INSTRUCTION

No.__, dated __/__/2017

ON

DEFINING THE SECURITY LEVEL ON PERSONAL DATA PROCESSING THROUGH SECURITY SYSTEMS PURSUANT TO LAW NO. 19/2016 "ON ADDITIONAL PUBLIC SECURITY MEASURES"

Pursuant to point 3 and 4 of Article 12, Article 14 and point 3 of Article 20 of the Law No. 19/2016 "*On additional public security measures*", the Information and Data Protection Commissioner (hereinafter the Commissioner),

INSTRUCTS:

Article 1

Object

The object of this instruction is to define the security level that should be ensured by private and public entities during personal data processing through the means defined in Article 8 of the Law No. 19/2016 "On Additional Public Security Measures".

Article 2

Scope

This instruction is applicable to all private and public entities which in terms of the Law No. 19/2016 "On Additional Public Security Measures" are required to take additional security measures according to Article 8/a/b of this law and be provided with security certificate by the responsible authority.

Article 3

Definitions

The terms of this instruction have the following meanings:

"*Private and public entity according to the Law No. 19/2016 "On Additional Public Security Measures*" means a data controller, in terms of the Law No. 9887/2008 "*On Personal Data Protection*", as amended.

"*Data processing*" is any action performed with individuals' data through additional security measures.

"*Personal data processor*" is the person authorized in a written form by the head of the public entity or the administrator of the private entity, whom processes personal data through additional security measures on behalf of the controller.

"*Recipients of personal data*" refers only to bodies as provided for by Article 13 of the Law No. 19/2016 "On Additional Public Security Measures".

Other terms used in this instruction have the same meaning with those provided in the Law No. 9887/2008 "On Personal Data Protection", as amended.

Article 4

Personal data processing

1) The processing of personal data through additional security measures is performed only for the purpose stipulated in the Law No. 19/2016 "On Additional Public Security Measures".
2) Personal data that are processed with additional means set forth in Article 8/1/a and b of the Law No. 19/2016 "On Additional Public Security Measures", that make a person directly or indirectly identifiable, are dealt with in accordance with Article 14 of the Law No. 9887/2008 "On Personal Data Protection", as amended.
3) The disclosure of personal data is prohibited except for cases provided for in Article 13 of the Law No. 19/2016 "On Additional Public Security Measures".

Article 5

Notifying prior to the processing of personal data

Private and public entities, after establishing additional security measures and prior to initiating the processing of personal data, carry out the "Notification/"Notification update with the Office of Information and Data Protection Commissioner (hereinafter the Commissioner's Office), according to the model no. 1 attached to this Instruction, pursuant to point 3 of Article 12 of the Law No. 19/2016 "On Additional Public Security Measures".

Article 6

Obligations of public and private entities

1) Every public and private entity establishing additional security measurers is required to :

    a) Prior to installation and activation of video surveillance systems, or the use of other additional measures, shall carry out a data protection impact assessment and document it;
    b) Put the CCTV sign in the surveillance premises, according to the model no. 2 attached to this instruction;

c) Authorize in writing the person/s whom is entitled to manage the installed/established mean as additional security measure, as well as the level of access to the data processed;
d) Request the completion and signature of "*Confidentiality Declaration*" by any authorized person;
e) Manage and administer with evidence actions taken during the processing of personal data with additional security measures;
f) Monitor compliance with security standards for automated data protection against their accidental or unauthorized destruction, as well as against unauthorized access, alteration and dissemination;
g) Allow the exercise of every persons' right, personal data subject, to consult the processing of the respective data and document on this right;
h) Establish written rules for putting in place additional security measures, processing of personal data, authorized persons to access the database, data retention period as well as means of their destruction;
i) Ensure that the CCTV positioning records video within the purpose of its installation;
j) Ensure that any transmission of data on the internet be encrypted, allowing access only to their provider and recipient;
k) Include in the data protection regulation levels of access to the persons accessing it, interaction of the database, etc.

Article 7

The authorized person for the processing and administration of personal data

1) The authorized person should be the person in charge in terms of the Law No. 9887/2008 "On Personal Data Protection", as amended.
2) The authorized person should:
   a. Notify the Commissioner's office within 48 hours in the event where the system is compromised, manipulated or modified without authorization;
   b. Notify the Commissioner's Office for the disclosure of personal data according to Article 13 of the Law No. 19/2016 "On Additional Public Security Measures".

3) Communications with the Commissioner's Office will be made in written form or electronically.

Article 8

Camera surveillance policies

1) Camera surveillance policy is published on the official website of the private or public entity in an easily readable format.
2) Camera surveillance policy should:
   a. Describe the purpose and use of the system, the processing made on personal data and security measures;
   b. Define compatibility confirmation with the Law No. 9887/2008 "On Personal Data Protection", as amended and instructions adopted by the Commissioner;
   c. Describe the applied measures;
   d. Provide a brief description on the areas to be covered by the CCTV system (such as entrances and exits, server room, storage rooms, etc.);
   e. Define the period of data retention;
   f. Identify the procedures that should be followed by data subjects in order to verify, alter or delete their information;
   g. Inform data subjects on their right to address the Commissioner at any time;
   h. Provide information contacts of the entity, whereas individuals may be informed on video surveillance policies.

Article 9

The special regulation

Any entity liable to this instruction is required to reflect in the special data protection and data security regulation, the security level on data protection, access level, means and manners for destroying data upon the termination of the processing purpose.

Article 10

Final provisions

1) Failure to implement requirements of this instruction will be subject to sanctions set forth by the Law No. 9887/2008 "*On Personal Data Protection*", as amended.
2) All private and public entities are bound to implement this instruction, subject to the Law No. 19/2016 "*On Additional Public Security Measures*".

This Instruction enters into force after the publication on the Official Gazette.

COMMISSIONER

BESNIK DERVISHI

Model No. 1

ANNEX OF THE NOTIFICATION FORM TO THE PUBLIC OR PRIVATE ENTITY, SUBJECT TO THE LAW NO. 19/2016 "ON ADDITIONAL PUBLIC SECURITY MEASURES'

Pursuant to Law No. 19/2016 "On Additional Public Security Measures" and instruction no. 46, dated 28/03/2017 of the Commissioner.

1) Entity information

- Designation_____
- BIN_____
- Address_____
- Phone number_____
- Email address_____
- Website_____

2) Authorized person:

- Name/Surname_____
- Phone number_____
- Email address_____
- Authorization or contract with third parties

3) Entity category: (e.g. private/public education institutions of all levels; gambling/casino entities; administrators of stadiums, sport premises, movie theaters, theaters, concert halls, museums; administrators of second level banks, money exchange entities and those of trading and processing of precious metals; centers university and regional public / private health hospitals; entities that have ownership/administration, shopping centers; entities, which during the performance of their economic activity, in open/closed premises, have over 50 employees; entities which during the performance of their economic activity, make an annual turnover of 10 million ALL, etc.).

4) Additional security means:

- High resolution CCTV
- Infrared CCTV
- Automatic reader of license plates

- ID optical reader
- GPS

5) Description of CCTV system:
   - The number of installed cameras: 1-5, 6-15, 16-30, 31+
   - Storage period of recordings: 24x7, activated by motion, time interval
   - Description of the premises under surveillance (internal/external premises, passageway, entrance-exit, perimeter of the facility, etc.):

     _____

   - CCTV model and brand: _____

6) The security level of additional measures:
   - Special regulation
   - Written rules in the general regulation
   - Camera surveillance policy
   - Obtaining consent from 75 % residents
   - Interaction of the database
   - Auditing reports
   - Compliance certificate

❖ After reviewing the form, filing papers requested and confirmation by the Commissioner's office, you may initiate the processing of data.

To the entity: _____ To IDP Commissioner: _____

Name/Surname: _____ Received from: _____

Date: _____ Date: _____

Seal: _____

❖ Means the filing of the document/documents with the Commissioner's office electronically via email or via mail.

CAMERA SURVEILLANCE AREA

Data subjects may exercise their rights under the Law No. 9887, dated 10/03/2008 “On Personal Data Protection”, as amended, with:

_____

(Controller’s name)

Subject to the Law No. 19/2016 “On Additional Public Security Measures”

_____

(Controller’s contacts)

In the event of personal data misuse or violation of privacy through CCTV system, citizens are entitled to complain to:

Information and Data Protection Commissioner.

Phone: 0800 20 50 *www.idp.al* *info@idp.al*