Client Alert | Data, Privacy & Cybersecurity

Guideline on Conducting Data Inventory is Published by Turkish Personal Data Protection Authority

May 2019

Authors: Emre Özşar, Selin Kaledelen, Damla Çay

The Turkish Personal Data Protection Authority (the "Authority") has published on its website the long-awaited guideline on the preparation of data inventories by data controllers on April 29, 2019.

The guideline includes the required steps and the minimum amount of information for producing the inventory. Moreover, the guideline contains certain recommendations with respect to data inventory and compliance with data protection legislation in general.

Legal Background and Minimum Content

Pursuant to Article 5(1)(ç) of the Regulation on Data Controllers Registry published in the Official Gazette on December 30, 2017 (the "**Regulation**"), the data controllers who are under the obligation to get registered to the Registry of Data Controllers (the "**Registry**") are also obliged to keep a data inventory.

As per Article 4 of the Regulation, a data inventory should contain the following minimum information:

- data category
- purposes of and legal grounds for processing personal data
- recipients / groups to which the data is transferred
- groups of data subjects
- maximum data retention period necessary for the purposes of processing
- data to be transferred abroad
- technical and administrative measures required for data security

Purpose of Conducting a Data Inventory

The inventory shows all data processed by a data controller. The data controller can monitor its own compliance with the data protection legislation by using this detailed analysis. The inventory is advised to be used while producing documentation for the following:

The guideline shows five specific issues where the inventory shall be referred to in compliance process pursuant to the data protection legislation:

i. registration with the Registry;

ii. fulfilment of information responsibilities;

iii. responding the data subject requests;

iv. defining the scope of the explicit consent; and

v. preparation of the data storage and destruction policies.

Additional Content and Form of the Data Inventory

As explained above, there is a minimum content for a data inventory. However, in addition to the minimum content required, the data controllers are recommended to include the maximum amount of information possible to the inventory (e.g. the department, unit or person who processed the data, the name and explanation of the process and the activity where the data is processed, whether information responsibilities had been fulfilled when the data was first obtained, the source and the method of obtaining the personal data, the storage environment of the data, the purpose and method of transfer, etc.).

Similarly, the Board allowed the data controllers to determine an appropriate form and storage environment for the inventory by taking into account appropriate criteria; and although there is no clear description/definition of such "appropriate criteria" enumerated in the guide we believe such criteria will consist of the following: i) the quality and the number of the data processed and the data subjects, ii) the variety of the personal data, iii) data transfers within the data controller or to the third parties, iv) difficulty level of the technical and administrative measures, and etc.

Preparatory Steps for Conducting Data Inventory

The guideline contains a section recommending steps for keeping and preparing data inventory and its usage for data compliance purposes as follows:

i. The data controller assigns a person (or ideally, a team or committee) working in law, IT or HR departments who has a comprehensive knowledge of data protection legislation and detailed information on the data processing processes and the data processed.

ii. Such person/team makes a detailed analysis of all data electronically or physically processed by the data controller. This analysis contains the following:

- Defining the type of the personal data (i.e. whether or not the data is under the special categories of personal data in the meaning of Article 6 of the Personal Data Protection Law no. 6698 (the "**PDPL**"))
- Determining each step where the data is being processed (obtaining, saving, erasing, destroying, anonymizing, updating, storing, changing, transferring, etc.)

Preparation of the personal data workflow diagram is also advised.

iii. The person/team in charge prepares the inventory and privacy statements accordingly, determines the data which does not meet any legal ground for processing or does not have a processing purpose by using the inventory and destroys such data as soon as possible. The destruction or erasure of data will be made in compliance with data controller's appropriate policies and procedures.

iv. Awareness trainings on the data protection are to be provided to all employees of the data controller.

Preparation of Data Inventory

For data inventory, the following information must be included to fulfil the legal requirements:

i. data processed on process or activity basis

ii. the type of each data determined (i.e. whether or not the data is under the special personal data categories in the meaning of Article 6 of the PDPL)

iii. legal ground for each data processed (these grounds are enumerated under Articles 5 and 6 of the PDPL)

iv. processing purpose of each data (note that if the data controller is unable to define a purposes of processing, it is obliged to delete or destruct such data)

v. data subject group of each data

vi. period of storage of each data processed (note that if a specific period is not determined under the relevant legislation, the data controller should determine the necessary period for the purpose of processing pursuant to Article 4(2) of the PDPL and by taking into account the criteria provided by Article 9(4) of the Regulation)

vii. receiver/receiver groups to whom each data is being transferred

viii. whether or not each data transferred abroad

ix. technical and administrative measures taken for each data processed (the Personal Data Security Guideline prepared by the Board and the Board's Decision dated January 31, 2018 and numbered 2018/10 should be taken into account in the determination of such measures)

The guideline highlights that since a data can be processed in different processes and activities, it may have different legal implications for processing, and there may be different storage period, technical and administrative measures. Hence, it is important to determine the data breakdowns in every process and activity and take into account that a data may be processed more than once in different processes.

The data controllers can use the data categories, processing purposes, data subject groups, receiver groups and technical and administrative measures sections in the Registry as a guide while determining such information of a data to be included in the data inventory.

Data Inventory Template

In the Annex 1 to the guideline, a template is provided for data inventory containing the minimum content required by the Regulation. Below, we provide a condensed version of this template:

ORGANIZATION	PROCESS	PERSONAL DATA						STORAGE AND DESTRUCTION	TRANSFER		SECURITY MEASURES TAKEN	
Department	Activity	Data Category	Personal Data	Personal Data Under Special Category	Processing Purpose	Data Subject Group	Legal Ground	Storage Period	Receiver/ Receiver Groups	Data Transferred Abroad	Administrative Measures	Technical Measures
Human Resources	Forming Employee's Personnel File	Personnel		Criminal Record	Performance of Responsibilities Arising from Service Agreement and Legislation	Employees	Provision by Law	10 Years as of the Ending Date of Employment	Social Security Institution and other Authorized Intuitions and Authorities	No Cross-border Data Transfer	In addition to the administrative measures taken for personal data, periodic trainings are provided to the employees working in the processing processes of personal data under special category, special security measures are taken for the processing and storage environments of such data, unauthorized access is prevented, if physical transfer is necessary, the document is sent with a "confidential document" notice.	In addition to the technical measures taken for personal data, policies and procedures for the security of personal data under special category are determined, access authorizations and roles are clearly determined, periodic authorization controls are conducted, cryptographic methods are used in the electronic environments where such data is processed, cryptographic key is kept in a secure environment, transaction records are locked, periodic security tests are made.

Conclusion

The personal data inventories can be considered as the synopsis of the data controller for personal data processing activities, which is the first step to be taken while conducting data protection compliance projects. In addition, in order to have appropriate and clear documentation, data inventories are advised to be established by experts who are specialized in law, and IT (and process). Inventories facilitate the factual assessments of the risk of the processing activities performed by a controller or processor on individual's rights, and the identification and implementation of appropriate security measures to safeguard personal data which are key components of the principle of accountability.

The data inventories should be kept up to date and be reviewed periodically by people who are assigned for this purpose only. Changes made in data inventory should be reflected to the Registry records as well.

GKC Partners
Ferko Signature
Büyükdere Cad. No: 175 Kat: 10
Levent 34394
Turkey

T + 90 212 355 1300