THE PERSONAL DATA PROTECTION AGENCY'S PUBLIC ANNOUNCEMENT ON THE RECOMMENDED MEASURES TO BE TAKEN BY DATA CONTROLLERS REGARDING USER SECURITY

The "Public Announcement on Technical and Administrative Measures Recommended to be Taken by Data Controllers Regarding User Security" was published on the website of the Personal Data Protection Authority ("Authority") on February 15, 2022.[1]

As the result of the recent data breach notifications within the scope of Article 12 of the Personal Data Protection Law no. 6698, the Authority established, specifically websites of data controllers operating in sectors such as finance, e-commerce, social media and games, the user account information (username and password) used to access the user accounts have been published publicly on some other websites. Without knowledge of the users, data controllers' websites have been entered by third persons and the personal data of the users have been accessed. This personal data can even be offered for sale for an economic value and can be archived and remarketed as data sets by ill-intentioned persons.

To prevent widespread data breaches or minimalize the effects of the data breaches on data subjects, the Authority recommends the data controllers make their risk assessments and take the appropriate technical and administrative measures listed below.

TECHNICAL AND ADMINISTRATIVE MEASURES
• Two-factor authentication systems should be established and alternative security measures should be offered to users starting from the membership stage.
• In case of logging in on different devices other than the frequently used ones, the login information must be sent via e-mail/SMS etc. to the data subject's contact addresses through the methods.
• Applications should be protected with HTTPS or in a way that provides the same level of security.
• Safe and up-to-date hashing algorithms should be used.
• The number of unsuccessful login attempts from the IP address should be limited.
• It should be ensured that the relevant persons can view the information about at least the last 5 successful and unsuccessful login attempts.
• Data subjects should be reminded that the same password should not be used on more than one platform.
• A password policy should be established by the data controllers and the passwords of the users should be changed periodically or it should be reminded to the data subjects.
• The newly created passwords should be prevented from being the same as the old passwords (at least the last three passwords), technologies such as security codes (CAPTCHA, four processes, etc.) that distinguish between a computer and human behaviour should be used for logins to user accounts, and IP addresses allowed to be accessed should be limited.
• The length of the passwords used to log in to the systems should be at least 10 characters, and strong passwords should be created for the combination of upper- and lower-case letters, numbers and special characters.
• If third party software or services are used to access the systems of data controllers, security updates of these software and services should be carried out regularly and necessary checks should be made.

Kind Regards,

Koyuncuoğlu & Köksal Law Firm

* As the explanations given in our newsletter are prepared pursuant to the legislation in effect in the Republic of Turkey and the disclosures made to the public by the relevant official authorities, in case of uncertainty, we advise you to seek advice and support from us before the final transactions are carried out. Otherwise, our Law Firm cannot be held responsible for the actions to be taken on the basis of the explanations contained herein and the consequences of such actions.

[1] For Access: https://kvkk.gov.tr/Icerik/7177/Kullanici-Guvenligine-Iliskin-Veri-Sorumlulari-Tarafindan-Alinmasi-Tavsiye-Edilen-Teknik-ve-Idari-Tedbirlere-Iliskin-Kamuoyu-Duyurusu