PROCEDURE ON PERSONAL DATA INFRINGEMENT INTERVENTION and CRISIS MANAGEMENT

Version : 1

Issue date : 01.01.2020

1. PURPOSE

According to the paragraph 5 of the article 12 of the Law on Protecting Personal Data, no: 6698 (the "Law"), in case that the personal data processed is obtained by others through illegal ways, **Öz-Ege Tütün Sanayi ve Ticaret Anonim Şirketi** (Öz-Ege Tobacco Industry and Trade Joint Stock Company, the "**Company**"), as the data officer, is obliged to notify this situation to whom it may concern and the Personal Data Protection board (the "Board").

This Procedure on Personal Data Infringement (the "**Procedure**") is issued in order to inform the employees on how to intervene to the crisis to occur in case that the personal data is obtained by other through illegal ways, in other words, there is personal data infringement, and what are the steps to be taken.

2. RESPONSIBILITY

All employees of the company are responsible for the application of the procedure. The employees acting to the contrary to the procedure shall be subjected to the provisions of the "Discipline Procedure".

3. PERSONAL DATA INFRINGEMENT

Personal data infringement emerges in cases such as obtaining the personal data illegally, ensuring unauthorized access to the personal data illegally, disclosing the personal data to unauthorized persons unintentionally/intentionally, deleting, altering or harming the integrity of the personal data illegally.

The situations included below are usually assessed as personal data infringement:

- The physical documents or electronic devices, containing personal data, are stolen or lost,
- The electronic papers, containing personal data, is taken outside the company through hardware or software,
- The user names and passwords, specific to the person, are obtained by unauthorized people,
- Confidential information is disclosed illegally,
- The e-mails containing personal data and/or confidential information are transferred, sent to unrelated people outside the company,
- Ensuring access to the personal data illegally through the performance of virus or other attacks (e.g. cyber-attack) to the information technology (IT) equipment, systems and networks.

4. CRISIS INTERVENTION TEAM

In order to intervene to the crisis situation occurred or may occur in case of personal data infringement, and to fulfill the obligations anticipated in the scope of the law, a crisis intervention team (the team) is formed, to which the participant determined from the departments below are included:

- Data officer contact person,
- Data officer top manager (the General Manager)
- The manager of the department in which the infringement took place,
- Members of the PDP (personal data protection) committee
- The top managers authorized by the data officer on PDP subject (PDP top managers)

5. CRISIS INTERVENTION PROCESS

According to the decision, dated: 24.01.2019 and no: 2019/10 of the Personal Data Protection Board on the Methods and Principles on Personal Data Infringement Notification (the "**decision**"), it is required that notification is done immediately and within at the latest seventy two (72) hours from the date when the company finds outs the personal data infringement, through suitable methods such as informing the Board and directly to the persons if the contact address of the related person can be accessed within shortest time reasonable, if not, by broadcasting over the internet site of the company.

In order to fulfill the obligations in question, in each data infringement case, first of all, certain steps should be followed in the company:

- Preliminary evaluation on the crisis,
- Conducting prevention and recovery activities,
- Evaluation of the risks,
- Notification, and
- Evaluation and improvement.

5.1. Preliminary evaluation on the crisis

In case that a real or potential data infringement is in question before the company, all related personal is obliged to notify the situation to the data officer contact person immediately and without delay. In this scope, the related employee issues a report containing the topics below and informs the data infringement to the data officer contact person.

- Occurrence date and hour of personal data infringement,
- Date and hour of finding out the personal data infringement,
- Explanations on the personal data infringement incident,
- The person and record number, affected by the personal data infringement, if known,
- The descriptions on the steps taken, precautions taken, if exist, in the date when the personal data infringement is found out,
- Name surname, contact information of the employee/employees issuing the report and date of the report.

The data officer contact person, considering the issues stated in the scope of the report, does a preliminary evaluation. When doing this evaluation, starts a comprehensive investigation for researching the data infringement together with the team, by also considering whether there is a real data infringement or not, the scope of the infringement, and the effects which may take place.

5.2. Conducting prevention and recovery activities

The prevention and recovery activities are conducted under the supervision of the team for mitigating the effect of the data infringement on the Company and related persons. In this scope, first the departments required to be informed for the data infringement and these people are guided about the steps required to be taken for controlling the infringement, preventing, if possible, and mitigating the damages. Afterwards, it is tried to find out who are and which records are to be effected by the data infringement and the contact information of

these people, if exists, is also specified. Simultaneously, it is assessed if there are other institutions and organization, required to be informed due to the data infringement or not.

5.3. Evaluation of the risks

Personal data infringements may cause a lot of negative impacts on the persons affected by the infringement, such as identity theft, restriction of the rights, fraud, financial loss, loss of reputation, loss of the security of the personal data, and discrimination. Therefore, it is very important to evaluate very carefully what kind of effects may be caused by the personal data infringement on the Company and persons affected by the infringement and to reveal the risks.

When the risks are evaluated by the team, it should be considered separately the nature, sensitivity and volume of the personal data affected by the infringement and the number of the persons affected and who are the person groups, the effect of the data infringement on the activities and reputation of the company, the precautions taken for mitigating the effect of the data infringement, and the possible results of the infringement. The data infringement is assessed as the “low level, medium level or high revel risk” based on their results.

- **Low level risk:** the infringement has no negative affect on the related persons or this effect remains at negligible level.
- **Medium level risk:** the infringement may cause negative impacts on the related people, but this effect is not big.
- **High level risk:** the infringement causes serious level of negative impacts on the affected people.

The data officer top management is informed by the team on the data infringements defined as medium and especially high level risk.

5.4. Notification

It is required that the data infringement is notified to the third persons outside the company for purposes such as taking precautions mitigating the possible impacts of the infringement for both in the scope of the legal obligation and related with the data infringement.

5.4.1. Notification to the Board

The data officer contact person is especially obliged to notify the Board this situation without delaying as from the moment when he is informed on the personal data infringement and within at the latest seventy two (72) hours. Because of this, it is important that all employees in the company inform any data infringement incident to the data officer contact person without losing time, for the company not to be subjected to any sanction.

For the notification to the Board, the personal data breach application form, published in the internet site of the Personal Data Protection Institution (the “**Institution**”). In cases where it is not possible to provide the information included in the form at the same time, this information may be provided at stages without causing delay. In case that the notification to the Board is not done within seventy two (72) hours on a valid grounds, the reasons for delaying is described to the Board together with the notification.

5.4.2. Notification to the persons affected by the breach

After the persons impacted by the personal data infringement are specified, the company has to inform the related persons as soon as possible directly if the contact address of the related person is accessible, through suitable methods (*e.g. publishing an announcement related with the situation over the internet site*) if not accessible.

It is required that the infringement notification, to be done by the company to the related person, is done with a clear and plain language and, as a minimum, contains the elements below, according to the decision of the board dated: 18.09.2019 and no: 2019/271 related with the minimum elements required to be included in the data infringement notification done to the related person by the data officer:

- When the infringement takes place,
- Which personal data is affected by the infringement, based on personal data categories (by sorting out personal data/personal data with private nature distinction),
- Possible results of the data infringement,
- The precautions taken or recommended to be taken for mitigating the negative impacts of the data infringement,
- Including the communication way elements, such as name and contact information of the contact persons or full address of the internet page, call center of the data officer, which enable hat the concerned people get information related with the data infringement,

5.4.3. Other notifications

In addition to the notifications, the company has to do legally, it may be required that the third persons are informed, considering the elements such as the nature, size of the data infringement, whether the breach constitutes a crime or not. These persons may be the other data officers or data processors, external consultants, judicial authorities, and banks. The team separately evaluates whether there is such necessity or not and, if necessary, informs.

5.5. Evaluation and improvement

It is required that all information, impacts and precautions taken related with the personal data infringements are recorded and kept ready for the supervision of the Board by the company. The data officer contact person and team do an evaluation for determining whether the steps taken related with the date infringement are suitable or not and what can be the elements which may be improved/developed for a possible data infringement. In this scope the team issues an evaluation and improvement report containing the elements below:

- Which steps are needed to mitigate the impacts of possible personal data infringements,
- Whether an improvement is required in any policy, procedure or reporting because of the personal data infringement,
- Whether it is necessary to take an additional administrative and/or technical precaution is taken for preventing repetition of the personal data infringement,
- The necessity of a personal awareness training to prevent repetition of the infringement,
- Whether it is necessary to invest to the resources/infrastructure for mitigating subjecting to the infringements and the effects of the costs.

6. RELATED POLICIES AND PROCEDURES

This procedure should be dealt with all policies and procedures entered into force related with protecting and processing of the personal data before the company.

7. UPDATE

This procedure, without considering the needs for changing in the corporate or legally arisen contents, reviewed once (1 time) a year and recorded. Even if the procedure is updated, the changes occurred in the legislation shall be applied immediately.