ARKAS HOLDING A.S.
CRISIS RESPONSE PROCEDURE
6.11.2019 / Version No: 1

TABLE OF CONTENTS

ARKAS HOLDING A.S.
CRISIS RESPONSE PROCEDURE
6.11.2019 / Version No: 1

1. Purpose

According to Paragraph 5 of Article 12 of the Personal Data Protection Law No. 6698 (Law) ARKAS HOLDING A.S. (Company) is obliged to notify the data subject and the Personal Data Protection Board (Board) as soon as possible if the processed personal data are illegally obtained by third parties.

This Crisis Response Procedure (Procedure) has been issued to inform the employees about how to respond to the crisis in case of personal data breach and what steps to take if personal data are illegally obtained by third parties.

2. Responsibility

All employees are responsible for the implementation of the Procedure. Employees acting contrary to the procedure shall be subject to the provisions of "Disciplinary Regulations".

3. Personal Data Breach

Personal data breach occurs in cases such as illegal obtaining of personal data, unauthorized access to personal data in violation of the Law, accidental/deliberate disclosure of personal data to unauthorized persons, unlawful erasure, alteration or disposal of the integrity of personal data.

The following situations are generally considered as personal data breaches:

- Theft or loss of physical documents or electronic devices containing personal data,
- Obtaining of personal usernames and passwords by unauthorized persons,
- Illegal disclosure of confidential information,
- Incidental transmission and sending of e-mails containing personal data and/or confidential information to irrelevant persons outside the company,
- Providing illegal access to personal data through cyber viruses or other attacks on IT equipment, systems and networks (i.e. cyber-attack).

In case of the above mentioned or similar cases, please act as specified within this Procedure.

4. Crisis Response Team

A Crisis Response Team (Team) is established to involve participants identified from the following departments in order to respond to a crisis situation occurring or likely to occur in the event of a personal data breach and to fulfil the obligations stipulated under the Law:

- Data Controllers' Contact Person [1]
- Data Controller Senior Management (General Manager)
- Manager of the Department in which the Breach has Occurred
- KVK (Personal Data Protection) Advisory Group
- Senior Managers Authorized by the Data Controller regarding Personal Data Protection (KVK Senior Management

5. Crisis Response Process

In accordance with the Decision of the Personal Data Protection Board dated 24.01.2019 and numbered 2019/10 regarding the Procedures and Principles of Notification of Personal Data Breach (Decision), the Company should notify the Board **without delay and within 72 hours at** the latest after detecting the

[1] For companies that do not conduct VERBIS registries/notifications, a Data Inventory Responsible will represent the company within the Crisis Response Team instead of a Data Controllers' Contact Person.

personal data breach and the company should notify the data subject **as soon as reasonably possible** after the determination of the persons affected by the data breach if the contact address of the data subject is available, if the contact address of the data subject is not available, appropriate methods should be used for notifying the related persons such as an announcement to be made on the company's own website.

In order to fulfil these obligations, certain steps must first be followed within the company in the event of a data breach:

- Preliminary assessment of the crisis,
- Blocking and recovery,
- Assessment of risks,
- Notification,
- Evaluation and improvement.

5.1. Preliminary Evaluation of Crisis

In the event of an actual or potential data breach at the Company, all relevant employees are obliged to notify the Data Controller immediately and without delay. In this context, the relevant employee prepares a report containing the following issues and reports the data breach to the Data Controllers' Contact Person.

- Date and time of personal data breach,
- Detection date and time of personal data breach,
- Explanations related to personal data breach event,
- If known, the number of persons and records affected by personal data breach,
- Descriptions of the steps taken and the measures taken, if any, on the date of detection of the personal data breach,
- Name, surname, contact information and report date of the employee (s) preparing the report.

The Data Controllers' Contact Person shall make a preliminary assessment taking into account the matters specified in the report. When making this assessment, the Data Controllers' Contact Person initiates a thorough investigation with the Team to investigate the data breach, taking into account whether there is an actual data breach, the extent of the breach, and its possible effects.

5.2. Blocking and Recovery

Blocking and recovery activities are carried out under the supervision of the Team in order to reduce the effects of data breach on the Company and data subjects. In this context, the departments that need to be informed about the data breach are identified first and they are guided regarding the steps to be taken to control the breach, if possible to prevent it and to reduce the damages.

Subsequently, it is attempted to determine which persons and records are to be affected by the data breach and if available, their contact details are determined. It is evaluated simultaneously whether there are other institutions or organizations that should be notified due to data breach.[2]

5.3. Assessment of Risks

Personal data breaches can have many negative effects on persons affected by the breach, such as identity theft, restriction of rights, fraud, financial loss, loss of reputation, loss of security of personal data, discrimination, etc. For this reason, utmost importance must be given to carefully evaluating the possible consequences of personal data breach for the Company and the persons affected by the breach and revealing the risks.

[2] For example, it may be necessary to apply to the prosecutor's office due to a cyber-attack.

When assessing the risks by the team, the nature, sensitivity and volume of personal data affected by the breach, the number of individuals affected and who the groups of persons are, the impact of the data breach on the Company's activities and reputation, the measures taken to reduce the impact of the data breach and the possible consequences of the breach should be considered separately. As a result, data breach is characterized as "low, medium or high risk":

- **Low Risk:** The breach does not cause any negative effect on the persons concerned or its effects remain negligible.
- **Intermediate risk:** Breach may cause adverse effects on the persons concerned, but the effects are not substantial.
- **High Risk:** The breach causes serious negative effects on the affected persons.[3]

The Team notifies the Senior Management of Data Controller regarding data breaches identified as medium or high risk (especially in high risk data breaches).

5.4. Notification

The data breach should be notified to third parties outside the Company both within the scope of legal obligation and for the purposes of taking measures regarding the data breach and reducing the possible effects of the breach.

5.4.1. Notifying the Board

The Data Controllers' Contact Person shall be obliged to notify this situation to the Board **without delay and within maximum 72 hours from the moment it becomes aware of the personal data breach**. Therefore, it is of utmost importance that all employees within the Company inform the Data Controllers' Contact Person of any data breach without delay, so that the Company is not subject to any sanctions.

Personal Data Breach Application Form published on the website of Personal Data Protection Authority (Authority)[4] shall be used in the notification to be made to the Board. Where it is not possible to provide the information contained in the form at the same time, this information may be provided gradually without delay.

In case of failure to notify the Board within 72 hours with a justifiable reason, the reasons for the delay shall be explained to the Board together with the notification to be made.

5.4.2. Notifying the Affected Persons of the Breach

The Company should notify the data subjects as soon as reasonably practicable after the identification of the persons affected by the personal data breach, directly if the contact address of the data subject is available and by appropriate means if not available (e.g. release of a notice

---

[3] Personal Data Protection Authority: *"In determining the level of data breach that has taken place, it is necessary to evaluate how much potential impact it has on the persons concerned. In the evaluation of the potential impact in question, the nature of the breach, the reason for the breach, the type of data exposed in the breach, the measures taken to reduce the impact of the breach and the categories of persons affected by the breach should be taken into consideration. "*

It can be considered that a list of participants with only their first name and phone information carries **a low level of risk** in case of breach.

A **moderate level of risk** is acceptable if the breach has negative effects on the persons concerned but does not have a large impact. Although important information of the persons is subject to breach, security measures taken by the data controller after the breach and the fact that the effects of the breach have been significantly reduced can be given as an example of this type of risk.

In particular, it can be considered that the breach bears **a high level of risk** if the number of persons and/or records affected by the breach is numerically high, the data subject to the breach contains sensitive data or important information of persons such as credit card information.

However, the Authority's explanations and decisions on the subject of risk assessment should be followed.

[4] The application form can be accessed from https://www.kvkk.gov.tr/SharedFolderServer/CMSFiles/617f166c-24e1-42b5-a9cb-d756d6443af9.pdf

on the website). Such notifications shall be made by the Data Controllers' Contact Person with the support of the Team.

Regarding the minimum elements to be included in the data breach notification made by the data controller to the data subject, pursuant to the Decision of Personal Data Protection Council dated 18.09.2019 and numbered 2019/271, the breach notification by the Company to the data subject should be made in a clear and simple language and shall include at least the following items:

- When the breach occurred,
- Which personal data are affected by the breach on the basis of personal data categories (separating personal data/special categories of personal data),
- Possible consequences of personal data breach,
- Measures taken or proposed to be taken to reduce the negative effects of data breach,
- The name and contact details of the contact persons that will provide data subjects more information regarding the data breach or the full address of the data controller's web page, call center etc. are included.

5.4.3. Other Notifications

In addition to the notifications that the Company is legally obliged to make, it may be necessary to notify third parties by considering the nature and the level of the data breach, whether the breach constitutes as a crime or not. The third parties to be notified may be other data controllers or data processors, external consultants, judicial authorities, banks. The team also evaluates whether such a notification is necessary and makes the related notifications if so.

5.5. Evaluation and Improvement

All information, effects and measures taken regarding personal data breaches should be recorded by the Company and kept ready for review by the Board. The Data Controllers' Contact Person and the Team shall conduct an assessment to determine whether the steps taken in relation to the data breach are appropriate and what could be improved and enhanced in case of a possible data breach. In this context, the Team prepares an evaluation and improvement report that includes the following items.

- What steps should be taken to reduce the impact of possible personal data breaches
- Whether any policy, procedure or reporting needs improvement due to personal data breach
- Whether it is necessary to take any additional administrative and/or technical measures in order to prevent the recurrence of personal data breach,
- Requirement of personnel awareness training to prevent recurrence of the breach,
- Whether additional investment in resources/infrastructure is necessary to reduce exposure to breaches and reduce financial impacts.

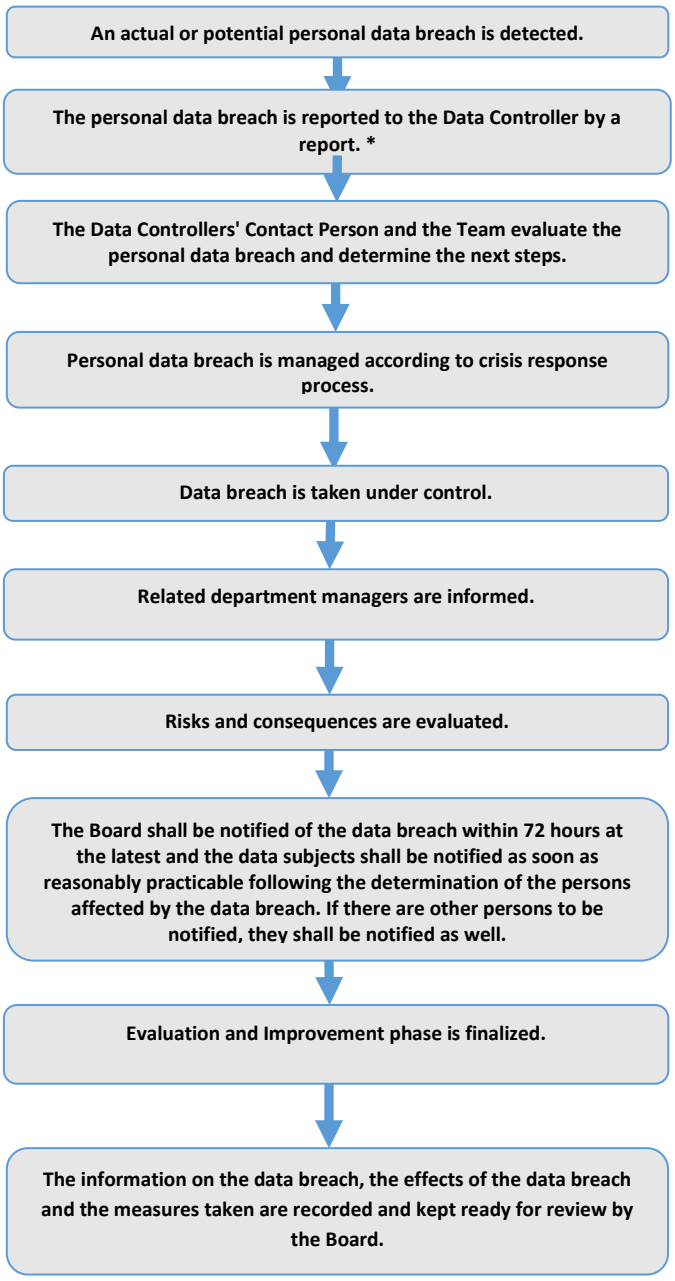
6. Related Policy and Procedures

This Procedure should be implemented in line with all the policies and procedures in place within the Company regarding the protection and processing of personal data.

7. Update Procedure

This Procedure is reviewed and updated once a year regardless of the alteration requirements in its corporate or legal content. Even when the procedure has not been updated, any changes that occur in the legislation are to be put into effect immediately.

ANNEX-1/Crisis Response Flow



* In the event of an actual or potential data breach at the Company, all relevant employees are obliged to notify the Data Controllers' Contact Person immediately and without delay.