

Precautions to be taken by Data Controllers While Processing Specially Qualified Personal Data

Principle decision of the Personal Data Protection Authority (“Authority”) outlining necessary precautions to be taken by data controllers while processing specially qualified personal data has been published on the Official Gazette on March 07, 2018. The decision is based on Article 6/4 of Turkish Personal Data Protection Law numbered 6698 (“Law”) which states that sufficient precautions defined by the Authority must be also taken into account while processing specially qualified personal data. The Authority in its decision points out a systematic, manageable and sustainable policy and procedure so as to assure the security of personal data and accordingly mentions concrete precautions to be taken for processing of specially qualified personal data.

Rules For Employees of Data Controllers Who Process Specially Qualified Personal Data

Additional obligations imposed on data controllers for their employees who process specially qualified personal data (members of the HR departments could be held within this concept) are as follows:

- Organizing regular trainings to these employees in terms of the security of specially qualified personal data and the Law as well as relevant regulations,
- Executing confidentiality agreements with these employees,
- Defining precisely the scope of the authority and the time period of the accessibility to the personal data of users who have an access to specially qualified personal data,
- Controlling the authority of the employees periodically,
- Ceasing immediately the authority of employees to access the specially qualified personal data and taking the data inventory back from them when their position is changed within the organization or when they no longer work for the data controller.

Rules Specific to the Platform in Which Personal Data is Kept

The Authority in its decision splits the platforms into two; electronic and physical where the specially qualified personal data is processed, preserved and/or accessed and then sets forth obligations for each platform.

According to the decision, if the platform is electronic;

- Personal data must be preserved by using cryptographic methods and cryptographic keys must be kept in secure and different places,
- Records of every move of data process must be kept in a secure way, security must be kept updated for the platforms where data is preserved,
- If the data is accessed through software, users must be authorized accordingly,
- Sufficient security tests must be made and their results must be recorded regularly for the platforms where the data is kept and
- If distant access is required, authentication of identity must be provided at a sufficient level,

If the subject platform is physical;

- It must be ensured that sufficient security measures are taken and
- Unauthorised entrance and exit must be prevented for these platforms.

Rules Related to Transfer of Personal Data

The Authority sets forth different security precautions according to the platform to be chosen while transferring specially qualified personal data. Therefore if data is transferred;

- Through e-mail, using the corporate e-mail address with the password or registered electronic email account,
 - through Platforms such as CD, DVD, memory stick, encrypting through cryptographic methods and keeping the keys in different places,
 - between servers in separate physical platforms, using VPN or sFTP while transferring,
 - Through physical places, taking necessary precautions to overcome the risk of document getting lost, stolen, or seen by unauthorised persons and sending the document in the format of “classified documents” must be preferred.
- Last, the decision states that as well as the abovementioned precautions, technical and administrative precautions stated in the Guidelines of Personal Data published in the website of the Authority so as to provide necessary level of security for those data must be also taken account by data controllers.



BEGÜM YAVUZDOĞAN OKUMUŞ
MANAGING ASSOCIATE

+ 90 (212) 354 00 24
begum.yavuzdogan@gun.av.tr

Begüm is a managing associate in Gün + Partners and she has been working for the firm since 2007. Her practice focuses on corporate and M&A, competition and technology, media and telecom.