GDPR Case Study:
Doorstep Dispensaree Ltd

Sam Boger CS2390, Brown University, 2020

1 Introduction

In December 2019 the UK issued their first fine due to violation of the GDPR to the data controller Doorstep Dispensaree Ltd (DDL) for failure to properly secure and protect the personal information of their data subjects. DDL stored this information in documents that were not properly physically secured nor protected against damage from the environment. This was considered a serious violation in part because the documents contained personal medical information and identifiers. This report will discuss what went wrong in DDL's data protection practices, how the fine amount was decided, and what DDL and similar companies could do to prevent such violations.

2 Background

The EU's General Data Protection Regulation (GDPR) defines the responsibilities of *Data Controllers* and *Data Processors* who process personal information and similarly the rights of *Data Subjects* to have their information and privacy protected. It further describes how controllers and processors can be held accountable when they fail to meet those obligations. While this regulation certainly considers digital information processing, it is agnostic as to the mechanism of storage and explicitly covers data stored in traditional filing systems as well.[1]

DDL is a pharmacy supplier operating in several regions in England that provides delivery services particularly for the elderly and otherwise vulnerable [4]. To provide this service it seems reasonable that they would need information about their clients such as names, National Health Service (NHS) insurance numbers, prescriptions, and other personal details.

[1] "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." [7]

3 Origin of Investigation

The investigation by the Information Commissioner's Office (ICO) was initiated as a byproduct of the Medicines and Healthcare products Regulatory Agency (MHRA) conducting a separate investigation into DDL regarding possible unlicensed and unregulated medicine distribution which was later halted due to insufficient evidence. During the MHRA's search, permitted by a warrant, they identified "47 crates, 2 disposal bags and 1 cardboard box full of documents containing personal data" consisting of approximately 500,000 documents relating to an unknown number of data subjects and therefore notified the ICO of a possible GDPR violation [5].

4 The Violations

The primary problem identified by the The Information Commissioner ("the Commissioner") was that DDL stored the documents containing the personal information of the Data Subjects in an insecure area and that exposed the documents to damage from the natural environment. In particular, upon inspection some of the documents were "soaking wet". Furthermore, DDL's privacy policies given to customers did not adequately specify how their customer's data would be collected and processed [5]. As a result, DDL was found to have violated several articles of the GDPR, including articles 5, 13, 14, 24(1), and 32:

1. Article 5 specifies that data processing should prevent "unauthorized or unlawful processing and against accidental loss, destruction, or damage". Clearly the insecure storage and exposure to the elements did not live up to this requirement.

2. Articles 13 and 14 describe what information the privacy notice must contain, including reasons for processing the data, retention policies, where to file complaints, and the third party sources of their personal information. The Commissioner found all of these lacking in DDL's privacy notice.

3. Article 24 describes a responsibility of the data controller to implement procedures such that they are able to demonstrate compliance with the GDPR's provisions, which presumably DDL was unable to do.

4. Article 32 lists requirements for security of processing, including ensuring availability of personal information, which again was not possible due to DDL's information storage practices.

5 The Fine

The Penalty Notice contains the fine levied against DDL, 275,00 GBP, and the rationale for the amount. Factors against DDL included that the Commissioner was notified of the incident by MHRA, not DDL itself, as well as general resistance to the investigation as perceived by the Commissioner. The notice describes the data protection practices of DDL as "cavalier" and demonstrating "negligence". Another factor was that the data subjects whose rights were violated were largely elderly and otherwise vulnerable and that the data was "special category data" which includes sensitive health information. Lastly, DDL attempted to implicate a waste disposal company Joogee Pharma Limited who it claims should have properly disposed of the documents in question, but the Commissioner deemed them a data processor and otherwise still claimed DDL was the data controller responsible for the violations. In favor of DDL, the notice describes that they have taken steps to improve data protection training for their employees and clarified some of their policies since the enforcement, although that work is incomplete and ongoing. The overall conclusion was that the violation was "extremely serious". [6]

6 Prevention

The enforcement and penalty notices describe how to prevent such violation. Data controllers, and in particular those who process medical information, need to take this regulation seriously and adhere to the spirit and detailed requirements in the GDPR. In particular, DDL needed to either secure and protect these documents, or ensure their proper destruction perhaps by shredding them. Another note of concern from the Commissioner was that the data protection policies were vague and mostly templates of existing policies, rather than specific to their business. This signals that there is an expectation that data controllers will avoid boilerplate best practices and must instead describe their particular use cases.

7 Broader Impact

Several media pieces describe this case and all note that this was the first actual fine issued due to GDPR violations in the UK. [1] [3] [2] Other noteworthy aspects include that it concerns physical documents and in particular the insecure storage and maintenance of the information. This shows that all aspects of processing including retention, protection, and deletion, are pivotal components of the GDPR, not just provisions against improper use or collection of such information.

8 Conclusion

DDL failed to protect the information they possessed of their data subjects by leaving documents unprotected and exposed to the elements. The ICO investigated and eventually issued a substantial fine. The scope of the GDPR is intentionally broad, covering small and large business, digital and physical documents, and negligence as well as nefarious misuse. This case affirms that all data controllers should consider GDPR violations as legal, PR, and financial risks that can be prevented with relative ease compared to fighting against investigations and fines.

References

[1] London pharmacy fined after careless storage of patient data. *European Data Protection Board*, 2019. https://edpb.europa.eu/news/national-news/2019/london-pharmacy-fined-after-careless-storage-patient-den.

[2] Laura Donnelly. Pharmacy receives first ever fine for breaking gdpr rules. *The Telegraph*, 2019. https://www.telegraph.co.uk/news/2019/12/20/pharmacy-receives-first-ever-fine-breaking-gdpr-rules/

[3] Luke Irwin. Doorstep dispensaree becomes the first uk organisation to receive a gdpr fine. *IT Governance*, 2019. https://www.itgovernance.co.uk/blog/doorstep-dispensaree-becomes-the-first-uk-organisation

[4] Doorstep Dispensaree Ltd. dispensaree.co.uk.

[5] Stephen Eckersley of the Information Commissioner's Office. Enforcement notice to doorstep dispensaree ltd. 2019. https://ico.org.uk/media/action-weve-taken/enforcement-notices/2616741/doorstop-en-20191217.pdf.

[6] Stephen Eckersley of the Information Commissioner's Office. Penalty notice to doorstep dispensaree ltd. 2019. https://ico.org.uk/media/action-weve-taken/mpns/2616742/doorstop-mpn-20191217.pdf.

[7] The European Parliament and the Council of the European Union. Regulation (eu) 2016/679 (general data protection regulation). *Official Journal of the European Union*, 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.