DOĞAN GROUP

POLICY ON DELETION, DESTRUCTION OR ANONYMIZATION OF PERSONAL DATA

APRIL 2018

CONTENTS

1. OBJECTIVE

The objective of this Policy (''Policy'') is to specify rules that must be followed within the company (''Company'') to delete, destruct or anonymize the personal data in accordance with Law No. 6698 on Protection of Personal Data (“PDP”).

2. SCOPE

This Policy; determines the rules on the deletion, destruction or anonymization of all personal data collected by the Company, transferred to the Company and processed by the Company.

3. ROLES AND RESPONSIBILITIES

3.1. Executive Committee

The Executive Committee is responsible for the approval of this Policy. The Executive Committee is the authorized mechanism for the preparing, publishing, updating, and dismantle of this Policy when needed.

It is the responsibility of the Executive Committee to take action on policy-related applications, to increase and to supervise the effectiveness of the activities within Doğan Holding structure.

The Executive Committee is also responsible for taking precautions for compliance of the staff to this document and reporting it to the Audit and Risk Management Presidency for review of the matters contrary to this document.

3.2. Information Systems

Directorate of Information Systems are responsible for the preparing, developing, executing and updating of this Policy. Directorate of Information Systems reviews this policy, when necessary, in terms of its actuality and need for development.

Doğan Holding Information Systems Manager is responsible for publishing the prepared document on the corporate portal

3.3. Corporate Communication

Doğan Holding Corporate Communications Manager is responsible for the in-house distribution of the prepared document.

4. RULES ON DELETION, DESTRUCTION OR ANONYMIZATION OF PERSONAL DATA

The basic rules for the deletion, destruction or anonymization of personal data are set out as below.

4.1. Personal Data Deletion Rules

When the data are deleted, the process / standards required by the legislation and the following rules should be complied:

- The data must be deleted from the physical documents on which they are stored.
- The data must be deleted from the physical files in which they are stored.
- The data must be deleted from the digital media in which they are stored.
- The data must be delted from magnetic medium, such as camera recordings or tape backups, on which they are recorded.
- Along with being in digital or magnetic medium, deletion of data should be done in cases where the whole medium does not need to be destructed.
- The data recorded must be deleted from the storage devices that are not in active use and from backup units (e.g. cloud storage etc.) used for backup purposes.
- Data processed in fully or partially automated ways and stored in digital medium is deleted by the data deleting methods of the relevant software

4.2. Personal Data Destruction Rules

When the data are destructed, the process / standards required by the legislation and the following rules should be complied:

- The data is destructed from the physical record on which it is recorded, so that it can not be used again.
- The data is destructed from the physical files on which it is recorded, so that it can not be used again.
- The data is destructed from the digital medium on which it is recorded, so that it can not be used again.
- The data is destructed from the magnetic medium on which it is recorded, so that it can not be used again.
- Along with being in digital or magnetic medium, deletions are made which do not require the destruction of the whole media and the data is destructed.

4.3. Personal Data Anonymization Rules

During the anonymization process, nothing that will help redetermine the identity of the related person is left in his/her personal data records. Anonymization of personal data may be provided by means of the following sample methods and procedures / standards as stipulated in the legislation:

a) Data Masking

Protecting the personal data, which may be a direct identifier, on the database by encrypting it or hiding it so as to remove the singularity and preventing the retrospective determination of the data of the person concerned. For example, upon request of the person concerned, the T.R. ID number field may be masked in the database by a sha512 or similar encryption method. However, the same method does not apply to the name of the person concerned, because it may be possible to reach an individual in a filtering process that can be done from the persons who may have the same name at the same time. As another example, such as during the destruction of the fingerprint image the same graphic information always overwritten on the data

b) Data Production

Reconfiguration of impossible non-returning methods such as parasitic spreading or scattering of random characters to prevent personal data from being associated with the person concerned. For example, the fields for grouping open address provincial data in a format that can uniquely identify the person concerned are fixed and the information in the remaining areas (street, house number, etc.) is filled with random characters.

Depending on the characteristics of the data fields during the anonymization process, different methods can be used in different data fields of the same data set to the extent that is allowed by databases and softwares. For example, Anonymization can be done by using different methods for addresses, different methods for T.R. ID numbers. Successfully anonymized information can no longer be considered as a personal data. In this case, the clear consent of the person concerned shall not be sought for the anonymization and the person concerned shall not be able to use the rights specified in the PDP and related legislation about the information made anonymized.

5. RISKS THAT MAY BE ENCOUNTERED BY NON-IMPLEMENTATION OF THE POLICY

5.1. Cases in which employees do not comply with the Policy

It is presumed that the person who does not comply with the rules set forth in this Policy does not obey the Policy. In case if it is determined that the Policy is not respected, it is immediately reported to the Unit

Manager and to the Audit and Risk Management Presidency. The Unit Manager will notify Human Resources Department if it deems necessary.

5.2. Legal Sanctions and Risks

Failure to comply with the said Policy may result to encounter with two different risks Even if the personal data is processed in accordance with the provisions of the PDP and other relevant legislation but is not erased, destructed or anonymized by the data officer in case of the disappearance of the reasons which require the processing and upon request of the official or the person concerned, according to Article 17/2 of the PDP, those who do not delete personal data or make them anonymous will be subject to a punishment according to Article 138 of the Turkish Criminal Code ("TCC") numbered 5237.

In case if the data to be destructed are not destructed, Article 138 of the Turkish Criminal Code provides that those who are obliged to destruct the data in the system despite the expiration of the time periods set by the law are punished with imprisonment from one year to up to two years because that they did not fulfilled their duties.

In the case of the early deletion, destruction or anonymization of personal data, it will become impossible for data authorities to fulfill legal obligations.

6. PUBLICATION OF THE POLICY

This Policy hereby shall be stored on two different media, namely on paper, and in electronic medium. The updated versions of the documents are posted on the corporate portal, and on the website.

Copies bearing original signatures are stored at the Office of the Vice Presidency of Finance and the controlled copies are stored by the Chief Legal Consultancy, and when required, there are destroyed by the Chief Legal Consultancy with the approval of the Department Manager

7. UPDATING PERIOD

This Policy hereby shall be reviewed at least once a year, and if required, they are updated as per the principles set forth in the Documentation Management Procedures.

8. EFFECTIVENESS

This policy hereby shall become effective on the date of acceptance by the Executive Committee

9. ABOLISHING THE POLICY

In case it is decided that it will be abolished, the former copies of this Policy hereby, bearing original signatures shall be canceled by the Chief Legal Consultancy with the written approval of the Department Manager (by posting a cancellation stamp thereon, or by writing "canceled" on it), and shall be stored by the Office of the Vice Presidency of Financial and Administrative Affairs.