UK Court Reduces ICO GDPR Fine By Two-Thirds

Date : September 10, 2021

Introduction

In the recent court ruling in the case of Doorstep Dipsensaree Limited v The Information Commissioner, the UK's First-tier Tribunal ("the Tribunal") reduced a fine for data protection breaches imposed by the UK regulator the ICO under EU GDPR by two-thirds on the basis that the number of individuals affected by the breach had been significantly overestimated by the ICO; we wrote about the original ICO decision here https://www.corderycompliance.com/first-uk-gdpr-fine/. This article sets out highlights of the ruling.

What's this all about?

In July 2018 the Medicines and Healthcare Products Regulatory Agency ("MHRA") undertook a search (under a warrant) at premises (a yard) used by a waste disposal business which had been tasked (as data processor) with destroying material containing personal data for which Doorstep Dipsensaree (a pharmacy) was the data controller. The owner of Doorstep Dipsensaree also owned the waste disposal business and the premises in question.

The MHRA informed the ICO that 47 stacked, unlocked crates had been recovered from the premises which contained both personal data and special category personal data that related to Doorstep Dipensaree's pharmacy business; the MHRA subsequently sent the ICO a memory stick containing images and video footage of the premises at the date of the search warrant, as well as sample documents. The MHRA told the ICO that approximately 500,000 documents had been recovered and that the data in question concerned residents in care homes including the following data: names; addresses; dates of birth; National Health Service numbers; medical information; and, details of prescriptions. Similar material was also found in two disposal bags and in a cardboard box. Needless to say, under EU GDPR (and UK GDPR), as so-called special category data, extra protection is required for health data.

In December 2019, having initially considered imposing a fine of £400,000, the ICO imposed its first fine under EU GDPR of £275,000 on Doorstep Dispensaree for leaving around half a million documents unsecured at the back of its premises.

At the time of the search, many of Doorstep Dipensaree's data protection policies and procedures were not up to date and did not comply with EU GDPR: only two policies referred to EU GDPR, which were provided as blank templates; there was no data retention policy; the "Standard Operating Procedure – Disposals of Medicines Policy" had been backdated to August 2018, having been drawn up in February 2019; and, the other policy documents had not been updated to reflect EU GDPR.

Therefore, the ICO also ordered Doorstep Dispensaree to comply with various measures including updating all of its policies and procedures to ensure data protection law compliance.

Doorstep Dispensaree appealed against the fine arguing that fewer than 75,000 documents were involved, only some of which it claimed contained personal data and special category data. It also disputed that it was the data controller with regard to some of the data. It also appealed against the compliance measures.

What was the court's ruling?

The court allowed the appeal in part where it ruled as follows:

- An audit of the material undertaken by Doorstep Dispensaree's legal counsel identified that only 73,719 documents had been recovered from the premises in question and, of these: 7,351 contained no personal data; 6,229 contained a name only; 6,268 contained a name and address only; and, approximately 53,871 contained special category data. The Tribunal accepted this as reliable evidence and concluded that this therefore undermined the ICO's reliance on the 500,000 documents figure which it had wholly relied on

from the MHRA (which the ICO had only viewed a sample of at MHRA's premises) and which it had based the level of the fine on;

- However, the Tribunal found that, for various reasons, Doorstep Dispensaree was the data controller of the data processed by the waste disposal business;
- Further, the Tribunal also found that "the yard was not an appropriately secure area in which to store personal data, due to the fact that the yard could be accessed by the occupants of and visitors to three residential flats, via fire escapes that as a matter of common sense must be readily accessible. The unlocked crates in the yard could also potentially be accessed by business visitors to the Property. I conclude from this that [the waste disposal business'] methods of data storage was not appropriately secure and did not afford sufficient protection against accidental loss or destruction, and that this was a breach of the integrity and confidentiality requirements [under EU GDPR] for which [Doorstep Dispensaree] retained responsibility";
- In addition, the Tribunal found that "at the date of the search warrant [the waste disposal business] was storing personal data in a form that permitted identification of data subjects for longer than necessary. This is because the presence of personal data that was two or more years old indicates that not all data was destroyed when it was no longer required. [Doorstep Dispensaree] has confirmed that historic, hard copy documents were not required for record keeping purposes. Given […] the absence of any evidence that the historic records had only been passed to [the waste disposal business] for destruction recently, I am satisfied that the retention of this data by [the waste disposal business] was a breach of the storage limitation requirements of [EU GPDR] for which [Doorstep Dispensaree] also retained responsibility […]. I note in addition that […] no contemporaneous evidence has been adduced to show when and how [the waste disposal business] securely destroyed personal data on [Doorstep Dispensaree's] behalf";
- Also, the Tribunal found that "[Doorstep Dispensaree's] failure to devise adequate data processing policies contributed to [the waste disposal business'] breaches of relevant data processing requirements. In particular, I find that the absence of a retention policy and of a clear explanation by [Doorstop Dispensaree] of the processes [the waste disposal business] must follow when destroying personal data incidental to the destruction of medicinal waste must have contributed to [the waste disposal business'] breaches as it was provided with no appropriate procedures to follow. I conclude as a consequence that [Doorstep Dispensaree's] responsibility for [the waste disposal business'] breaches also amount to a breach of the requirements of [EU GDPR], in that [Doorstop Dispensaree] failed to implement appropriate and organisational measure to ensure that [the waste disposal business'] processing was performed in accordance with [EU GDPR], as well as a breach of the requirements of [EU GDPR], in that [Doorstop Dispensaree] failed to implement appropriate measure to ensure a level of security appropriate to the risks";
- Finally, the Tribunal noted "in particular the [ICO's] conclusions as to the gravity of the breach and the risk of significant emotional distress being caused to a vulnerable group of data subjects were they to become aware of the contraventions. I also agree with the [ICO's] conclusion that the serious breaches of the data processing principles occasioned by [the waste disposal's business] activities were largely due to [Doorstop Dispensaree's] negligence in relation to its [EU GDPR] obligations";
- In conclusion, given the gravity of the breaches along with the aggravating factors, the Tribunal was "satisfied that the level of the penalty imposed should not be reduced by a percentage based on solely on the lower numbers of documents" and so, all things considered, the fine was cut by two-thirds from £275,000 to £92,000. The Tribunal also upheld the compliance measures that the ICO had ordered Doorstop Dispensaree to undertake, notably drawing attention to Doorstop Dispensaree's data protection policies which it seemed to still be relying on "some of which are incomplete and unclear".

It is not yet known whether either party will appeal the ruling.

What are the takeaways?

The takeaways are as follows:

- It is always worth considering whether a fine can be appealed – carefully review the basis on which a regulator has based its findings and consequent fine;
- Make sure that your policies and procedures are complete, up to scratch and up to date, including your

respective data retention and data destruction/disposal policies;
- Ensure that you take special care with personal health data;
- Make sure that it always made clear in your arrangements with vendors as to who is the data controller and who is the data processor; and,
- Last but by no means least, always make sure that you dispose of personal data securely!

Resources

Cordery's GDPR Navigator subscription service is an expansive set of resources and a community of peers helping companies deal with GDPR and related issues. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

The Tribunal's judgment can be found here Doorstep Dispensaree Tribunal Appeal Decision August 2021

We have written about the ICO's fine on B.A.
here https://www.corderycompliance.com/ico-fines-ba-for-data-breach/ and the ICO's fine on Marriott
here https://www.corderycompliance.com/ico-fines-marriott-for-data-breach/.

We report about data protection issues here https://www.corderycompliance.com/category/data-protection-privacy/.

We report about compliance issues here https://www.corderycompliance.com/news/.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1784
jonathan.armstrong@corderycompliance.com

Andre Bywater
Cordery
Lexis House
30 Farringdon Street
London EC4A 4HHOffice: +44 (0)20 7075 1785
andre.bywater@corderycompliance.com