GDPR Violation Case Study: Tusla's Data Breaches

Yingjie Xue
Brown University

Abstract

On May 17th, 2020, Tusla, Ireland's Child and Family Agency, was fined 75,000 Euros for violations of General Data Protection Regulation (GDPR). The reason for this fine is that information about children was wrongly disclosed to unauthorized parties. In this article, we investigate more details in Tusla's data breaches.

1 Introduction

On May 17th, 2020, Tusla became the first organization who was fined for General Data Protection Regulation(GDPR) violation in the State. The fine was issued by Data Protection Commission, and the amount of fine was 75000 Euros [8]. The fine was enforced after an investigation that was commenced by DPC in October 2019, in respect of data breach notifications that it had received from Tusla [7].

There were three cases that contributed to this fine, where information about children was disclosed to unauthorized parties. The data breaches happened and were reported to DPC by Tusla during February and May 2019 [6]. In the first breach, the contact and location information of a mother and child victim was disclosed to an alleged abuser. In the second breach, contact, location and school details of foster parents were accidentally disclosed to a grandparent. Consequently, the grandparent contracted the foster parent. In the third breach, the address of children in foster care was disclosed to their imprisoned father, who used it to correspond with his children [1].

The fine was issued due to the judgement that it violated were Article 5 and Article 6.

Background Tusla is a Child and Family Agency, which is now the State agency responsible for improving wellbeing and outcomes for children. It is dedicated to children protection, early intervention and family support services [3]. Tusla processes personal data to support the protection of children and for the welfare of families. Thus, the data it processes are high sensitive, e.g. health and welfare data, as well as criminal history information.

In these three data breach cases, the date subjects are the children and their family members involved in the cases. Tusla is both data controller and data processor.

Cause There is not much information about why this data breach happened. However, from an article [5] describing the data breach risks that Tusla suffers, and from its data breach history [4], we can guess that Tusla was not professional at protecting their data. According to the article [4], there were 71 breaches in the second half of 2018 and 130 incidents in 2019. The cases attributed to loss of an unencrypted device, unauthorized access to personal data, files getting lost or stolen and deliberate disclosures of sensitive information. The vast majority of the cases, a total of 163 out of 201, involved an "employee error or omission" [4]. Thus, my speculation is that the data breaches involved in this fine were caused by employee error or omission, where the employees accidentally sent the information to unauthorized parties.

After the data breaches When those data breaches were found, Tusla reported the data breaches to DPC in a timely fashion. After the investigation was completed in October 2019, Data Protection Commission (DPC) confirmed the fine in May, 2020 [8]. A spokesperson for Tusla said the organisation didn't intend to contest the fine and will accept and respect the DPC's (Data Protection Commission) decision.

2 GDPR Violation

As to this fine that DPC issued to Tusla, DPC claimed that Tusla violated Article 5 and Article 6, and the type for this infringement was defined as "Insufficient legal basis for data processing". Taking a close look at the article:

Article 5(f) [2] says, personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful

processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Apparently, Tusla has violated this clause since it disclosed personal information to unauthorized parties.

Article 6 [2] includes the justifications for lawfulness of processing, which Tusla lacked. Particularly, the data subjects include kids, which imposes more strict requirements for data processing.

3 Prevention

As indicated by the article [4], data breaches in Tusla are not uncommon. Tusla is suffering high risks of data breach [5]. For example, there was an inquiry that commenced in November 2018 regarding 71 personal data breaches. The cause of the breaches included inappropriate system access, disclosure by email and post. [6].

While there are some general factors to consider to protect data confidentiality, integrity and availabilities for any business, such as risk analysis, necessary encryption of data, access controls, security of IT equipment, and data backup and restoration, Tusla has something to focus on particularly. According to an investigation of data breaches in Tusla [4], the majority of those cases are caused by employ error or omission. For example, of 201 cases investigated, 47 were caused by an error involving sending data to incorrect email address. 51 cases involved postal address mistakes and 19 cases were described as "record shared in error". Thus, training employees to protect data is high priority. To name a few, the employees should be taught how to reduce risks when sending correspondence containing personal data. They should double check that the letter or email is addressed to the correct recipient and make sure that the recipient is a trustworthy individual and is entitled to receive the personal data. If sensitive data are sent, use password to protect them. The password should be sent to the recipient in another correspondence [9]. Some data breach cases involved stolen files and loss of devices. This indicated that Tusla also did not appropriately protect its IT equipments.

All in all, Tusla should hire data protection experts to help me set up their security settings for data protection or give them guidelines for set it up by themselves. After the setup, it is better to have security experts work as employees to protect the security of their IT equipment, especially network security on a daily basis. For example, the experts can help them manage the access control of personal data, make custom data security policies, train employees and protect their computers from network attack.

4 Discussion

If Tusla had not reported the data breaches to DPC timely, the fine would have been larger. The fine seemed fair from Tusla's point of view cause they did not intend to appeal. The fine that Tusla received warns every business of the importance of compliance with the data protection laws, i.e. GDPR in this context. DPC also demonstrates its determination to enforce its power to penalize those who violate GDPR.

5 Conclusion

In this paper, we investigated Tusla's violation of GDPR in detail, involving three data breaches in this particular case, where personal data were accidentally disclosed to unauthorized parties. We speculated that the probable reasons causing those data breaches are employee omission or errors. Then we give recommendations for prevent data breach from happening in the future. Especially, training employees to protect the data Tusla collects and processes is high priority.

References

[1] 2019 irish data protection commissions report. https://www.dataprotection.ie/sites/default/files/uploads/2020-02/DPC%20Annual%20Report%202019.pdf.

[2] Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[3] Welcome to the child and family agency website. https://www.tusla.ie/about/.

[4] Over 200 data breaches at tusla in year-and-a-half. August, 2020. https://www.irishexaminer.com/news/arid-40033076.html.

[5] Tusla suffers 23 'high risk' data breaches - including stolen files and loss of devices - since last year. August,2020. https://www.thejournal.ie/tusla-23-high-risk-data-breach-incidents-5177097-Aug20

[6] Tusla 'accidentally disclosed' contact and location information of mother and child victim to alleged abuser. February 2020. https://www.thejournal.ie/tusla-data-breaches-5014377-Feb2020/.

[7] Ireland: Dpc fines tusla 75,000 for three data breaches under the gdpr. May 2020. https://www.dataguidance.com/news/ireland-dpc-fines-tusla-75000-three-data-breaches-unde

[8] Colm Keena. Tusla becomes first organisation fined for gdpr rule breach. May 2020. https://www.irishtimes.com/news/crime-and-law/tusla-becomes-first-organisation-fined-for-gdpr-rule-breach-1.4255692.

[9] Mason Hayes & Curran LLP. Responding to personal data breaches in light of tusla gdpr fine. https://www.lexology.com/library/detail.aspx?g=cf2f2909-9f44-4c2a-b8b1-53360a293629.