GDPR Case Study: Irish Credit Bureau DAC

Yongjeong Kim
Brown University

Abstract

On March 23, 2021, the Data Protection Authority of Ireland issued €90,000 fine on Irish Credit Bureau (ICB) due to the violation of Article 5(2), Article 24(1), and Article 25(1) of GDPR. The code change made by ICB caused the data breach at its database, which inaccurately stored the client credit information for closed accounts, lasting from June 28 to August 30, 2018. During the breach, incorrect account information was delivered to its members.

1 Background

This section describes the background information for the ICB data breach incident, as explained from the decision letter [2]. ICB stores the credit contract information of its financial institution members and their borrowers in its database and functions as a data library for the members. The members can utilize automated systems to store and access the data, but ICB manually updates the payment profile information on its database. To ensure the accuracy of the completed accounts, ICB had measures to prevent completed accounts from updates in its database with a filter. However, the code change made by ICB on June 28, 2018, resulted in the deletion of the filter and a change in the update permission on the completed account.

On August 27, 2018, ICB was informed of the potential technical error on the account records by its member and was able to analyze that the code change caused the error. However, ICB could not detect the error by itself but relied on its members' reports. ICB promptly took actions to resolve the issues including fixing the code for the filter removal error, informing its members of 98% of inaccurate records, notifying the Data Protection Authority regarding the data breach incident on August 31, 2018, and informing the rest of the members of 2% of the inaccurate records during September 4-5, 2018. After these actions, ICB changed its policy to ensure a risk analysis as well as thorough testing before code changes. It also asked its members to inform the data subjects who might have been affected by this breach.

Nonetheless, ICB was unable to avoid the charges against it for GDPR violations including Article 5(2), Article 24(1), and Article 25(1). The Data Protection Commission (DPC) found ICB responsible for storing inaccurate data, failing to identify risks, having inappropriate technical measures, and failing to demonstrate that ICB is GDPR compliant. While there were no known major events reported that actually affected its members from making the right decision on its clients, during the breach, 15,120 accounts were affected and 118 incorrect credit reports were provided to data subjects. DPC concluded that the violations are evident and the potential risk was severe. While ICB's actions were responsive after the incident such as reporting the data breach and fixing the code within few days, it failed to comply with some of the GDPR articles before the event such that whether its technical measures were appropriate was still in question. For instance, it failed to keep a record of the testing process and its testing mechanism was not able to detect the risk before and after the adoption.

2 GDPR Violations

This section illustrates the DPC's interpretations of ICB's GDPR violations and the appropriate fine, as explained from the decision letter [2]. DPC interpreted ICB as the controller on its database and found ICB responsible for the GDPR violations of Article 5(2), Article 24(1), and Article 25(1) for the reasons below. However, DPC believed ICB is a sole controller, not a part of joint controllers, thus Article 26(1) is not applicable for the case.

2.1 Article 5(2) and Article 24(1)

Article 5 [1] states that the controller needs to ensure security measures for the data protection and preserve the accuracy of the data. Article 24 [1] also emphasizes that the controller should ensure the measures and needs to be able to demonstrate the processing. While ICB had a good intention on the code change, DPC believed that ICB is a controller to

its database and failed to comply with these terms. ICB explained that it followed the testing procedures for the code changes as guided by ISO requirements. However, ICB was not able to demonstrate records for the testing and also failed to detect the removal of the filter at the time of testing even if it could cause significant risks on natural people. DPC also pointed out that submitted documents by ICB did not contain information on the risk analysis and measures to prevent risks.

2.2 Article 25(1)

DPC explained in its letter that ICB failed to comply with Article 25(1) such that it could not ensure the accuracy of the data during the breach (few months), did not measure the risk, and its testing measures were not appropriate.

1. Ensuring the accuracy of the data: ICB asserted that it relies on the accuracy of the data provided by its members; however, DPC pointed out *Huber v Bundesrepublik Deutschland* that, as the controller of the data in its database, ICB is responsible for ensuring the accuracy of the data while being stored and processed. Nonetheless, the code change resulted in inaccuracy and ICB reported some of these data to its members.

2. Risk analysis: DPC evaluated the risk of the data breach is high because the inaccurate information of the closed accounts might have resulted in credit refusal and the data subjects' decision toward finding alternative options, which could definitely impact rights and freedoms of the natural people. However, ICB failed to identify and test the risk.

3. Technical measures: as noted earlier, DPC explained that, even if ICB claimed to have the testing procedures for the code changes, it failed to keep the records for testing steps and also failed to test or identify the risk of the potential filter removal that was used for preventing updates on the closed accounts. Furthermore, DPC noted that the cost of adding these extra security measures would not require excessive costs to ICB.

2.3 Administrative Fine

Initially, DPC decided that €220,000 is appropriate given the number of data subjects impacted and the impact of the data breach as stated from Article 83(2)(a) of GDPR. However, DPC noted the actions taken by ICB after the incident such as informing the Data Protection Authority, its members as well as some of the data subject, fixing the error within few days and modifying its policy to prevent the potential data breach caused by developments in the future. Following are the list of fine reductions:

1. Article 83(2)(c): ICB took actions to mitigate the issues as mentioned above, thus reducing the fine by €55,000.

2. Article 83(2)(e): at the time of the incident report, ICB did not have any related case previously, thus reducing the fine by €25,000.

3. Article 83(2)(f): ICB actively cooperated with the authority by reporting the incident quickly and modified its policy to require formal approval for changes, thus reducing the fine by €50,000.

3 Discussion

The case illustrates how the controller needs to ensure that its policy is able to handle risks and prepare appropriate testing measures to prevent the risk. ICB's development process did not involve measuring the risks and the lack of testing documentation illustrates that the testing was not comprehensive enough to measure all risks that could have been involved. This case implies that simply following the ISO guidelines for its measure does not comply with the security measures described in GDPR. Furthermore, ICB's policy itself did not have strict management of the development process to ensure data protection. The failure of the error detection also implies that ICB's measure was not inclusive enough to detect the potential error after the adoption but relied on its members for the error detection.

ICB modified its policy to prevent the data breach in the future that explains what could have been done before the case. ICB could form a management team that analyzes risks before the development process and prepare a set of tests to ensure the risks are resolved. The development or other teams could document the design plan as well as testing procedures to comply with GDPR after the breach. ICB also could deploy the dynamic mechanism to keep logs of the processing after the adoption and monitor the logs for anomaly detection, instead of simply relying on reports of its users.

References

[1] General data protection regulation. https://gdpr-info.eu/.

[2] An Coimisiún um Chosaint Sonraí. Redacted_23̇03̇2021_decision_in1972p̈df. https://www.dataprotection.ie/sites/default/files/uploads/2021-05/Redacted_23.03.2021_Decision_IN-19-7-2.pdf.