets invented between then and before you turn thirty is incredibly exciting and creative and with any luck you can make a career out of it;
3) anything that gets invented after you're thirty is against the natural order of things and the beginning of the end of civilization as we know it until it's been around for about ten years when it gradually turns out to be alright really."

Douglas Adams, How to stop worrying and love the Internet

Contents

Introduction

This paper is part of the project "Defending human rights in the digital age", and is implemented by the Association for Privacy, Technology and Media "LENS" as leader, and NGO Kosovar Center for International Cooperation – KCIC as a co-implementer. The project is financed by the EU and is managed by the European Union Office in Kosovo. It lasts 20 months (January 2016 – August 2017), and it is co-financed by the Friedrich Ebert Foundation Pristina.

The aim of the project is to address the violations of human rights, freedoms and democracy, which have appeared or have gotten worse in Kosovo, in the age of technological development. The project intends to increase organizational capacities of Kosovo CSOs, as well as to increase citizens' awareness regarding the protection of personal data, the rights to privacy, freedom of speech and the freedom of press.

From the same series on digital rights you may find:

Laws in place and it's implementation

Secrecy of voting and voter data processing

Impact of digital communication to freedom of expression and media

Overview

Almost all of our daily activities generate data, our electronic communication, banking transactions, medical records, even our grocery shopping preferences, when put together can give enough information for a mathematical modeling or algorithm to build our profile, to satisfy the merchant's curiosity. Thus the private industry is increasingly interested to know who its customers are, by collecting personal information and understanding them better.

This paper elaborates the ways by which the private sector treats personal data with regards to privacy and personal data protection. It covers those sectors that most frequently deal with sensitive information and where the risk of abusing the right to privacy is bigger; it analyses the approach of financial institutions (banking), healthcare service providers, insurance companies, telecommunication companies and media service providers to see, among others, the level of compliance achieved (with regulations).

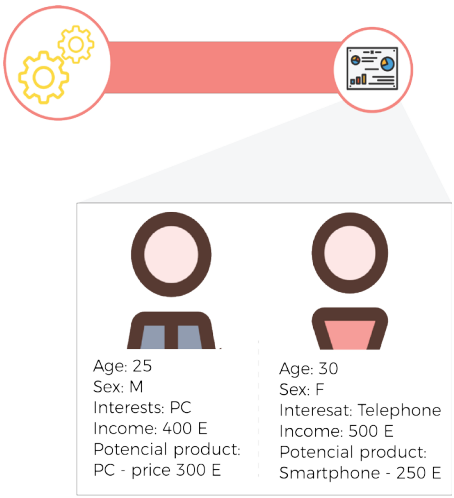
The paper illustrates the procedures for the treatment and processing of personal data, the amount of data that is collected by the private sector, as well as the procedures for addressing the violations of privacy.

The paper gives an overview of how personal data are collected and treated by the private sector in Kosovo, and it also addresses the practices of utilizing these data that would constitute the biggest concerns in the public policies; the implications of collecting, storing and processing of personal data; compliance of operators with the regulations in the country, as well as the compliance of the latter with the international directives

The data market – Who is interested in personal data

When a company has profile data for an individual such as his behavior on the market, his preferences, marketing can very easily be adapted so as to affect his spending.
This kind of targeted marketing on the internet becomes even easier; for companies monitoring the online activity of an individual, his internet browsing, clicks and engagement with their content, is of a high interest, as all of this is used by the algorithms to adapt their content and serve users what has a higher chance of catching attention, in other words to serve the content that one might buy.

It is worth mentioning that in the case of targeted marketing both the customer and the seller/advertiser benefit; the customers benefit because they receive only the information (advertisements) which interest them, thus access to the services and products they want, while the seller does not need to spend in spreading the information where doesn't interest. It is up to the customers to ignore the pages with content that does not interest them, or mark as spam the unwanted advertisement.



The advertising market gives the customers access in a wider scope of services, for example electronic mail (Gmail, yahoo, Hotmail), quick Internet search (google search), access to social networks (Facebook), in which case we willingly give up from some aspects of our privacy in exchange for services.

Procedures for collecting

and processing of personal data

The Law on Personal Data Protection, which has entered into force in Kosovo in 2010, regulates the main aspects on collection and use of personal data.
However, there are a number of laws and regulations, which to some extent assure and regulate the right to privacy. Although Kosovo is not a member of the EU as most laws are influenced from the European Union legislation, the legislation on privacy follows the EU directives as well. Therefore, in the legislation's compilation, but also in its implementation, Kosovo has relied heavily on the European Union.

With the recommendation and the technical assistance program of the EU, the LPPD has been reviewed in the past two years; the concept document on modification and amending along with the Law on Access to Public Documents was approved in the Government meeting on May 15, 2017. The amendment proposals foresee functional restructuring of the Agency for Personal Data Protection.

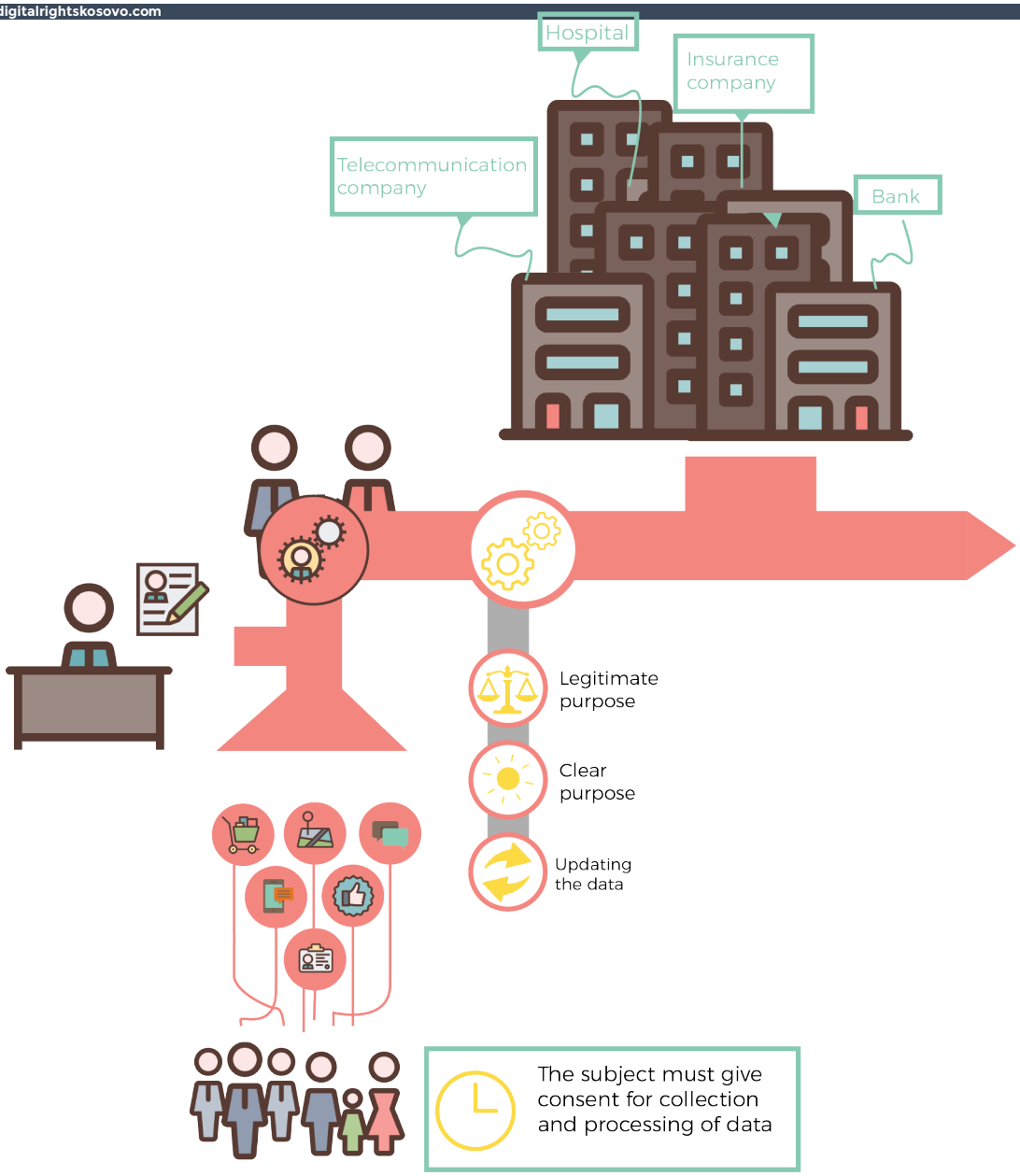
According to the proposed amendments it can be expected that the Agency structure will change, replacing the board of the agency with one commissioner.

The implementation of the law on access to public documents is also expected to be under the competencies of the agency.

The main provisions of the LPPD determine that data must be collected and used only for specific, clear, and legal purposes, with the consent of the customer, and they can be stored only until the aim of their use has been fulfilled. It is also stated that the processing of these data must be done impartially and without violating the dignity of the data's subject[1] .
Meanwhile the LPPD does not oblige the media, organizations, political parties, unions, and religious communities to keep a filing system for their collected personal data.

In any case where personal data are required from an individual, the law

1 L Nr. 03/L-172



foresees that they are notified about[2] :

The identity of the data controller (i.e. the representative or the contact point)

- The purpose of data processing
- Is giving their information obligatory
- Who has the right to access these data and how will these personal data be treated.

Meanwhile, to use the sensitive personal data in direct marketing, the law obliges operators to previously take written consent from their consumers (subject of

2 03/L-172 Article 10

the data).

The special provisions on personal data collection and storage that the private sector must abide by are also defined by the regulations/sublegal acts of the agency.

The difference from the subjects of the public sector is that the private sector is not obliged by law to assign a personal data protection officer (controller). The agency had in force an administrative directive which required the companies who have more than a 100 employees to assign an officer, however this directive has been repealed in 2015 as it was considered an unnecessary burden for the companies[3] . It goes in line with the EU directives that also do not require such appointing.

It is worth mentioning that since July 2016, when the mandate of the previously appointed NAPPD supervisors expired, the Agency has not exercised its function in full. The appointment of new supervisor/commissioner is expected to be done after the amending of the legal package (the Law on Personal Data Protection, and that of Access on Public Information). This amending as stated before, follows the Government's decision and the working group is expected to be set up and start working in the following weeks (June 2017).
According to the NAPPD annual report of the year 2015, the Agency has done 50 inspections in the private sector from the 84 inspections done throughout the year.

Source: Annual report NAPPD, 2015

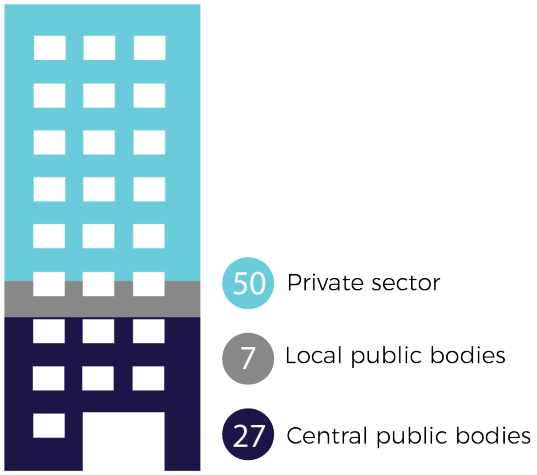


Figure 7 - Inspections according to institutions

3 Interview, General Director NAPPD, April 2017

The law allows companies (data controllers) to use personal data collected from accessible or legal public sources for direct marketing. However, the controllers must inform the subject of the data about their rights, and they are also obliged to allow the right to contradict (refuse) their marketing for a certain period or permanently. Furthermore, in cases when the company contracts a third party in this process, they are obliged to notify their consumers.

NAPPD's annual report for 2015 states that because the Agency has noticed that direct marketing is widely used by the private companies it has decided to inspect them. During the inspections irregularities have been found, such as sending of e-mails and SMSs without the client's consent, subscriptions on various offers and products to citizens without their permission. In this case, the Agency has made decisions through which they have ordered the discontinuation of these practices and in the same time has given legal advice on the on the use personal data for direct marketing purposes[4] . The Agency estimates that these inspections have brought noticeable improvements on the use of direct marketing by the private sector.

Apart from inspections, the agency is responsible and has been handling complaints of subjects on privacy violations. The agency, during the year 2015 has received in total 131 complaints, from which 47 inspections have been made and the necessary steps in accordance with the procedures and the Law on Persona Data Protection have been undertaken[5] . The agency has treated 11 complaints that are related to the social network "Facebook". From the total number of complaints, 21 of them were citizens' concerns with direct marketing with the aim of political promotions. Based on the presented surveys and expressed opinions, we can conclude that direct marketing is one of the issues that raises the most concerns in the public opinion.

4 Annual report 2015, NAPPD http://www.amdp-rks.org/repository/docs/ashmdhp_raporti_vjetor_2015_ALB.pdf
5 Annual report 2015, NAPPD http://www.amdp-rks.org/repository/docs/ashmdhp_raporti_vjetor_2015_ALB.pdf

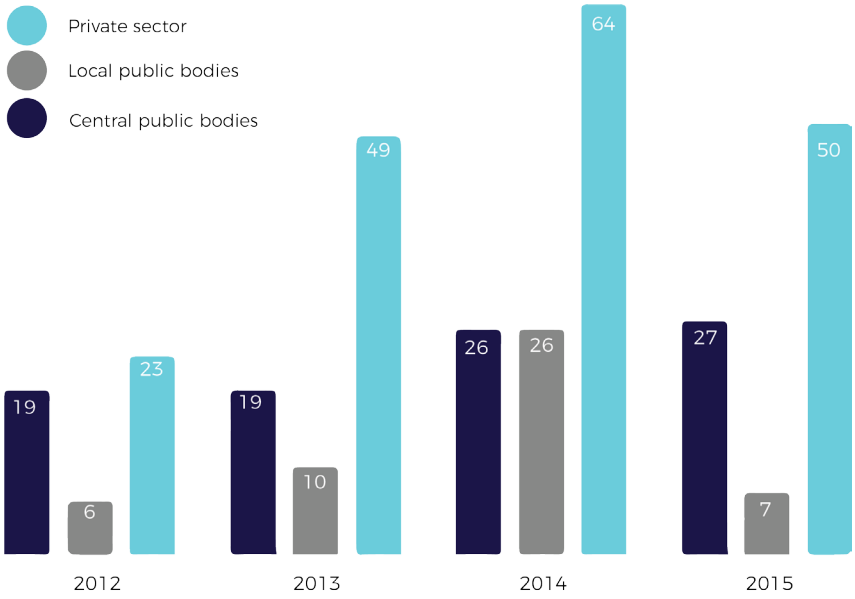


Figure 8 - Inspections according to institutions during years

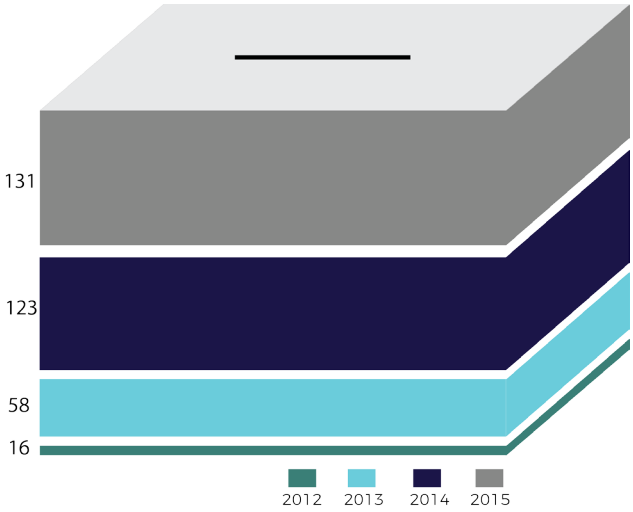


Figure 5 - Complaints reviewed over the years

"Citizens of the Republic of Kosovo have raised their concerns mostly on personal data processing by the controllers, in which case their data were processed with aim of direct marketing, unauthorized disclosure of data, unauthorized disclosure of personal sensitive data, processing of biometric data, processing of data without the subject's consent, processing of data through social networks, as well as the processing of inaccurate data. These complaints have been mainly directed towards the central institutions, local institutions, banking sector, micro-financial sector, insurance companies, health sector, shopping centers, and social networks." – Annual report 2015, NAPPD.

Who has the right to collect data

The law on personal data protection besides specifying the conditions for collecting and processing of personal data does not limit the nature of the companies that may collect personal information. Therefore, any subject from the private sector is allowed to collect customer data, with the condition that they treat them in accordance with the law provisions.

However, as has been mentioned before, this paper is focused on the commercial sectors which collect and store usually large amount of personal data. These sectors are: the health care sector, the banking sector and other financial and insurance institutions, as well as the telecommunications sector.

The health care sector

Patient confidentiality is part of the ancient oath of Hippocrates and it is a central part of the ethical tradition of medicine and health care. This confidentiality tradition is in accordance with the legal requirements in Kosovo, according to which personal data must be collected for a specific purpose, and must not be given to a third party accept in accordance with this purpose.

Considering the high sensitivity of medical information that is collected and processed by professionals of the sector, it is necessary that the engaged medical staff understand everything in regards with the use of personal data.

Patient confidentiality is reduced to:
ὄμνυμι Ἀπόλλωνα ἰητρὸν καὶ Ἀσκληπιὸν καὶ Ὑγείαν καὶ Πανάκειαν καὶ θεοὺς πάντας τε καὶπάσας, ἵστορας ποιεύμενος, ἐπιτελέα ποιήσειν κατὰ δύναμιν καὶ κρίσιν ἐμὴν ὅρκον τόνδε καὶσυγγραφὴν τήνδε...
... and is extended to all levels of data processing.

I swear by Apollo the Healer, by Asclepius, by Hygieia, by Panacea, and by all the gods and goddesses, making them my witnesses, that I will carry out, according to my abiliy and judgment, this oath and this indenture. -Hippocratic Oath

Th ne

aspect of personal data protection. This sector treats some of the most sensitive data, rightly it is expected by the patients that their information will be stored and handled in the safest way possible. It is important that all the employees in the heal care service, just as public health care and social care are careful in this aspect.

The main goal, the safekeeping of the citizens' health, is of an utmost importance. However many circumstances influence health care workers to deny individuals of their right to privacy, such as when faced with the challenge of balancing between public/individual interest and privacy, or when an individual's health as a subject or others who they might affect is put at risk.

While other commercial sectors do not handle sensitive data, the data processed by health care stations, the data on individual's medical condition, is defined by law as sensitive data [6]. Meanwhile, the regulation on the security measures during the procession of personal data obliges the subjects which process these data to identify critical parts of security particularly in regards with their availability, copying, archiving, destruction and anonymisation [7]. For this reason a double check is required for all the parts of the process, as well as a special care on prevention of illegal disclosure and abuse.

It is worth mentioning that in Kosovo, the majority of health services are offered by the public sector. Because of the lack of accurate statistical notes for every kind of intervention, as an example and just for orientation we will mention the births, where from the 24,716 births, according to the official data 22,804 have been in public hospitals. So the share of the public sector over 90%. Another characteristic for Kosovo is the small number of those who have health insurance, because at the moment there is only private health insurance which is not mandatory. Both these facts show an underdeveloped health and health insurance market, consequently the care for the treatment of personal data from this sector has not been raising concerns.

In most cases, besides information on their health condition, the patients tell the health personnel information such as name and surname, name of a parent, date of birth, place of birth, address, their ID number. Those

6 Article 1.16
7 Rr. 03/2015 and 06/2015 Article 20

who have health insurance give the health card number and insurance data such as type, coverage, terms etc.

The most important law on privacy protection in this sector is the Law No. 03/L-172 on the protection of personal data. This law in the second article, under paragraph 1.16 defines the data on medical condition as "sensitive data".

These data may be processed only in certain cases and special conditions, which are more precisely defined in Article 6. Furthermore, the paragraph 1.6 of the same article says that those data may only be used "if they are processed by the health care employees or the health personnel in accordance with the relevant laws with the purpose of protection of society's and individuals' health and the management of proper functioning of health services."

In a smaller part patient's privacy is also defined with the Kosovo Health Law, article 52 touches on issues such as data ownership, confidentiality, collection, storage and management in health institutions. According to this article, the collected data belong to the health institution, and that institution is responsible to guarantee their confidentiality, safety and their procession in accordance with the legal norms[8] .

The Law on Health, which defines health documentation such as prescriptions, notes and data collected in relation with an individuals health, personal identity and their medical condition, all information in which a health care professional has access while the patient is provided with health services, determines that the health condition of the population must be accessible for analysis and reporting by the National Public Health Institute.

This law also foresees that health care professionals and the health care institution must report their services without violating the rights of the users (patients) of health care, ensuring professional confidentiality in accordance with the law. According to this law the owner of medical information is the medical institution, which consequently is responsible for the collection, storing and the safe administration of this data, and they should guarantee the protection and confidentiality of personal data.

8 Law Nr. 04/L-125

Similarly the Law on Mental Health, which defines the rights of persons with mental health issues in the Republic of Kosovo, among other things, also guarantees the right to confidentiality of data on their mental condition [9]. Everyone who conducts activities that are foreseen in the mental health law is obliged to keep the confidentiality of all the information taken from patient in the health care institution. These persons are excused from the obligation of professional secret-keeping only when the information is given to the patient's curative doctor and/or social welfare organizations and in the cases which the bodies which in accordance with the law and provisions of personal data protection in power have the right to demand this kind of information.

The Law on the rights and responsibilities of the citizens in the health care also guarantees the confidentiality of personal data: an inhabitant of the Republic of Kosovo has the right to protect the confidentiality and the secrecy of their personal data and the information in regards with their medical condition and treatment, as well as any kind of information included in their medical documentation [10]. According to this law the citizens have the right to declare who may take information on their condition and the expected medical results, as well as who has the right to be notified completely or partially on health care data. However, this law foresees the possibility that the aforementioned data be revealed without the consent of the said inhabitant if the law defines it.

Furthermore, according to the law on personal data protection, health records may not be processed or collected by using only the binder code (binder code is a personal identification number or any other specific identification code defined by law, bound to the person, a number which may be used reveal or retract personal data from the filing systems in which the binder code is also processed). [11]

In general the healthcare service providers in the private sector tend to be very closed when it comes to giving information on their procedures for handling personal data. More transparency and openness is needed to research their practices. Furthermore, this transparency would increase citizen's trust and prepare them to provide consent for collection of their personal data.
Meanwhile we learn that bigger healthcare centers such as private

9 Law No. 05/L-025
10 Law No. 2004/38
11 Law No. 03/L-172 Article 11, paragraph 1.

hospitals, in the majority of cases have personal data treatment policies in place, however something like that is unlikely for the majority of the 1346 private units of healthcare which operate in Kosovo, that are small and operate in minimal staff requirements.

According to the NNAPPD upon inspection in hospitals it has been concluded that they possess a regulation on security measures. The Agency has requested the initiation of proceedings for misdemeanor at the competent court for a hospital, which allegedly did not have in place the procedures on the security measures.

On the other side, the big hospitals have complained in regards with the obligation not to demand document copies (IDs). According to them this is rendering it difficult to identify the patients in particular the identification of those who do not make their payments for the services in time.[12]

According to the law, personal data of deceased persons may be revealed only to recipients authorized by law, to legal descendants if they express interest and only if the revelation of the information is not prohibited in written by the deceased [13]. Whereas for research, historic, or statistical purposes the data of the deceased may be revealed in two cases, if the person has allowed it in written, or if legal descendants give consent about this.

Whereas the revelation of personal data without the consent of the subject of data may be done only when the revelation:

- is necessary for the protection of the subject's vital interest, as well as for the protection of other basic rights, e.g. when a patient's life is in danger
- is necessary to be in accordance with a legal obligation to which the data controller is subjugated to
- is necessary to perform a task which is in the public's interest or in exercising of an official authority given to the controller or a third party for whom the data have been revealed.

Note: when personal data are revealed to an authority, there should exist at least one written document signed by the authority in regards with

12 Interview, American Hospital, Prishtina
13 03/L-172 N.13

the required information by the data controller.

The big hospitals are currently storing collected information for a period of 5 years. Meanwhile the law[14] foresees that personal data may be stored only for the time that is necessary for the achievement of the purpose for which they were collected or until they are further processed. The lack of clear regulation is confusing for private bodies when it comes to the time frame for which they may store and process collected information. On the case of the achievement of the purpose of the processing, personal data shall be eradicated, deleted, blocked or made anonymous, unless the Law on Archives or another relevant law says otherwise.

The banking, financial and insurance institutions

The financial sector in the Republic of Kosovo is an example of the case where refusal to grant personal information hinders access to services. The data that this sector collects and processes are of a wide scope: identity data, including the address and phone number, information on the wealth of the individual, transactions, and in some cases there are also information on the location, for instance the IP address from where we access online banking services. It should be specified that for the collection of the necessary data for the maintenance of the contract, such as name, address, ID, etc, explicit consent is not required to be asked by the subject of the data. However, if the institution wants to use these data for additional purposes, such as marketing, consent should be explicitly asked. In these cases information related to this kind of processing should be provided to the citizens explicit and clear, they should not use the previously collected information and they must give the subjects the right of refusal. In fact, it is of utmost importance for private bodies to keep records of the given consent.

For health insurance companies, besides the provisions of the LPPD the Health Law, elaborated above, also applies.

The Law no. 05/L-045, on insurances defines the principles and basic rules for licensing, regulation and overseeing of insurers, reinsurers, insurance brokers and other subjects foreseen with this law, in order for the insurance

14 LPPD – Article 3.5

industry in the Republic of Kosovo to operate in a safe, sustainable and transparent way of protecting the rights and interests of policyholders. This law ensures the protection of privacy of all citizens (policyholders) regardless of the type of insurance they hold. The law clearly defines that the insurer collects, stores, and uses personal data, which are relevant for insurance policies and for solving claims which derive from any insurance issues according with this law, in accordance with the Law on Personal Data Protection.

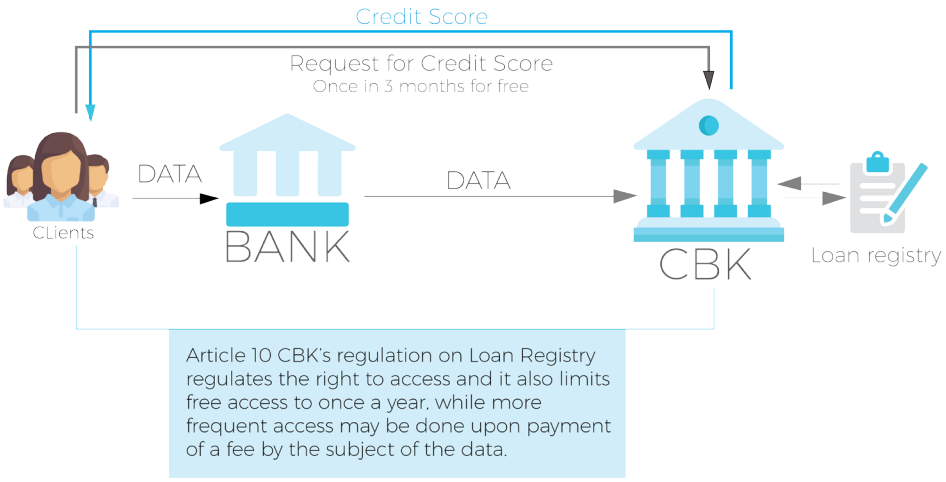
Furthermore, article 17 on system cataloguing, compels the data controller to assign among others[15] the deadline for storing these personal data, however the time frames for private companies remain uncertain and to be decided by them.

Often times some sensitive data may be withdrawn from data which in first sight may not look as sensitive. For example, food menus or healthcare center diets give sensitive information related to the patient based on their nutritional needs depending on their medical condition or their religious views. So, information on a patient's health or sensitive data do not reflect only on the medical records of a patient, sometimes such data may be extracted indirectly, therefore such data as nutrition, especially for insurance companies, are considered as sensitive.

Besides the financial institution that collect customers' personal data, the Central Bank as well, as an overseeing authority for financial institutions, has the role of the warrantor of personal data protector, seeing as it acts as the Controller of Collected Data by the financial institutions. Based on the CBK's regulation on Loan Registrations[16] , CBK compiles and administers Kosovo's Loan Registry through which it collects and distributes the information on loans to the financial institutions. This information is distributed with the aim of the improvement of loans quality and fulfillment of the overseeing duty of the Central Bank.

It should be mentioned that the CBK assumes the role of Data Controller

15 LPPD Article 17, Paragraph 1.7
16 Article 1, Article 6



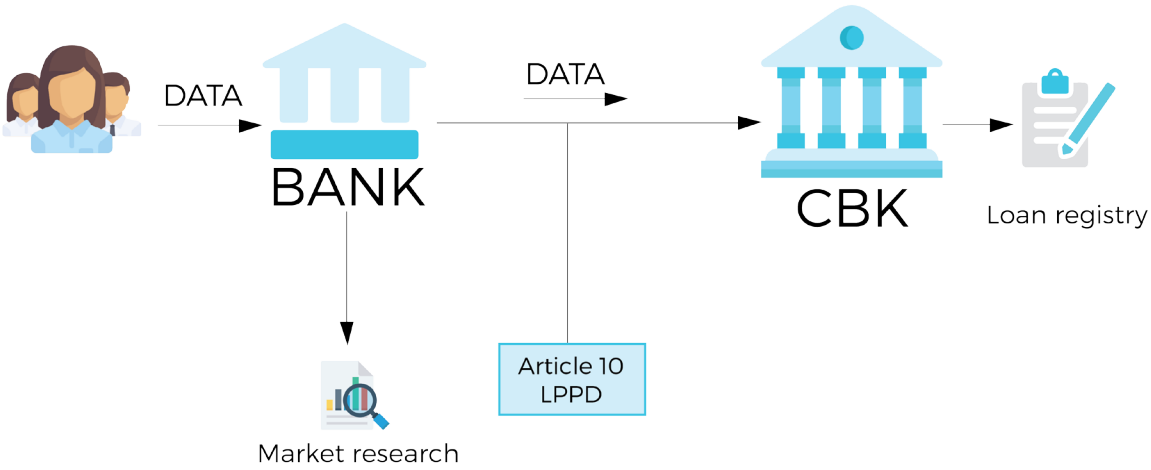
to fulfill its mission, which includes its responsibility to inform the data subjects, ensure the quality of personal recorded data in the Loan Registry, as well as to ensure the exercising of customer's rights. However, the CBK does not hold responsibility on the way the loan information is used or evaluated even in cases when such information is inaccurate, incomplete or delayed as a result of such reporting by the loan providers[17] , nonetheless, this should not diminish the overseeing role of CBK, which should verify and oversee the work of financial institutions, including here the accuracy of reporting.

To summarize, financial institutions collect personal information, and as it is foreseen with the CBK regulation on Loan registry are obliged to refer to article 10 of the Law on Personal Data Protection to inform the subject of the data in regards with the collection and processing of data. In addition these institutions communicate the personal data in regards with citizens' loan information in the Loan Registry of the Central Bank.

This obligation to report comes from article 2 of the CBK Regulation on Loan Registry: loan providers, including here all the banks and micro-financial institutions licensed as well as those none-banking financial institutions and insurance companies licensed to deal with certain loan activities, are obliged to report in the Loan Registry of the Central Bank.

CBK's regulation presents some restrictions in regards with exercising

17 Article 4.3 of the CBK on Loan Recording



of citizens' rights to privacy, such as implied negation of the right to contradict, which should be expressed clearly to the citizen in the given information by the financial institutions.

In addition, instead of the article 23 of the LPPD, article 10, paragraph 2 and 3 of the CBK's regulation on Loan Registry regulates the right to access and it also limits free access to once a year, while more frequent access may be done upon payment of a fee by the subject of the data (article 10.2.1). Article 10.3 of the CBK regulation further states " Loan providers shall report the applications of the subject of the data for loan reports to the Central Bank within three working days from the day of the reception of such applications. The loan report will be provided for the subject of the data who makes the request no further than five working days after the reception of the request by the Central Bank". The article in question limits the right to access on the subject's data after it ensures that such request should be reported to the Loan Registry and after the request has been accepted by the Central Bank, loan providers may secure a loan report of the subject of the data.
CBK's regulation does not manage to offer the citizens the right for additional information, as it is foreseen with the article 10.2.1 of the LPPD, for example such information as the receivers or the categories of the receivers of personal data. This means that a citizen must verify if the revelation was done for the loan provider in question, and verify if the controls to avoid an access to the loan information work properly.

The handling practices in this sector, which result from the agency's inspections, in particular in regards with the so-called Credit Score:

- Financial institutions are obliged to report to the CBK for every loan within 24 hours after the signing of the contract. This report is done online using the templates available on CBK web site.
- There are formal controls to verify the coherence of identity data, such as ID format, but there is no verification in regards to the accuracy of data, i.e. fake users, duplicated ID numbers, etc.
- No consent is taken from the subject of the data for data transferring, something similar to a "checkbox" which is collected by the provider of the loan which states that consent was taken.
- The department of complaints of CBK is responsible for citizens' rights and handles their complaints
- The complaints must be directed initially to the financial institution, and only in case of dissatisfaction of the citizen, he/she may complain to the Central Bank
- The request for access may be done in various ways; directly to the Central Bank, the loan providers branch, or through the web site of Central Bank
- Access to loan information from the subject of the data is secured for the last three months, and the subject of the data may have access on his data free of charge only once a year, while for more than once a year a fee is demanded.

Law enforcement authorities could be given access in the financial data of a given subject only through a court order. The new amendments that are being drafted, might guarantee this right for private executors as well.

In general we can conclude that the financial sector in Kosovo is managing to implement the law on personal data protection. According to the Agency, which has also inspected this sector, all the banks in Kosovo have put in place policies for handling personal data and have also appointed members of their staff for personal data protection.[18]

Although the law does not require standardization certification, the banks for instance have advanced in this regard, mainly because of the need to implement reporting requirements from the CBK, and because they are affiliated with regional/bigger banks, they are now certified on the security standard ISO 27 001 as well. Moreover all banking officials who in one way or another have access to personal data have a signed

18 Citation Inspection Support Office Coordinator NAPPD, April 2017

confidentiality statement or Non Disclosure Agreement. [19]

In case of suspicion of violation of the provisions of the law the NAPPD supervisors may impose temporary or permanent bans[20] on personal data processing if they cannot implement the necessary security measures or if there are any violation of law provisions on personal data protection. The supervisor may also ban international transfer of personal data in case of violation of the same principles. The latter one is especially important in the financial sector, which because of the nature of its licensed operators which are mostly foreign banks, and which often do not have a special IT for Kosovo, they do data transferring for their headquarters. This kind of transfer is also foreseen with the LPPD. In the past the agency has given opinions which have allowed such transfers. [21]

Collected personal data may not be stored for longer periods than it is necessary to achieve the aim for which the data has been collected or processed. In this case or after the expiry of the storing deadline, the data may not be stored in any form that enables the identification of the subject of the data, therefore they should be deleted, blocked, (in case they need to be available for execution reasons, or be stored to fulfill legal obligations related to archiving) and/or be anonymized properly in accordance with the security measures applied for personal stored data for longer periods and for historic, statistical, or scientific use [22].

Telecommunications sector

Because of the nature of their services, telecommunication service providers collect and process very sensitive information related to their customers. Considering the high popularity and utilization that

19 Inspection Support Office Coordinator NAPPD, April 2017
20 LPPD Article 49 Inspection measures
21 http://amdp-rks.org/?page=1,5,12
22 LPPD article 3.5

communication technologies have in our country[23] as well as the cases of leaked material drawn from communication interceptions, concerns are inevitable about security and the integrity of the communication services.

The nature of this data may vary from personal and identification information, to information on the traffic of our communication, location updates, as well as the content (following the law on interception of communications).

Because the telecommunication industry handles and transfers sensitive data, it is often target of cyber-attacks, which threaten the integrity and safety of networks as well as users' privacy. According to PWC Global State of Information Security 2016, last year incidents in the telecommunication sector have had an increase of 45% in comparison with the previous year. Both the operator's and the users' data are at risk from outside attacks. Some of the possible attacks are:

- DDoS attacks (Distributed Denial of Service)
- Abuse of sensitive hubs in the operator's network or in the end devices
- Compromising of subscribers through the so called social engineering, using various software. Phishing, or malwares
- Compromising and leakage of data by the network maintenance workers.

Law on Electronic Communications, specifically article 86, states that confidentiality of communication and traffic data in a public communication network and public electronic communication services, must be protected by the service providers.
All the operators are obliged to collect information on their subscribers in accordance with the user registration regulation; however, the Agency during an inspection done in 2011 has compelled mobile telephony operators to destroy the physical copies of customers' personal documents [24]. This is making telecom companies unable to evidence and correct mistakes on data entry is and is reported as one of the key problems by telecom companies in implementing the law on electronic communication and that of personal data protection.

23 80.6% penetration of the internet in households, 110.7% penetration of mobile telephony per inhabitant, RAEKP market report 2016

24 http://amdp-rks.org/?page=1,21&ddate=2011

According to the electronic communication law, and the recent regulation on technical and organizational standards on the Security and Integrity of Networks, approved in November 2016, RAEKP holds the economic operators responsible for the implementation and ensuring of security parameters, in order for the communication to be safe and users' privacy to be guaranteed.

The operators are compelled to notify the National Cyber Security Unit (KOS-CERT) for any incident that appears on their networks. Failure to report the incidents or wrong reports will be fined. The law on electronic communication compels the communication service providers to undertake previous measures to ensure the security, integrity and credibility of the communication service.

The service providers are obliged to prevent interception of communication, unless there is a court authorization to do such a thing for individual cases, always in accordance with the provisions of criminal proceedings code. No operator reports on systematic storing of SMSs or internet traffic.

Telecommunication operators state to have internal regulations on costumer's personal data exploitation, which are not public.
Collection and processing of data for any purpose by the operator may be done only with the customer's authorization. Companies include a paragraph in their contracts for subscribers and service users, through which they ask for customer's permission to use their data. However, none of them inform the customers on data treatment procedure. Among telecommunication companies, only IPKO has published their data protection policy on their web site.

Not all electronic communication providers have obtained the ISO certifications. IPKO is certified according to the ISO Standard 27000 and 27002, other operators claim that they implement the same practices, but without certification.
RAEKP may demand an audit from an independent subject, for instance in case of suspicion for violation of network security or services.
In the recent years there have been a history if incidents and abuses with personal data by the telephone companies, unauthorized usage, direct marketing etc. Sharing the data with third parties should be done only with the consent of the subject of the data and operators are obliged

to ensure the clients that their data will only be used for the purpose of their service also applies for this sector.
Regaining and building customers' trust may be done through additional efforts in these three directions:

- Ensuring that their data are on a high level of security and are protected from abuse
- Enabling the customer to have control on how their data will be used/exploited by the economic operators
- Ensuring that their data will not be used without their prior consent.

In the complaints directed to the Agency regarding suspicions of communication interception, the Agency has declared to not be competent to undertake any kind of action. According to the law on electronic communication interception in our country, a legal interception is considered only that for which a legal court order was issued by the competent court to authorize the interception [25].

The interceptions are supervised by the Interception Process Monitoring Commissioner, which is a mechanism within the institutional structure of the Judicial Council of Kosovo, which performs the annual check of the interception of communication legality in accordance with this law and reports to the Judicial Council of Kosovo and the State Persecutor on annually for identified violations[26] .

The data extracted from the interception of electronic communications may be stored in the Monitoring center, the Office of the State Persecutor, at Kosovo Police as well as in Kosovo's Intelligence Agency. The monitoring center and the state persecutor must destroy them no further than twelve months after the conclusion of investigations, while the police and the KIA should destroy the data no later than twelve months after the conclusion of investigations.
Network operators and service providers are not allowed to record, store or copy data of any call or message, they may store only meta-data for a maximum period of nine calendar months. In order to offer technical support foreseen by the law on interception, the assigned personnel from the company is authorized by the state persecutor to have access on the data. While the companies and the personnel have signed confidentiality agreements.

25 Law No. 05/L -030 Law on Electronic Communication Interception
26 Law no. 05/L -030 Article 32

Any interception which is made possible by the Liaison Office, Monitoring Center, a Network Operator and Service Provider is performed while respecting the confidentiality principle and the procedures with the law, in order that neither the target of the interception nor any other unauthorized person must be aware about the interception. [27]

All the data that are extracted during legal interception must be stored in a safe way, as required by the Criminal Code and the Law on KIA.[28]

The law on interception limits access which is allowed only for the persons who are directly involved in the investigation of the issue with which the data are related as well as with the individuals who are needed for the technical implementation of the legal interception order, and it states that only the data which are directly important for the official investigation and ongoing investigations may be stored.[29]

Privacy in the new media

Internet traffic monitoring

Modern web pages are continually increasing their user activity monitoring. Most of them have integrated tools, which trace and collect data on their visitors. Though collection mechanisms, they store, analyze and transform

27 Law no. 05/L -030 Article 20
28 Law no. 05/L -030 Article 25 1
29 Law no. 05/L -030 Article 25 2 3

the collected data into results in order to profile and know their user preferences better.

Examples of major user data analytic engines are Google Analytics[30] and Facebook insight[31] . Both these applications use cookies as a mechanism of collecting information, which are generated by the users/ subscribers. Moreover Google Analytics, offers tools free of charge for web pages which allow them to analyze their user traffic. Also for this service the platform uses cookies that are installed from the web page into the browser through a JavaScript code [32].

Cookies on the Internet

Most of the pages on the Internet use the so-called Cookies to analyze the user traffic that they attract. Cookies are data with small quantities of information, which are stored on the users' Internet browser. Which means that web page gives a cookie to its user (reader) when they visit it for the first time. With this cookie the page identifies the user (their IP address) and in this label is stores the data on the user's engagement with the content provided.

Cookies allow administrators to collect user preferences and trace their interaction with the content for a certain time [33]. The user may decide through their browser settings whether they want to accept them or not, and delete them whenever they want [34].

If authorized, cookies identify that a user has entered a page, trace their actions, and memorize their interaction data, which may vary in the nature of their use. The cookie transfer can also be done in an automatic manner.

In Europe, unlike other countries, the use of Cookies is allowed under certain conditions[35] , based on the legislation, which derived from the directive for ePrivacy 2009/136/EC [36], the guideline on data protection EC

30 Google Analytics: https://analytics.google.com/
31 Facebook Insights: https://.facebook.com/
32 http://javascript.about.com/od/reference/p/javascript.htm
33 Cookies in EU, http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm
34 Cookies in EU, http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm
35 Use of cookie in Europe http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm
36 EU ePrivacy: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0136

45/2001[37] and the directive 2000/31/EC[38] on E-commerce, although they include other technologies, it is referred to as the Cookie Law[39] as Cookies are most popular.

There are other applications such as advertising platforms and networks[40] , or open source content platforms[41] which use cookies to trace and memorize users' behavior. Among them is the Wordpress platform[42], which widely used in Kosovo as well, especially by the commercial sector.

In Kosovo, the web pages are not compelled to notify users when they are applying cookies, therefore they don't ask for their consent.

European Union web pages are obliged to follow the instructions on privacy and data protection[43] and inform the user that they will not be using unnecessary cookies during the collection of data. More specifically Article 5.3 of the directive on ePrivacy[44] requires prior consent, notifying the user through a pop up window to allow or deny the cookies. Which means that users should be asked if they agree on the use of cookies and similar technologies before the data collection begins[45].

Furthermore, web pages owners/administrations, if they collect information from the users and share them with third parties, they are obliged to notify the user, as well as give them the option of their deactivation if they do not agree to be subject of data collection.
After the adoption of directive on ePrivacy as a form of constrain web pages to be more open with their users about the technologies they use during data collection, concerns have been raised among organizations which generate content on the internet on how they can apply the rules on cookies[46]. However notification windows are now common on EU, with explanations in the terms and conditions of service, as well as in the web pages' privacy policies.

As an illustration below an example of such notification:

37 EU Data Protection: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:EN:HTML
38 EU directive on E-commerce: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031
39 Cookie Law: https://www.cookielaw.org/the-cookie-law/
40 Advertising platform: https://www.google.com/adsense/start
41 https://wordpress.org/
42 Open Source: https://en.wikipedia.org/wiki/Open-source_software
43 Privacy and data protection in the EUhttps://secure.edps.europa.eu/EDPSWEB/edps/EDPS
44 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML
45 EU legislation on cookies: http://ec.europa.eu/ipg/basics/index_en.htm
46 Examples of placements of cookies https://econsultancy.com/blog/63118-17-useful-examples-of-eu-cookie-law-compliance/

The news portal bild.de[47] in Germany explains the use of cookies and data collection technologies and notifies each first visitor on its service terms and conditions and privacy policies. Among other things in this information is included:

- Ways how the users can use their online services
- Privacy policies
- Purpose of the collection of user's data
- Technologies and cookies which are used to collect user data
- Which information are collected from the users
- Which third party application they used for their services
- Cases which the data is shared with third parties
- Information on why these data are shared with third parties
- Information on how to deactivate cookies

Reaction mechanisms

Procedures on blocking content of IP addresses require action from Computer Emergency Response Center KOS-CERT, a functioning unit within the REACP that serves as a national focal point on coordination and management of network incidents in Kosovo. KOS-CERT's main purpose is to face the risks in electronic communication systems in our country. KOS-CERT must keep the community informed on potential risks and when possible to inform about the types of risks before they happen.

On violations of privacy with published content, involving criminal acts, the laws in place are Criminal Code as well as the law on combating and prevention of cyber-crime, whereas the competent authority for reaction is Kosovo Police, specifically the sector on cyber-crimes within the Kosovo

47 Bild.de: http://.bild.de/corporate-site/datenschutz/datenschutz/artikel-datenschutz-2952512.bild.html

Police

> If regulation is to do any good, it must address harms caused by the use of information. P. H. Rubin & T. M. Lenard "Privacy and the commercial use of personal information" 2002

In ty
in RT
w RT
web page as well. Reporting to this unit of RAECP is a legal obligation for the operators, in accordance with the law on electronic communications. However operators may block content or IPs only with orders from the persecutor's office.

KOS-CERT is authorized to treat all kinds of incidents of computer security, which happen, or threaten to happen in cyber community. The level of support from KOS CERT varies depending on the type and gravity of the incident or the issue, the size of the community, the affected users, and current resources of the KOS CERT.
Nonetheless, no direct support is foreseen for the end users, they are expected to contact with the system's administration, network administrator or their ISPs for help. KOS-CERT then supports them with coordination and incident management. This is defined with the RAECP regulation[48] on network security.

Network operator Vala reports 25 cases of complaints[49] for violations of privacy during the year 2016. While the operator Ipko declares that it didn't have any[50] complaints on violations of privacy in the past 9 years.
During the entirety of last year only one IP address was blocked with the order by the general persecutor.

Controversial cases

Promotional messages – Direct marketing

Unauthorized promotional messages and direct marketing are some of the issues that seam to raise most concerns in the public.
According to the law on privacy protection[51], the company/controller may use only personal data collected in accordance with paragraph 1 for direct marketing. This data includes first names, permanent or temporary residence address, telephone number, email address, and fax number.

48 Regulation no.29 Technical and organizational standards on the security and integrity of networks and/or electronic communication services, article 3
49 Interview with Vala, Personal data protection officer, April 2017
50 Interview with Ipko, Personal Data protection officer, April 2017
51 LPPD, article 59

With prior consent of the subject of the data, the data controllers may process other personal data, however, they may process sensitive personal data only if they have written consent

There is a known case of the violation of the privacy of a mobile phone user: when a company has taken advantage of an agreement with the operator Ipko, and the contract with PTK/VALA, in which case the Agency, and afterwards also the Basic Court in Prishtina, have found that the company had committed misdemeanor according to article 59, paragraphs 1 and 2, and it was fined in accordance with article 82, paragraph 1 of the Law on personal data Protection 03/L-172.

The inspection from the Agency was done after some received complaints for SMSs which were sent without prior consent of the citizens (the data's subject). The company "Marketing Online-KS" was fined with 5000 Euros.[52]

Direct marketing is allowed only when personal and contact data is collected through legal means, in addition it requires a clear and written consent from the data subject. In order to comply with the LPPD requirements, companies should include more information on data processing for marketing. Consent forms should include optional subscription to marketing services.

Opt-in example (good practice)
"Tick if you would like to receive information about our products and any special offers by post ☐ / by email ☐ / by telephone ☐ / by text message ☐ / by recorded call ☐"

53

Collecting of fingerprints

Another case that has raised concerns among citizens was the use of biometric information for identification, precisely the identification

52 http://www.amdp-rks.org/?page=1,10,184#.WSw0NFKB2Rs
53 https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf

through fingerprints used by companies in the country. According to LPPD fingerprints are considered biometric data, and private subjects may use biometric characteristic only if it is unquestionably required for people's security, property security and protection of confidential data or business secrets. If this is achievable with easier tools, an exception is when the use of these data is done when crossing state borders[54] .

In any case, the subjects (besides when collection is allowed by law) should ask for prior consent from the agency to start using biometric data. The agency has given permission to use biometric data in some cases, including the use in a fitness center, after verifying that the data will not be stored or processed in the center, but only in the equipment that is distributed to the subscribers[55] .

Unnecessary collection and processing of biometric information, in particular when combined with a weak security of ICT infrastructure creates ground for sensitive privacy violations. Users should make sure these data is processed with the highest security and only when unquestionably required for people's security, property security and protection of confidential data or business secrets, as defined by the LPPD.

An example of detailed consent form is below:

54 LPPD article 66
55 Citation ALPPD, the exterior affairs official

Personal Data Protection (PDP) Customer Consent Form

Please allow up to 30 calendar days for processing from date of receipt.

1. I hereby agree and consent that X Company (" Xcompany ") may collect, use, disclose and process my personal information set out in my application form, account opening documents and/or otherwise provided by me or possessed by X, for one or more of the purposes as stated in X's Personal Data Protection Terms and Conditions, which in summary includes but is not limited to the following:

   (a) processing my application for and providing me with the services and products of X as well as services and products by external providers provided through the company;

   (b) administering and/or managing my relationship and/or account(s) with X; and

   (c) sending me marketing, advertising and promotional information about other products/services that X, X's affiliates, business partners and related companies may be offering, and which X believes may be of interest or benefit to me ("Marketing Messages"), by way of postal mail and/or electronic transmission to my email address(es);

   Opt Out for subclause (c)
   Please be informed that you have the right to opt out of receiving Marketing Messages. Kindly visit www.Xcompany.com.rks for further details on how you may exercise your right to opt out of receiving Marketing Messages. Kindly note that if you do not exercise your right to opt out of receiving such Marketing Messages, you will be deemed to have consented to the receiving of such Marketing Messages by X, X's affiliates, business partners and related companies and X, X's affiliates, business partners and related companies will continue to provide such Marketing Messages to you.

   (d) sending me marketing, advertising and promotional information about other products/services that X, X's affiliates, business partners and related companies may be offering, and which company X believes may be of interest or benefit to me (the "Marketing Purpose"), to my telephone number(s) (as set out in my application form, account opening documents and/or otherwise provided by me or possessed by X) by way of:

   ☐ voice call/phone call*
   ☐ SMS/MMS (text message)*
   ☐ email

   Opt In for subclause (d)
   *If you AGREE AND CONSENT to X, X's affiliates, business partners and related companies and their third party service providers processing your personal data for the Marketing Purpose and contacting you as described in this subclause (d), indicate your preference for the mode of communication and consent by inserting a "☒" in the box.

   Note: Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, cons ectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat

   (collectively the "Purposes ")

2. My personal data may/will be disclosed by to its third party service providers or agents (including its lawyers/law firms), which may be sited outside of Kosovo, for one or more of the Purposes, as such third party service providers or agents, if engaged by X, would be processing my personal data for X for one or more of the Purposes.

3. By signing below, I represent and warrant that I am the user and/or subscriber of the telephone number(s) as set out in my application form, account opening documents and/or otherwise provided by me or possessed by X, and that I have read and understood all of the above provisions, including the Personal Data Protection Terms and Conditions.

I have read and agree to the above.

Name:

Date:

The data business, loyalty cards

The loyalty cards business in Kosovo remains underexploited, therefore the handling of data in these loyalty programs is expected to become more important or customers, with the greater inclusion of clients.

In the past two years loyalty cards have appeared mainly in the supermarket chains, and judging by the little offers by merchants and low popularity, neither the merchants nor the customers seem to value them that much. While for citizens as expected discount of prices are their main motive for using them, which currently may be collected in the form of a bonus, meaning that the citizens are encouraged to spend more; in this way they collect bonus points, which after a while may be used to make purchases at the same business, or be rewarded a price-gift in exchange for their bonus.

There is a business that is fully oriented in the data market, which is called ManaCard. Even though, the business model of this company seems to be mixed with traditional marketing and is unclear. In regards to personal data, this card collects information on customers which is shared with other partnered businesses, in exchange it allows cardholders to benefit from dedicated discounts.

It is worth mentioning that in the conditions of the use of this card[56] there are no clarifications in regards with the collection and processing of data by the company, and it does not refer to the LPPD. In this case the asymmetry of information between the company and the customer is very high.

New technologies for better privacy protection

Besides enforcing and implementing the regulations, technology itself can play an important role in protection and implementation of these regulations. Through technology and careful its design, unnecessary access, collection and further processing of personal data, in favor of

56 https://mana.cards

protection of individuals' privacy can be limited. The companies, however, oftentimes hesitate to implement such measures because of the impact in operational costs.

The main issue in regards with the treatment of personal data in Kosovo remains the indiscretion of the personnel who has access in personal data. In this point the citizens, through the supervisory authorities (market regulators and NAPPD) must influence the companies to implement limited and authorization only access in the personal data they collect. In addition ask for the implementation of higher security and ethical standards in handling personal data.
The software itself allows the application of a set of procedures and functions with the aim of tracking user access. Some of the procedures and measures necessary to protect information of personal data (which in literature is referred to as data protection and information security) are:

- Protection and control of access in facilities and equipment (software systems)
- Protection of used applications on personal data processing
- Prevention of unauthorized access in personal data stored or transmitted (protection of network integrity)
- Ensuring of efficient methods of blocking, destruction, deletion or anonymization of personal data
- Updating of procedures and measures of achieving an appropriate level of personal data protection
- Raising awareness for the executives, employees and persons who work with data processing on security measures (technical and organizational) and their obligation on maintaining confidentiality even after their contractual relationship with the data controller ends (the obligation to secrecy)

Recommendations

The Agency should resume its functions, in particular in inspecting activities. For this to happen amendments to the Legislation which includes the Law on access to public information and the Law on personal data protection should be concluded as soon as possible.
The Agency must continue to offer support on the implementation of the

LPPD for instructions and public, but in particular should start providing support for health care units. Agency should extend this support in the form of clear instructions especially for the smaller health care units, which do not possess large capacities to properly handle personal data. These instructions should include collection and processing procedures of personal data, as well as guidelines for timeframes for storing data.
All the private subjects should increase their transparency in regards with treatment of personal data, the Agency can help by offering support on compiling written consents, which must be clear for the citizens.

Hospitals and other health care centers must raise the awareness of personnel in regards with respecting patient confidentiality. Even though currently the hospitals and other healthcare centers deliver almost no information on the treated patients (except with the cases of contagious illnesses or IVF), the Law on Health foresees this reporting, therefore the Agency in cooperation with the Ministry of Health as well as other institutions should prepare healthcare units to compile this information without violating the patients' privacy.

The Agency should increase supervision for healthcare service providers as well as insurance companies to ensure protection of citizens' privacy.
Ownership of data should be reviewed ensuring that patients have more control on the processing and collecting of their data, in particular by health care sector where the law defines the institutions as owners.
Similarly, for financial and insurance institutions, ownership and access to personal information should be facilitated without the additional fees that are currently in place.

Citizens' complaints should not be directed initially to the private body so that only in case of dissatisfaction of the citizen, he/she may complain to the oversight authorities. Regulatory bodies should exercise this function, facilitating exercising privacy rights for citizens.
Classification of personal data and the subjects should be done in order to avoid unnecessary collection and processing of personal data.
Communication of companies with citizens should increase in regards with attacks or attempts of electronic communications network integrity violation, in order for the citizen to be informed and to know how to update and how to back-up their data.
Emergency reaction units as well as Internet service providers, including those who provide content, must communicate the reaction procedures

in case of privacy violations.

It is recommended that operators (ISPs) and law enforcement bodies create a quick reaction team, in order to react by closing the possibilities of personal data being shared on the internet. In this case the involvement of the state persecutor, the police, RAECP and ISPs is required, all of which seam to have the technical knowledge as well as the connection with the aforementioned bodies, this function may be performed by the existing CERTs and it would protect citizens from abuse with content in cases of privacy violation.
The companies must implement limited access and with required permissions in personal data, as well as implementing higher standards of security and ethics during the treatment of personal data. Citizens and regulators can play a role by demanding more attention from the data controllers.

Companies that deal with direct marketing should be more careful when obtaining personal information, they need to notify the citizens about the treatment of their data as well as guarantee temporary or permanent interruption of marketing any time the citizens demand it.
Web pages in the country should be obliged to notify the visitors on the usage of cookies. For this reason it is necessary to adopt the EU legislation. Furthermore, in order to further strengthen the role of the agency and the raising of its capacities, it is recommended that the Convention 108 on Protection of Individuals in Case of Automatic Personal Data Processing should be ratified.

References

1. 1P. H. Rubin & T. M. Lenard “PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION” 2002
2. https://www.privacyinternational.org/node/44
3. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/guide_org/
4. https://www.gov.uk/government/uploads/system/uploads/

attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf
5. http://www.amdp-rks.org/repository/docs/ashmdhp_raporti_vjetor_2015_ALB.pdf
6. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/435817/The_commercial_use_of_consumer_data.pdf
7. http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=3137&context=facpubs
8. https://www.privacyinternational.org/
9. http://www.coll.mpg.de/sites/www/files/text/burkert.pdf
10. http://www.acma.gov.au/~/media/mediacomms/Research%20library%20reports%20old/pdf/attitudes_towards_use_of_personal_info%20pdf.pdf
11. http://www.acma.gov.au/~/media/mediacomms/Research%20library%20reports%20old/pdf/attitudes_towards_use_of_personal_info%20pdf.pdf
12. https://www.wired.com/2017/04/stronger-privacy-laws-save-advertising/?mbid=social_fb
13. http://www.legisquebec.gouv.qc.ca/en/showdoc/cs/P-39.1
14. https://www.fff.org/2014/03/04/private-vs-government-data-collection/