INSTRUCTION

No. 14, DATE 22.12.2011

"ON THE PROCESSING, PROTECTION AND SECURITY OF PERSONAL DATA IN THE PUBLIC ELECTRONIC COMMUNICATION SECTOR"

Pursuant to article 30 and letter (f) paragraph 1 of article 31 of law no. 9887, dated 10.03.2008 "On the Protection of Personal Data", the Commissioner:

INSTRUCTS

Article 1

Scope

This instruction applies to the circulation and location of data in these two entities: legal entities and natural persons as well as, with the necessary data regarding the identification of the registered subscriber or user.

This instruction does not apply to the content of electronic communications.

Article 2

Purpose

The guideline aims to ensure an equal level of protection of fundamental rights and freedoms and in particular the right to privacy, taking into account the processing of personal data in the electronic communication sector and to guarantee the free movement of data and of electronic communication services equipment in the country.

Article 3

Specific, clear and legitimate purposes

Controllers who receive personal data from a data subject clearly state that they have to fulfill one or more specific legitimate purposes. Collecting data routinely and indiscriminately is illegal.

Article 4

Further processing

1. Controllers who collect data for one or more legitimate purposes may not use it for any purpose other than that for which it was collected.
2. Similarly, telephone service providers hold personal data for the purpose of providing a telephone service to subscribers and functions related to telephone bills, line repairs. They are required to maintain the movement and location of the data for up to two years.
3. In case a subscriber terminates the relationship with a telephone service provider, the service provider cannot process the subscriber's personal data, for direct marketing purposes. The only exception is when before the termination of this relationship, the subscriber has clearly given his consent for the maintenance of such contacts.

Article 5

Sufficient, appropriate and non-redundant data

1. Controllers must set specific criteria to assess what is appropriate, sufficient, and not excessive, and these criteria apply to any data processing.
2. Controllers do not collect or hold personal data that they do not need, arguing that the data may be used in the future.

Article 6

Data protection principles

1. Service providers ensure that, in the public electronic communication available, security principles apply to the data to be stored as follows:

a) the data retained should be of the same quality as the data on the network and the entities enjoy the same security and protection of their data;
b) data to be subject to appropriate technical and organizational measures for their protection against accidental or illegal destruction, accidental loss, unauthorized storage or unauthorized processing, use and detection;
c) the data to be subject to appropriate technical and organizational measures to ensure that they can only be accessed by authorized personnel; and
d) data, other than those available and stored, should be destroyed at the end of the storage period.

Article 7

Use of data for direct marketing

1. The use of automated call system without the intervention of the individual, fax machines or e-mails for direct trading purposes is only permitted only with respect to subscribers who have given their prior consent.
2. Notwithstanding paragraph 1, when a natural or legal person receives from the subscribers electronic data for e-mail, in the context of the sale of a product or service, the same natural or legal person uses these electronic contact details for direct marketing of products similar or its own services, provided that subscribers are given the opportunity to clearly and visibly, free of charge, to initially refuse such uses.
3. The data, in relation to subscribers (natural persons), processed within electronic communication networks that contain data on private life are stored to the extent and time necessary to provide the service for the purposes of the law and for liaison payments.
4. Any further processing of such data by the provider of electronic communications services available to the public, for the marketing of electronic communications services or to ensure the added value of the services, is permitted only if the subscriber has consented. Consent is given on the basis of accurate and complete information provided by the provider of electronic

communication services available to the public regarding the types of further processing it intends to perform. The subscriber has the right not to give or to withdraw the consent of such processing.

5. In any case, the practice of sending e-mails for direct trading purposes that conceal the identity of the sender on whom the communication was made, or without a valid address to which the recipient may send an order, is not permitted.
6. Data on communication traffic used for direct trading services or to ensure the added value of services to be deleted or made anonymous after the provision of the service. Service providers keep subscribers informed of the types of data being processed, the purposes and duration for which it was made.

Article 8

Communication confidentiality

Controllers guarantee the confidentiality of communications and the circulating data related to it, according to the purpose of a public communication network and publicly available electronic communication service, according to national legislation. Controllers prohibit listening, typing, storing or other types of interception or surveillance of communications and circulating data in question by persons other than users without the consent of interested users, unless they are legally authorized to do so.

Article 9

Security and information security

1. Service providers take appropriate measures to protect the security of their services, if necessary in cooperation with the network provider, and inform subscribers of any particular risk of breach of network security.
2. Internet service providers provide electronic Internet communication services to inform users and subscribers of the measures they must take to protect their security of communication, for example by using certain types of programs, antiviruses or any other means of protection.
3. The request to inform subscribers of specific security risks does not relieve a service provider of the obligation to take, at its own expense, the necessary and immediate measures to improve any new and unforeseen security risks and restore normal level of service security.

Article 10

Data protection

1. Data controllers should be clear about the time period for which personal data is kept and the reasons why the information is being retained. If the purpose for which the data is obtained has ceased and personal information is no longer needed, the data is deleted or alienated in a secure manner.
2. The data is anonymous to remove any personal data. In order to comply with this legal requirement, data controllers assign specific responsibilities and establish procedures to

ensure that files are emptied regularly and that personal data is not kept longer than necessary.

3. Orientations in relation to the Public Electronic Communication service are only for data created or processed as a result of a communication or a communication service and are not related to the data contained in the communicated information.

Article 11

Subscriber Number

1. Controllers ensure that subscribers are informed, free of charge, before they are included in the counters, regarding the purpose of a printed or electronic subscriber counter, available to the public in which their personal data is included and in any further exploitation options based on the search functions included in the electronic versions of the counter.
2. The controllers ensure that subscribers are given the opportunity to determine whether their personal data is included in a public counter, and if so, the extent to which such data is relevant to the purpose of the meter defined by the numerator, and to verify, correct, or retrieve such data.
3. For any purpose of a public numerator other than a detailed search of the contact of persons on the basis of their name and, when necessary, a minimum of other identifiers, the subscribers may be asked for additional consent.

Article 12

Final provisions

1. All public and private controllers in the territory of the Republic of Albania are responsible for the implementation of this instruction.
2. Failure to comply with the requirements of this instruction constitutes a violation of the law on personal data protection and is punishable under Article 39 thereof.
3. This instruction enters into force immediately and is published in the Official Journal.

COMMISSIONER

FLORA ÇABEJ (POGAÇE)