DPA Announces the Procedure to be Taken by Companies in Cases of Data Breaches

Turkish Data Protection Authority Announces the Procedure to be Taken by Companies in Cases of Data Breaches

Article by Ertuğrul Can Canbolat, Baran Can Yıldırım, and S. İrem Akın

INTRODUCTION

Article 12 of the Turkish Data Protection Law No. 6698 ("**Turkish Data Protection Law**") entitled "*Obligations Regarding Data Security*" deals with the obligations of the data controller.

Article 12/1 of the Turkish Data Protection Law states the data controller shall take all necessary technical and organizational measures to provide a sufficient level of security. In addition, Article 12/5 of the Law obliges the data controller to notify the Board of Protection Personal Data ("**Board**") as well as data subjects in case personal data is acquired through unlawful means by stating that "*in case processed personal data are acquired by others through unlawful means, the data controller shall notify the data subject and the Board of such situation as soon as possible. The Board, if necessary, may declare such situation on its website or by other means which it deems appropriate*."

A similar provision is also present in Article 33 of the European Union General Data Protection Regulation ("**GDPR**"). However, contrary to Article 33 of the GDPR, Article 12 of the Turkish Data Protection Law does not foresee the procedure as to how such notifications should be made by the data controllers.

In this regard, Turkish Data Protection Authority ("**DPA**") announced on February 18, 2019 the procedure that should be followed by the data controllers when a data breach occurs. In accordance with the procedure[1],

- the data controller shall notify the data breach to the DPA not later than 72 hours after becoming aware of such breach,
- the data controller shall notify the concerned data subjects in the shortest time possible following the determination of the affected individuals (**i**) directly if the contact information is known and (**ii**) through its website if the contact information is not known,
- where the notification to the DPA is not made within 72 hours, the notification shall also explain the reasons that caused the delay,
- the "*Personal Data Breach Notification Form*"[2], which is published in the DPA's website, shall be used for the notifications to be made to the DPA,
- where it is not possible to provide the information included in the form at the same time with the notification, the concerned information may be provided following the notification without undue delay,

- the facts, effects and the measures taken regarding the data breach shall be documented by the data controller and the records thereof shall be kept available for the DPA's examination,
- in case personal data held by the data processors is acquired by others through unlawful means through the data processor, the data processor shall notify the data controller without undue delay,
- if the data breach is related with a data controller located abroad and the results of such breach affects the individuals residing in Turkey or if the concerned data subjects benefit from the products and services of the data controller in Turkey, then the data controller shall notify the DPA under the same principals stated herein,
- the data controllers shall prepare and periodically review a "*Data Breach Response Plan*" which clarifies the issues such as (**i**) to whom the data breach will be internally reported and (**ii**) the responsible person for the notifications and for the evaluations regarding the possible consequences of the data breach.

The Personal Data Breach Notification Form requests important information in order to help both the data controller and the DPA to weigh the effects and risks that may arise from a data breach. The form is separated into five parts as follows; (**i**) the data controller, (**ii**) the data breach, (**iii**) the possible consequences, (**iv**) (if any) the specific results due to a cyber attack and (**v**) the measures taken by the data controller. The form includes questions regarding the nature of the data breach such as the source of the breach, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned, the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller.

CONCLUSION

This latest announcement is another example that the DPA's practices and procedures continue to grow. Since the Turkish Data Protection Law is based on the old Directive 95/46/EC rather than the GDPR, there may be gaps between the Turkish Data Protection Law and the GDPR. Therefore, the DPA closes these gaps and establishes a system in compliance with the latest and most comprehensive regulation through its decisions.

Footnotes

1 https://www.kvkk.gov.tr/Icerik/5362/Veri-Ihlali-Bildirimi

2 https://kvkk.gov.tr/SharedFolderServer/CMSFiles/e0413853-cd8c-428f-9315-2e8b3d874b46.pdf