Turkish Data Protection Authority Announced Data Leakage of a Dutch Bank

Turkish Data Protection Authority Announced Data Leakage of a Dutch Bank Revealing the Importance of Effective Information Security

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

Under Article 12/5 of the Turkish Data Protection Law, the data controllers are obliged to inform the Turkish Data Protection Authority ("**DPA**") in case the personal data processed on their behalf is acquired by others unlawfully. In line with this provision, ING Bank A.Ş. ("**ING Bank**") notified the DPA that personal data of almost 20 thousand people were unlawfully transmitted to third parties. Accordingly, the DPA on March 2, 2019 made an announcement on its website providing the details of the incident[1].

The data breaches are generally occurred as a result of the cyber-attacks of third parties. ING Bank's notification, however, reveals that the breach was caused by one if its -now former- employees who accessed unauthorizedly to certain databases of Risk Center of the Banks Association of Turkey ("**TBB**") containing personal data belonging to mostly other banks' customers. The employee then transmitted the obtained data unlawfully to third parties, which proves that information security does not always depend on the cyber security that prevents malicious cyber-attacks of third parties.

ING Bank stated that during a project carried out by Risk Center of TBB regarding information security, suspicious inquiries rendered by an ING Bank employee were found. This triggered an internal investigation in ING Bank in October 2018, which reportedly included seizing and inspecting the devices of the concerned employee. The preliminary findings of the investigation raised strong suspicions that a data leak has occurred which may also be considered as "*disclosure of client secret*" under the Banking Law No. 5411. Although the concerned employee was not authorized to make the concerned inquires through ING Bank's system, the employee disabled the authorization system and accessed directly to the TBB's concerned database.

The concerned employee in 2018 run inquiries by using the identity numbers ("**ID**") and tax identification numbers ("**TIN**") of companies which are generally not a client of ING Bank and have leaked the results of these inquiries outside of the bank through electronical devices several times. ING Bank stated that the information obtained as a result of the inquiries are related only with corporate credit records such as, among others, turnovers, IDs of the shareholders, and shareholding structure, some of which are classified as personal data within the meaning of the data protection rules.

In this regard, ING Bank concluded that (**i**) IDs and names of 19,055 individuals and (**ii**) credit reports, address information and phone number of 1,172 sole proprietorships and partnership companies were leaked outside of the bank.

Since the data leaked outside of ING Bank apparently belongs to other banks' customers, we might expect further data breach notifications to the DPA soon by the said banks. A similar incident happened when Optimum Otomotiv Satış Sonrası Çözümleri Tic. A.Ş.'s ("**Optimum**")[2], which deals with car rental activities, notified the DPA regarding a data breached occurred in its system, which included personal data of many customers of other car rental companies. Following that, several car rental companies including Enterprise[3]and Garanfi Filo[4], who were in a business relationship with Optimum, separately filed notifications to the DPA and stated that their customers' data may have been obtained by the third parties as a result of the said breach.

ING Bank asserted that as a result of a thorough investigation, which included examining system logs and witness statements, there is no suspicion that any other individual took part in the data leak. The bank further stated that the method used to disable the authorization system is now blocked. The notified breach proves that the information security does not only depend on the strength of the cyber security programs but also the internal means that efficiently and effectively authorize the relevant personnel and keep track of work conducted within the scope of such authorization. Companies subject to such data breaches might have further problems such as damage claims of other affected companies, whose customers' personal data was leaked, or directly of the data subjects.

In accordance with the notification, ING Bank is now working co-ordinately with TBB to notify the data subjects regarding the concerned leak.

Footnotes

1. The DPA's decision dated 01.03.2019 and numbered 2018/43.

2. The DPA's decision dated 24.01.2019 and numbered 2019/16.

3. The DPA's decision dated 14.02.2019 and numbered 2019/28.

4. The DPA's decision dated 25.02.2019 and numbered 2019/32.