DATA BREACH RESPONSE PLAN

PART ONE

Purpose, Scope and Definitions

Purpose

Art 1 – The purpose of this Plan is to regulate roles and responsibilities as well as due procedure and principles to be followed in case of possible data breach incidents, in order to ensure proper protection of fundamental rights and freedoms of individuals, with an emphasis on the right to privacy of private life, and to prevent unlawful processing of and unlawful access to personal data and to ensure the protection of personal data; in case of a data breach incident in order to fulfill the obligations of taking all kinds of technical and administrative measures required.

Scope

Art 2 – This Plan covers ÇOK A.Ş. by employees involved in the processing of personal data, regardless of whether it is processed on physical or electronic media.

Definitions

Art 3 – For the implementation of this Plan, the following should be understood to mean;

a) **Explicit consent:** Freely given, specific and informed consent,

b) **Data subject:** The natural person, whose personal data is processed,

c) **The Law:** The Turkish Law No. 6698 on the Protection of Personal Data dated 24 March 2016,

d) **Personal data:** Any information relating to an identified or identifiable natural person,

e) **Processing of personal data:** Any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means,

f) **The Board:** Turkish Personal Data Protection Board,

g) **Plan:** ÇOK A.Ş. Data Breach Response Plan,

h) **Data breach:** Unlawful acquisition by others of personal data processed by data controller,

i) **Data processor:** The natural or legal person who processes personal data on behalf of the data controller upon his authorization,

j) **Data filing/registry system:** The registry system which the personal data is registered into through being structured according to certain criteria,

k) **Data controller:** The natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system.

PART TWO

Data Breach

Data Breach

Art 4 – Pursuant to Paragraph 5 of Article 12 of the Law, a Data Breach means unlawful acquisition of personal data which is processed by ÇOK A.Ş.

In addition to the above definition; any accidental destruction, loss, alteration, unauthorized disclosure and / or access to personal data transmitted, stored or processed will also be considered a Data Breach under the Plan.

PART THREE

Aims, Officers and Responsibilities

Aims

Art 5 – In the event of a Data Breach, the objectives of ÇOK A.Ş. in the scope of the Plan are:

1. Investigate internally the incident that caused the Data Breach in all relevant departments (in cooperation with law enforcement and other public institutions and organizations where necessary),
2. Identify the source of the Data Breach,
3. Identify the categories of personal data affected by Data Breach,
4. Identify the groups/parties affected by the Data Breach,
5. Determine the potential impact on the parties affected by the Data Breach and to minimize the damages arising from such impact, if any,
6. Determine the magnitude of the impact on ÇOK A.Ş.
7. Determine the expected time of recovery after Data Breach,
8. In case of a cyber-attack:
    a. Whether information systems are affected by cyber-attack,
    b. The elements of the breach that occurred as a result of the attack,

c. Determine the impact of the cyber-attack on the organization of ÇOK A.Ş.,

d. Determine the estimated time of recovery after cyber-attack,

9. Determine the steps to be taken to prevent recurrence of Data Breach and to calculate the estimated time to complete them,

10. Take the necessary steps to notify the incident and the damage resulting from Data Breach:

a. Within 72 hours to the Board in accordance with the Law,

b. To the affected persons as soon as possible by appropriate methods,

c. To employees as soon as possible,

d. If necessary, to other organizations or institutions in the country in accordance with applicable legal provisions,

11. Notify other competent data protection authorities or related institutions abroad within the period in accordance with the applicable legal provisions,

12. Organize post-incident internal audits and training activities, enhance internal communication in order to minimize future occurrences of Data Breaches,

13. Prepare notifications on Data Breaches, their effects and measures taken and to keep them available for review by the Board.

Officers and Responsibilities

Art 6 – In case of Data Breach, ÇOK A.Ş. departments in charge will be determined in accordance with the nature of the incident causing the breach; however, in each case at least one representative from each of the departments listed in the table below shall be appointed. The responsibilities of the representatives are also indicated in the table below.

Department in Charge	**Responsibilities in Case of Data Breach**
Data Protection Officer / Consultant	1. Investigate the event that caused the Data Breach internally in all relevant departments (in cooperation with law enforcement and other public institutions and organizations where necessary). 2. Identify the source of the Data Breach.

	3. Identify categories of personal data affected by Data Breach. 4. Identify the groups / parties affected by the Data Breach. 5. To identify the potential impact on the parties affected by the Data Breach and work to minimize the damages arising from such an impact, if any. 6. Determine the magnitude of the impact on ÇOK A.Ş. on the organization as a result of Data Breach, commercial losses and/or decrease in operations, losses in reputation and / or financial losses and to minimize them in accordance with the Law. 7. Determine the expected time of recovery after Data Breach. 8. Determine the steps to take in order to prevent the infringement from recurring and to estimate how long they will be completed. 9. Notify the Board within 72 hours of the event or loss resulting from the Data Breach in accordance with the Law. 10. Notify other data protection authorities or relevant institutions abroad within the time period in accordance with the relevant legal obligations. 11. Record information on Data Breaches, their effects and measures taken and make them available for the review of the Board. 12. Organize post-event internal audits, training and internal communication activities in order to to alleviate the effects of Data Breach and minimize the risk of future Data Breaches. 13. If personal data fell into the hands of third parties by unlawful means and the data processor in question makes a notification to the data controller to this effect, make ensure that the necessary notification is made to the Board.

	14. Ensure that the Plan is reviewed every 6 (six) months after the effective date.
IT Department	In the event of a data breach via cyber-attack or other electronic means; 1. Determine whether information systems were affected by Data Breach. 2. Identify the elements of the breach. 3. Determine the effects of Data Breach on the organization of ÇOK A.Ş. 4. Determine the expected time of recovery after Data Breach.
Human Resources Department	1. Determine whether the Data Breach was caused by a ÇOK A.Ş. employee. 2. Determine whether ÇOK A.Ş. employees were affected by Data Breach. 3. Determine the elements of the breach and the effects thereof on the organization of ÇOK A.Ş., and the expected time of recovery after Data Breach. 4. Organize post-incident training activities and enhance internal communication. 5. Inform employees as soon as possible of the incident and of the loss resulting from Data Breach.
Legal Department	1. Perform post-incident internal audits. 2. Inform persons affected by the Data Breach about the incident and losses resulting from it as soon as possible using appropriate methods.

	3. If necessary, notify other domestic organizations or institutions within the time required in accordance with relevant legal obligations.
Table 1: Officers and Responsibilities within the Scope of Data Breach Response Plan	

PART FOUR

NOTIFICATION

Notification by Data Controller

Art 7 – Data Breach notifications should be made to the Board and affected persons in order to ensure that measures are taken to prevent or minimize the negative consequences. Pursuant to this Plan prepared in accordance with the Board's decision dated 24.01.2019 and numbered 2019/10, ÇOK A.Ş. should;

1. Notify the Board of Data Breach without delay and within 72 hours at the latest from the date of learning of the incident,
2. Following the proper identification of the persons affected by the Data Breach in question, notify the them as soon as reasonably possible, directly if the contact address of the person can be reached, if not, by appropriate methods such as through the publication on the website of the data controller,
3. In the event that the Board cannot be notified within 72 hours due to a justifiable reason, the reasons for the delay should be explained to the Board along with the notification to be made,
4. Fill out and attach "ANNEX-1 Personal Data Breach Notification Form" to the notification to the Board,
5. Where it is not possible to provide the information requested in the form at once, provide the information gradually and without delay,
6. Record and make available for review by the Board all information on Data Breaches, their effects and measures taken.

All the above-mentioned transactions regarding notifications shall be carried out by the units specified in Art 5 of this Plan and as detailed in the table included below it.

Notification by Data Processor

Art 8 – In the event that the personal data stored by a data processor is unlawfully acquired by others, the data processor must notify the data controller (ÇOK A.Ş.) without any delay. Following the notification by the data processor, ÇOK A.Ş. will notified to the Board following the process elaborated in Art 6 of the Plan.

Cross-border Data Breach

Art 9 – In case a Data Breach occurs at a data controller abroad and the consequences of this breach affects persons resident in Turkey or the data subjects benefit from the relevant products or services in Turkey, this data controller will also notify the Board in accordance with the principles laid out in Art 6 of the Plan.

PART FIVE

Miscellaneous Provisions

Entry into Force

Art 10 – This Policy entered into force as of the date of publication on the Company's website.

Revision of the Plan

Art 11 – This Plan, which has been prepared and put into effect, is to be reviewed periodically every 6 (six) months.

TABLE OF UPDATES

Changes to this Plan up to this date are listed in the table below.

UPDATE DATE/VERSION CODE	**SCOPE OF UPDATES**
20.01.2020	Plan publication date