Project implemented by Human Dynamics in association with:
IPS Institute
AlmavivA S.p.A.
Czech Office for Personal Data Protection OPDP
Privacy International

Project office:
Directorate for Personal Data Protection
10, Samuilova 10,1000 Skopje
Tel: (+389) 2 3230 635
Email: ipa_dzlp@dzlp.mk

Document 2.1.4 - 10

GUIDELINE FOR PROCESSING OF PERSONAL DATA IN THE ELECTRONIC COMMUNICATIONS SECTOR

Component 2
Activity 2.1.4 - 10

The content of this report is the sole responsibility of Human Dynamics and can in no way be taken to reflect the views of the European Union

Support to the Directorate for Personal Data Protection
This project is funded by the European Union

Table of Contents

I. INTRODUCTION

What is the purpose of this Guideline?

The purpose of this Guideline is to summarize the basic personal data processing principles and rules in a user-friendly manner and to provide instructions and advices for the citizens in order to improve the exercising of their personal data protection's right. The information contained in this Guideline will help the target group to better understand and exercise their data protection right in the electronic communication sector.

Who are the addressees of this Guideline?

The Guideline is primarily designed to be a used by the citizens who are subscribers and users of electronic communication networks and services. The Guideline aims to educate the subscribers and users to recognize whether their personal data is handled lawfully. In addition, operators and service providers of public communication networks and services (hereinafter: operators and providers) who process personal data of their subscribers and users may also find this Guidelines useful.

How is the Guideline structured?

The Guideline is written in a way to include the most relevant legal provisions and the frequent issues that citizens face with when their personal data is processed in the electronic communication sector. The first part of the Guideline presents and explains the most relevant personal data terms and principles, which apply "universally". The main part is dedicated to the legal obligations for those who process data in the electronic communications sector and the corresponding rights of the subscribers and users of their services. At the end of this Guideline, useful information on exercising subscriber's and users' rights is given, including a template used for that purpose.

II. KEY NOTES ON PERSONAL DATA PROTECTION

Why is protection of personal data important?

Nowadays, citizens' right to privacy and personal data protection is rightly seen as one of the most significant human rights. It is recognized and valued worldwide. Therefore, this right has been set in the Constitution. **Article 18 of the Constitution guarantees the security and secrecy of personal data!** In addition, it guarantees to the citizens protection from any violation of their personal integrity deriving from the registration of personal information through data processing. The protection extends to all areas of life of the citizens (private, professional, health services, public administration, etc.).

Huge number of persons is not aware yet of the importance of practicing and protecting this right! Many entities that collect and process data are not aware of the measures they need to take in order to protect the personal data. Sometimes, they collect personal data without legal basis or without clearly and freely given consent of the citizens. Moreover, citizens provide their personal data and agree to be publicly disclosed, although in many cases they are not bound to do so or not aware of the consequences of doing so.

Electronic communication is an area where various personal data is processed! Almost every citizen in the country is user of electronic communication services, thus becoming personal data subject. There are more than 100 national and local operators and providers (land line and mobile telephony operators, internet service providers, cable TV providers, etc.) who collect and process personal data. Subscribers and users of their services reveal personal data when they conclude contracts to become subscribers of post-paid mobile telephony or cable TV. Users by surfing the internet create cookies - files that reveal certain personal data to the Internet Service Provider and web site owner. As of all these reasons, rules pertaining to personal data processing must be well known to all, obligations must be followed by operators and providers and rights exercised by the subscribers and users.

What is the meaning of the most important personal data and electronic communications terms?

In order for the readers to get familiar with the personal data processing rules in e-communications sector and their rights in that respect, they need to understand the meaning of

the commonly used terms in these two areas. Each legal definition is followed by an example.

"Personal data" is any information pertaining to an identified or identifiable natural person, the identifiable entity being an entity whose identity can be determined directly or indirectly, especially as according to the personal identification number of the citizen or on the basis of one or more characteristics, specific for his/her physical, mental, economic, cultural or social identity. ***In the area of electronic communications the most frequent type of personal data collected from the subscribers and further processed by operators/providers are: name, address, phone number, e-mail address, etc.***

"Special categories of personal data" are personal data revealing the racial or ethnic origin, the political views, religious or other beliefs, membership in a trade union and data relating to the health condition of the people, including genetic data, biometric data or data referring to the sexual life; therefore are subject to special restrictions on their processing. ***In the area of electronic communications these types of personal data of the subscribers are not processed, at least not by the operators/providers.***

"Personal Data Subject" is any natural person (citizen) to whom the processed data refer. ***In the area of electronic communications, personal data subjects are the subscribers and users of services.***

"Consent of the personal data subject" is freely and explicitly given statement of will of the citizen whereby s/he agrees to the processing of his/her personal data for previously determined purposes. ***In the area of electronic communications, templates of contracts and requests (should) contain provision which gives a choice to the subscriber to agree on personal data processing.***

"Controller of the Personal Data Collection" is any natural person or legal entity, a state administration body or other body, who, independently or together with others, determines the purposes and the ways of personal data processing (controller). ***In the area of electronic communications controllers are: landline and mobile phone operators, Internet Service Providers (ISP), providers of transmission of radio and TV signals to end users (cable TVs), etc.***

"Personal Data Collection Processor" is a natural person or a legal entity or a legally authorized state administration body processing the personal data on the behalf of the controller. ***In the area of electronic communications, those who control data also process data. In addition, other parties may also process data on behalf of operators/providers.***

"Personal data processing" is any operation or a sum of operations performed on personal

data, automatically or otherwise, such as: collection, recording, organizing, storing, adjusting, or altering, withdrawing, consulting, using, revealing through transmitting, publishing or making them otherwise available, aligning, combining, blocking, deleting or destroying. ***In the area of electronic communications, concluding and storing subscriber contract or placing the subscribers data in the phone directory are deemed as personal data processing operations.***

Definitions of the most important **e-communication terms,** such as operator, provider, electronic communication network and service, can be found at: http://www.aek.mk/index.php?option=com_glossary&lang=mk

III. OPERATORS/PROVIDERS OBLIGATIONS AND SUBSCRIBERS/USERS RIGHTS REGARDING PROCESSING OF PERSONAL DATA IN THE ELECTRONIC COMMUNICATION SECTOR

How is the personal data collected and what should the subscriber/user be informed about?

Operators/providers should ensure that **collecting data is done in a fair manner** and that subscriber's right to information is secured. Subscribers and users should know that **when their personal data are collected information must be provided, at the time of conclusion of the contract/provision of the service, on the:**

- identity of the operator/provider (e.g. company name and seat) and of its authorized representative;
- purposes of the processing;
- users or categories of users of personal data;
- intention to communicate data to third parties, including types of recipients, purpose for which the data will be disclosed and right of the subscribers to object to from disclosing for specific purposes (e.g. for direct marketing);
- compulsoriness of responding to questions and possible consequences of not responding (unnecessary questions should not be asked); and
- existence of the right to access and the right to correct personal data.

In addition, **subscribers may at anytime request from the operators/providers information**:

- whether their personal data are being processed;
- on the purposes and legal base for personal data processing and the users or categories of users to whom the personal data are being disclosed;
- on the logic of automated processing in case such processing is applied.

When should the subscriber be informed and its consent given for specific data processing?

When operators/providers want to process subscribers' or users' data they must inform them and/or obtain their consent for personal data processing. The **subscriber must be informed on**

collecting and/or processing of data in the following circumstances:

- at the time of ***concluding subscriber contract*** – e-communication service (e.g. cable TV) will be provided if there is contract concluded between the provider and subscriber;

- for the ***type of traffic and location data to be processed*** and the duration of such processing, including the possibility that location data may be transmitted to third parties for the purpose of providing the value added service; and

- on the ***purposes of the Overall Directory*** and of the use of such data.

Subscriber's **prior freely and clearly given consent on collecting and/or processing of data must be required** and right to withdraw the consent must be given in case of:

- processing of traffic and location data; and

- unsolicited communication - automated calling systems for making calls (opt-in) and direct marketing (opt-out).

What type of subscriber data may be collected and/or published by the operators?

Operators/providers may obtain and store only those **data on their subscribers**, which are prescribed in the law, and the data may only be used for:

- concluding, monitoring and termination of subscriber contracts;

- billing for services; and

- preparation and issuing of subscriber directories.

On termination of a subscription, these data must be stored for:

- one more year from the date of issuance to the subscriber of the latest bill for services provided; or

- if during this period an order is issued by the competent body for the storage and transmission of such data, for the period stipulated by the order of the competent body.

***Collecting personal data**, including PIN for the purposes of concluding contract is legally based, but collecting and storing a copy of ID card and M1/M2 form as employment prove is not legally based, it is too excessive requirement and it might not be a full prove of the identity and employment status (fake ID card and M1/M2).*

***Processing of personal identification number of the citizen (PIN)** as a special category of personal data, may be carried out only:*
- if prior explicit consent is given by the subscriber;
- for the realization of the rights and obligations of the subscriber or the operator/provider, and
- in other cases stipulated by law.

What type of communication data are subject to protection?

There is specific type of data in the e-communications sector that relates to the privacy of the subscribers and users. So, in addition to the usual personal data that is subject of protection (name, address, PIN), the **following sector-specific types of communication/data** are protected:

- content of communications (including URL) – e.g. phone conversations, e-messages (e-mail, SMS), etc.

- traffic data and location data relating to communications – e.g. phone numbers dialed or received, visited web sites, location where the call was made from; and

- unsuccessful attempts to establish a connection – unable to reach a subscriber or to visit web site is also recorded and protected.

*Computers that are connected to the internet are assigned **unique identifiers known as Internet Protocol (IP) addresses** to identify and communicate with each other. The most common type of IP address is displayed as four numbers between zero and 25 (e.g. 83.29.144.255). An IP address in isolation is not personal data. But an IP address can become personal data when combined with other information or when used to build a profile of an individual, even if that individual's name is unknown.*

All forms of surveillance, interruption, recording, storage, transfer and diverting of communications and data are prohibited, except in cases where it is necessary for the purpose of conveyance of a message as a fax message, e-mail, e-mailbox, voice mail, SMS message, and when it takes place in the context of lawful interception of communication by specially entitled authority such as the Ministry of Interior with a previously obtained court order.

Are there cases where operator/provider can process confidential information?

Operator/provider may obtain, use or provide confidential communications information to others only to the extent essential for the provision of specific public communications services. If operators/providers need to obtain information on the content of communications, or copy or store communications and related traffic data, they must:

- inform the user, and

- erase the information on the content of communications or the communications, as soon as technically feasible, after the information or communication is no longer required for the provision of the specific public communications service.

If operators/providers want to use the network to store data or to gain access to data stored in the terminal equipment of subscribers or users for further processing, then it is only permitted if they:

- inform in advance the subscriber or user of the purpose of processing of such data;

- give the subscriber or user the right and opportunity to refuse such processing; and

- provide the subscriber or user with a designated point of contact to which to communicate such refusal.

Storage of or access to data is permitted for the sole purpose of faster carrying out the transmission of a message over an electronic communications network, or if essential for the provision of an information society service which the subscriber or user explicitly requested.

When are the subscribers and users allowed to record communications?

Subscribers or users may record communications, but in such case they must:

- inform the sender or recipient of the communication thereof, or

- adjust the operation of the recording device so that the sender or recipient of the communication is informed of its operation.

The objective behind permitting recording of communications and the associated traffic data is to secure evidence of market transactions or any other business communications, or within organizations receiving emergency calls, for their registration, identification and resolution.

Is the video surveillance and audio recording by the operators/providers permitted?

Some digital and cable TV providers have placed cameras on public places through which 24/7 broadcasting is enabled (online or through special TV channel). **They are allowed to do so only if the following conditions are met**:

- faces of the persons that appear on the screen must be disguised which can be done by using a special software, or

- system to be configured so that the recording is with lower resolution, thus making the people faces unrecognizable.

Most of the operators/providers have call centres with the purpose of providing answers and information to their subscribers. If these centres conduct audio recording of the calls, they must inform the caller on the recording and purpose of the recording (e.g. assessment of the service quality).

What are the operator/provider obligations in regards to traffic communication data?

Subscribes and users should be aware that operators and providers are obliged **to keep unprocessed the traffic data for the last 24 months** and only in the country. This is required because of the possible investigations carried out by the law enforcement authorities. In addition, they may also **store and process traffic data required for billing and interconnection payments** until payment for services. This is done to protect operator's/provider's business interests. Operators and providers are obliged to stipulate in the subscriber contract the manner of storage, duration and processing of traffic data.

What are the operator/provider obligations in regards to the location data?

Location data define the geographical location of the terminal equipment of a user of electronic communications service. Location data relating to users or subscribers may be processed only:

- in anonymous form,

- on the basis of a prior consent by the user or subscriber, and

- to the extent and for the duration necessary for the provision of a value added service.

Users or subscribers who have consented to the processing of location data must have the possibility, using simple means and free of charge, of **temporarily refusing the processing of such data** for each connection to the network or for each transmission of a communication.

Processing of location data without the data may be transferred to third parties providing value added services, while the location data referring to emergency call numbers must be supplied to the competent body responding to emergency calls (e.g. Emergency Medical Help, Police, etc.).

What are the subscribers rights in relation to the calling and connected line identification?

Operators and providers are obliged in their general conditions for conclusion of subscriber contracts to determine the possibility of presentation and prevention of calling and connected line identification.

The following must be provided by the operator/provider to the calling user before each call:

- possibility, using simple means and free of charge, of preventing the presentation of the calling line identification (phone number will not show on the display of the phone device), and

- automatically and free of charge to prevent the identification for all calls from their lines.

Operators and providers are obliged to override the prevention of calling line identification for emergency calls.

The following must be provided by the operator/provider to the called user before each call:

- possibility, using simple means and free of charge, of preventing the presentation of the calling line identification,

- if the identification is possible prior to the line being established, the called subscriber must have the possibility, using simple means, of rejecting incoming calls where the calling line identification has been prevented by the called user or subscriber,

- enable the called user, to use the possibility, using simple means and free of charge, of preventing the connected line identification to the calling user.

If a subscriber receives malicious or nuisance call, then he/she may request in writing that the operator trace such calls, In such case, the operator/provider may temporarily record the origin of all calls ending in the network termination point of such subscriber, including those for which prevention of calling line identification has been requested. Data on tracing must be stored and supplied to the subscriber who requested tracing of malicious or nuisance calls and the same are also delivered to the competent body (Ministry of Interior).

What are the subscribers' rights in regards to the automatic call forwarding?

Subscribers must have the possibility, using simple means and free of charge, of stopping automatic call forwarding by a third party to their terminal equipment, only if the implementation is technically feasible or would not cause disproportionate costs.

What are the subscriber's rights in relation to Overall Phone Directory?

Overall Phone Directory is a collection of personal data that is publicly available with the aim of helping the users of voice telephony to find the phone numbers.

- Subscribers to publicly available telephone services have the **right to an entry** in the Overall Phone Directory.
- All end users such services **must have access** to the Overall Phone Directory.

If the subscriber wants its personal data to be entered in the Directory that does not mean that all the data should be available to the public (entered in the Directory). Subscribers must be informed and given the opportunity to determine the personal data that will be included in a public directory. Refusal to be included in a public directory, and verifying, altering or erasing personal data shall be free of charge.

Who is entitled to process personal data within the operator/provider?

The obligation to protect confidentiality and privacy of communications refers to all operators' and providers' agents, employees, representatives, and other parties under their direction and control. All these persons have to be introduced with the principles for personal data protection prior to accessing the personal data. Operators/providers are obliged to keep records for persons authorized for providing personal data processing.

A phone operator has recently sent SMS to its subscriber indicating that his personal data (name, phone number) must be entered in the Overall Phone Directory. Subscriber has a right to an entry in the Directory, not an obligation.

IV. USEFUL ADVICES ON EXERCISING THE SUBSCRIBER'S/USERS' RIGHTS

What rights does the subscriber/user have in regards to the data changes?

Upon the request of the subscriber or if operator/provider determines on its own, the operator/provider must supplement, amend, delete or prevent the use of the personal data, if they are incomplete, incorrect or not updated and if their processing is not in conformity with the law.

Who should the subscriber turn to in order to exercise the rights?

Right to object to the processing of his/her data shall be exercised in the first instance before responsible person/officer of the operator/provider. The responsible person/officer must implement procedures that enable rights to be exercised in a simple, fast and efficient way, which do not entail undue delay or cost (respond to the request must be given within 15 days). When a responsible person concludes that exercise of rights is not justified, the subscriber should be informed of the reasons that led to this conclusion.

How can the right to complain be exercised?

If the client is not satisfied with the responses and information given by responsible person/officer within the bank, and considers that his/her rights are violated or information provided insufficient, s/he can submit a request to the Directorate for Personal Data Protection (DPDP) for confirming violation.

How to submit complaint for personal data protection?

It's very easy and simple. Whenever one believes that her/his right of personal data protection is violated and has some facts or prove for the violation, s/he can submit to the Directorate for Personal Data Protection:

Request (complaint) for determining a violation of the right of personal data protection or
Initiative to the the Directorate to perform inspection over the personal data processing performed by the controller of personal data collection.

In order to facilitate these procedures, the Directorate has developed forms of Request (complaint) and the Initiative for performing inspection, which are published on the Directorate's web site (www.dzlp.mk/mk/prijavi zloupotreba).

DPDP inspectors in conducting inspections have noticed the following activities of the operators/providers which are not in compliance with the law:
- Operators do not keep records of the persons authorized to process personal data
- Internal acts of the operators establishing technical and organizational measures for providing secrecy and protection of personal data are not fully in compliance with the law
- contracts contain father name and ID card number of the subscribers, without having legal basis for that.

What is the role of the Directorate for Personal Data Protection?

For the purpose of supervising the lawfulness of the undertaken activities while processing and protecting personal data, a DPDP is established as an independent state body. DPDP main tasks that are of interest for the subscribers/users of e-communication services are the following:

- resolving subscribers' complaints for violation of their data protection rights; and

Inspectors may, within the inspection supervision, among other measures order:

- blocking, deletion or annihilation of the personal data;

- completion, updating, correction, revealing or providing personal data secrecy;

- implementation of additional organizational and technical measures for securing secrecy and protection during the personal data processing; and

- prohibition for further personal data processing.

In addition to this, DPDP has and awareness raising and advisory role and for that purpose provides guidance on the protection of personal data and conducts training to the interested parties, especially data controllers and processors.

To find out more about the work of DPDP and other useful information relating to personal data protection, please visit the following web site: http://dzlp.mk/mk