GDPR Case Study for Doorstep Dispensaree Ltd.

Qiaonan Huang
Brown University

Abstract

This paper is a GDPR case study for a London pharmacy company called Doorstep Dispensaree Limited ("**Doorstep**") based on the official Enforcement Notice[1] issued by the UK Information Commissioner's Office ("**ICO**"). This is the first penalty notice issued by ICO under the GDPR regulation. The main violations of GDPR are focused on Articles 13 and 14, based on the information investigated and estimated by the Medicines and Healthcare products Regulatory Agency ("**MHRA**"). ICO issued this enforcement notice in December 2019 with an initial fine of £275,000. This was later appealed in February 2021 by Doorstep and reduced to £92,000, and the enforcement notice was upheld.

1. Background

On 24 July 2018, the MHRA executed a search warrant at one of Doorstep's premises. They found around 50 containers in the rear backyard, full of documentations that were neither secure nor marked as confidential waste. MHRA estimated there were around 500,000 documents, containing information such as names, addresses, date of birth, NHS number, medical information, and prescriptions. Under the GDPR regulation, we can treat Doorstep Dispensaree Limited as a controller, and the staff will be the processors for these documents. MHRA is the responsible data protection agency that executes the investigation and provided evidence. ICO then proceed with all the relative material and issued Doorstep with a penalty notice.

2. GDPR Violation

With this story provided upfront, the ICO first distinguished that Doorstep as a controller violated the data protection principle set out in Articles 5, 24, and 32. Then by referring to the privacy notice provided by Doorstep, the ICO also found it did not contain all the information required by Article 13 and/or 14.

2.1 Privacy Notice

When constructing the Privacy Notice, Doorstep did not follow the specific requirements on GDPR such as explicitly indication of the controller, purpose of data usage, and retention time. Customers of Doorstep were under a high risk of privacy leak because they did not have a right to access according to the Privacy Notice.

This incomplete Privacy Notice became a violation regarding Articles 13 and 14. It is important to let the customers know and have direct control over their own data. This includes what data is collected, where this data is collected from, how it is going to be used, and what will happen after it is used. Customers should also have the right to either delete or change that information on file. Without being fully informed of what the data will be used for, the customers are suffering from the unknown danger of personal information leaks.

2.2 Doorstep

Doorstep as a controller has an inevitable obligation. The action that exposed customers' data in the rear yard without adding any security protection was certainly a violation of Article 5, 24, 32 and the dereliction of duty of the employees. Doorstep here failed to provide a reliable encryption method for personal data, keep personal data in a secure place, equip the ability to make data restorable, and equip the ability to test the data security. Moreover, the employees here as processors left users' data in an insecure place, which is also a risky behavior.

However, instead of blaming the processors, I am more concerned about if there is any appropriate training and regulation for user's personal data. If Doorstep treats user's personal data more seriously and had some guideline on how to handle them, employees will have a better sense on how to handle these current or

outdated documents instead of leaving them unprotected in the rear yard.

2.3 Conclusion

The ICO reviewed all the documents and then issue Doorstep a penalty of £275,000 according to the annual turnover threshold annual turnover condition for small company categorization. The good news is that since Doorstep is a pharmacy store mainly located in London, and the documents were left in the rear yard of their own property, there was not a serious consequence for this omission. However, the behavior of the employees and the mindless construction of Private Notice showed Doorstep's unconsciousness of personal data protection. This penalty can give every small company a warning on how serious the GDPR will take in effect to protect personal data.

3. Discussion

This is notice certainly triggered the alarm of many small companies to rethink their attitude toward customer's personal data. It will gradually become companies' responsibility to provide a more robust and reliable strategy to protect their customers.

However, since this is an Enforcement Notice, there is some missing information such as how Doorstep responded and how it ended. This requires us to look for more information online to see the progress of this case. According to what I have found online [3], Doorstep appealed this notice after three months in February 2020 and the fine was reduced from £275,000 to £92,000, but the Enforcement Notice was upheld.

This notice is certainly a good reading material of GDPR no matter for laypeople or professional people. This case is illustrated as a story, including how this regulator is involved, what was happening inside Doorstep, how the consequence is drawn, and how it would affect current customers. It also illustrates what right the ICO has to issue this notice, which increases the reliability of this notice. For layperson looking at this notice, he can know what Doorstep violated customer's right, and what should be considered as appropriate behavior. For the technical person, this notice also includes all the specific points of articles in GDPR that are violated, which gives the technical person good references regarding the whole situation.

One thing I am concerned about is the time elapsed during the process. MHRA sent an email to ICO regarding this situation on 31 July 2018, but the notice came out and was finalized on 17 December 2019. It was initially reasonable to see about 17 months to do some investigations and conclude this case. However, when I refer to Ruairidh's article, I realize that ICO is using the estimated data provided by MHRA without further confirming. Doorstep in the appeal stated that "there were fewer than 75,000 in total, not all of which contained personal data and only a proportion of which contained special category data." [3]. This brings me some concerns about the processing speed. The GDPR is brought to the public in recent years, and we can expect that there will be more and more cases getting reported. Our eventual goal is protecting personal data under GDPR, so we also need more guideline that helps companies improve their privacy training. Instead of focusing on the penalty, regulating the investigation process and providing more training looks more like a sustainable way to achieve our goal.

Reference

[1]. Doorstep Dispensaree Ltd enforcement notice (ico.org.uk) https://ico.org.uk/media/action-weve-taken/enforcement-notices/2616741/doorstop-en-20191217.pdf

[2]. UK ICO Finally Issues GDPR Fine | Cleary Cybersecurity and Privacy Watch (clearycyberwatch.com) https://www.clearycyberwatch.com/2020/01/uk-ico-finally-issues-gdpr-fine/

[3]. Bitter pill for the ICO to swallow as fine on pharmacy reduced | Shepherd and Wedderburn (shepwedd.com) https://shepwedd.com/knowledge/bitter-pill-ico-swallow-fine-pharmacy-reduced