What has been the ICO's attitude to GDPR enforcement?

Victoria Hordern of Bates Wells considers what we can learn from the ICO's actions so far.

A law that is not consistently enforced is arguably not worth the paper it's written on. The General Data Protection Regulation 2016/679 (GDPR) was designed to strengthen the rights of individuals and the powers of regulators. The GDPR deliberately has an anti-trust style approach to fines e.g. 2% or 4% of global annual turnover. It's a framework which allows data protection authorities to bring out a hefty stick when they consider it to be justified. In particular, there had been concerns under the previous regime of the Data Protection Directive 95/46, that many EU Data Protection Authorities had limited ability to issue fines and so were without proper deterrents to punish bad practices. For sizeable multinationals, the fines that those Data Protection Authorities imposed were small change.

Since May 2018 Data Protection Authorities in the EU have begun enforcing the GDPR. To date, Spain appears to have been the most frequent enforcer. However, at the time of writing, Ireland has not issued a fine under GDPR. The biggest GDPR fine imposed so far has been the €50 million fine against Google in France in January 2019. Unsurprisingly, shortly afterwards, Google indicated that it would appeal the fine. One of the consequences of regulators issuing multi-million euro fines to global players is that those global players are more likely to appeal. Faced with the prospect of shelling out €50 million, evidently Google decided that it was worth opposing the fine despite the associated costs of fighting the action.

For Data Protection Authorities (DPAs), this could become a pattern which, paradoxically, leads to lower fines. Appeals of regulators' decisions take up valuable time and resources for them. Will the DPAs across the EU be able to take on the substantial players if levying high fines will bring legal challenges? If regulators face increasing challenges to the enforcement actions they impose, governments will need to step up to ensure that regulators are given proper independence and resources to carry out their role effectively.

Enforcement in the UK

What about GDPR enforcement activity in the UK? The Information Commissioner, Elizabeth Denham, publicly indicated in one of her myth-busting blogs in 2017 that it was scaremongering to suggest that the Information Commissioner Office (ICO) will be making early examples of organisations for minor infringements or that maximum fines will become the norm. And this is broadly how the past two years have unfolded.

While there is no legal requirement on the ICO to publish its intentions to fine, it did so for British Airways and Marriott International Inc. in July 2019 because both companies were under public reporting obligations due to their position as listed entities. Therefore, the ICO's statements on the two companies were in response to the public announcements that the two companies had themselves respectively made. Once an intention to fine is given by the ICO, there is a six-month period within which the organisation has the opportunity to put forward its arguments. But this period may be extended by agreement between the ICO and the organisation – this appears to have been what has happened with both BA and Marriott since we have not yet (at the time of writing) seen confirmation of any GDPR fines for these two companies[1].

> The ICO has been criticised as being slow off the mark in enforcing the GDPR.

But there was an early GDPR enforcement action in October 2018 where the ICO issued an enforcement notice against a Canadian company, Aggregate IQ. Under the enforcement notice, Aggregate IQ was required to notify the Information and Privacy Commissioner of British Columbia that it had deleted the personal data of UK individuals within 30 days. What was interesting about this regulatory action is that it related to an overseas company (a reminder that GDPR regulatory powers are extra-territorial). It also involved the ICO working with a regulator outside the EU (although Elizabeth Denham having previously held that role in British Columbia presumably helped!) and it was a response to the Cambridge Analytica data scandal.

We haven't seen any enforcement action yet by the ICO in other areas where it has been focusing its energies, for instance, in the world of adtech. Many will be aware that the ICO has been spending time and resources dealing with the complaints it has received about the use of data by the adtech industry (particularly real time bidding). The ICO identified the adtech sector as a priority, produced an update report in June 2019 and has indicated recently, in a January 2020 blog, that certain changes have already been made by the industry to deal with the ICO's concerns. However, despite this progress towards compliance by some players, the ICO highlights that others have their 'heads firmly in the sand' and consequently anticipates taking formal regulatory action in due course.

Or what about the use of cookies? As is well known, the advent of the GDPR influenced the concept of consent under the Privacy and Electronic Communications (EC Directive) Regulations 2003. The rules are pretty clear.

You need to obtain prior consent (to the GDPR standard) before placing cookies/ trackers that are not strictly necessary (or required as part of a communication transmission) onto a user's device. But compliance with this rule is not widely practised! Many websites are still getting to grips with the implications of the requirements. Arguably, a lack of regulatory enforcement in this area encourages an environment where organisations consider compliance to be optional.

The ICO has been criticised as being slow off the mark in enforcing the GDPR. While there are situations where perhaps a firmer and more rapid response would be welcome, Article 83 requires the ICO to ensure that any fine imposed is effective, proportionate and dissuasive.

The first GPDR fine from the ICO

The first GDPR fine issued by the ICO was in December 2019 where a London based pharmacy was fined £275,000. Unfortunately, the way Doorstep Dispensaree Ltd (Doorstep) handled its data protection compliance was wrong from the beginning. As a company that supplies prescriptions to residents at care homes, it was regularly dealing with health information (i.e. special category data) of vulnerable individuals. What it had failed to do was implement a system for securely retaining and disposing of the documents associated with the prescriptions. So it had no suitable policies detailing the process that would be followed, it had no clear training framework for staff, and the arrangement with the third party processor it engaged to dispose of documents was clearly not working.

Significantly, the ICO became aware of the poor practices of Doorstep because of an investigation being carried out by another regulator – the Medicines and Healthcare products Regulatory Agency (MHRA). It was the MHRA that located unlocked crates, bags and a box with 500,000 documents containing personal data on Doorstep's premises. The documents contained names, addresses, dates of birth, NHS numbers and medical information. A number of the documents dated back to 2016. The MHRA promptly informed the ICO and the ICO began communicating with Doorstep seeking to obtain further information about its data processing practices.

Regrettably the response of Doorstep to the ICO was not constructive and eventually the ICO had to issue an Information Notice as Doorstep did not answer the ICO's questions. Doorstep then went on to appeal the Information Notice on the grounds that to comply with the Information Notice would involve it in a risk of self-incrimination (an exception permitted under s. 143(6) Data Protection Act 2018) since it was the subject of a criminal investigation by the MHRA. The Tribunal ruled against Doorstep because it provided limited information about the scope of the criminal investigation and the scope for self-incrimination.

Eventually Doorstep provided information to the ICO but it was unfortunately inadequate, comprising policies that had not been updated for the GDPR, poor practical guidance for staff and reliance on template procedures that had clearly not been implemented. Although Doorstep began to improve its GDPR compliance as a result of the ICO's involvement, the ICO considered the breaches to be too serious. It imposed a monetary penalty notice and an enforcement notice.

The focus of the ICO's enforcement action, and why it considered a penalty was justified, related to non-compliance with Articles 5(1)(f), 24 and 32 as well as Articles 13 and 14. In other words obligations around security measures, accountability and transparency. Importantly, it did not matter that there was no evidence that any unauthorised person had accessed the data. Nor did it matter that no harm was demonstrated. While the Penalty Notice appears to reveal other areas of non-compliance, it is significant that these areas are not ones the ICO chose to enforce against Doorstep. For instance, while the Penalty Notice refers to obligations of Data Protection by Design and by Default, the failure of Doorstep to implement such measures does not appear to have been a factor in the fine. Additionally, the Penalty Notice refers to a third party processor who Doorstep blamed for the non-compliance. No contract between Doorstep and the processor was produced to the ICO, which would suggest a breach of Article 28, but again the ICO does not focus on this omission. Moreover, in Doorstep we have an organisation whose core activity was processing health data (potentially on a large scale), but there is no discussion in the enforcement notices of whether Doorstep had breached Article 37 (appointment of a DPO) nor Article 35 (carrying out a data privacy impact assessment).

Doorstep got it so badly wrong because it failed to understand its obligations under GDPR. It acknowledged the powers of the ICO too late and adopted a cavalier attitude to compliance. The fine was originally intended to be £400,000 but the ICO reduced it (NB. the previous policy of a discount for early payment has vanished). It appears that this was due more to the financial position of Doorstep rather than any enthusiasm from Doorstep to make up for its poor level of compliance. Given the number of individuals affected by the contraventions and the sensitive data at stake, potentially the fine should have been higher. Although, while the non-compliance appears to have stretched back to 2016, the ICO only considered the period of 25 May 2018 – 31 July 2018 in reviewing what enforcement action under the GDPR it should take.

Curiously, the Penalty Notice also refers to a requirement which appears to contradict ICO guidance elsewhere. So the Penalty Notice indicates that, as Doorstep's Privacy Notice did not state the Article 9 (processing special category data) condition, this was a contravention. However, the ICO's guidance on special category data (published November 2019) states that an organisation does not have to state which condition under Article 9 it is relying on in the privacy notice. Evidently organisations need to understand what the regulator's expectations are in order to consistently aim for compliance.

So what are the implications?

The assessment of the action against Doorstep offers a useful case study of the ICO's GDPR enforcement. Clearly this was an example of gross non-compliance given the sensitivity of the data,

number of affected individuals and substantial gaps in GDPR compliance. In both the Penalty Notice and Enforcement Notice the importance of accountability and evidence of accountability is evident. The Enforcement Notice sets out the requirement on Doorstep to update policies, procedures and Standard Operating Procedures to ensure compliance with data protection law including explaining staff responsibilities, giving advice to staff on data handling and secure disposal. Additionally, Doorstep must appoint a staff member to ensure that security measures are adhered to and to investigate security incidents. The ICO also requires Doorstep to instigate mandatory staff training and regular refresher training every 2 years and ensure staff are familiar with policies and procedures. One of the lessons of the Doorstep enforcement action is to ensure an organisation has a proactive approach to engaging with the ICO; everyone across an organisation should understand the importance of responding promptly to the ICO.

AUTHOR

Victoria Hordern is Partner and Head of Data Privacy at Bates Wells.
Email: V.Hordern@bateswells.co.uk

REFERENCE

1 We believe the ICO is currently considering the representations that have been made by both companies to decide what action to take. Additionally, the companies and the ICO have reportedly agreed to an extension of the regulatory process until 31 March 2020.

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

UK seeks an independent data protection policy

Full alignment with the GDPR cannot be taken for granted any longer as Boris Johnson, the Prime Minister, steers away from commitments made in the Withdrawal Agreement. By **Laura Linkomies**.

The UK's negotiating mandate with the EU on the UK-EU future relationship, published on 27 February, states that the "UK will have an independent policy on data protection at the end of the transition period and will remain committed to high data protection standards". This strategy is set and the focus is now on making it work.

The UK is seeking two adequacy decisions from the EU (one under

Continued on p.3

ICO publishes final online Age Appropriate Design Code

DPIAs, high level privacy settings and switching profiling "off" by default are aspects required by this code, subject to Parliamentary approval. By **Ben Slinn** of Baker & McKenzie.

On 21 January 2020 the ICO published its Age Appropriate Design Code of practice for online services following a public consultation in April 2019[1]. The ICO is required to prepare this statutory Code under Section 123 of the Data Protection Act 2018. In terms of next steps, the Code needs to be approved by Parliament, and following such approval there will be a 12-month transition period before

Continued on p.4

Issue 108 **MARCH 2020**

UNITED KINGDOM
report

ISSUE NO 108 **MARCH 2020**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS

Ben Slinn
Baker & McKenzie

Victoria Hordern
Bates Wells

Marta Dunphy-Moriel and Alexander Dittel
Kemp Little

Abigail Dubiniecki
Strategic Compliance Consulting

Claire Robson
Great Ormond Street Hospital Children's Charity

Emma Erskine-Fox and Gareth Oldale
TLT

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2047-1479

comment

Negotiations on EU-UK future relationship start in Brussels

The first round of the EU-UK future partnership negotiations have started, and will be followed by further negotiation rounds every two to three weeks in Brussels and in London. A high-level meeting is planned for June 2020. For data protection, if negotiations on adequacy for data transfers from the EU to the UK are simply at a technical level, the proposed timescale (end of 2020) could just be workable. However, at a political level, if data protection is used as a bargaining chip in the negotiations, things get much more complicated.

In the meantime, the UK is starting to conduct its own adequacy assessments (see p.1). It is hoped that the UK adequacy assessments and decisions can be taken more quickly than the EU has done, but this remains to be seen. For now, everything remains business as usual as the GDPR will continue to apply in the UK, and UK and EEA-based controllers will not need to take any immediate action. But as the Prime Minister seems to be more than willing to steer away from the GDPR, we need to monitor developments closely and, no doubt, organisations are paying even more attention to alternative transfer mechanisms.

In this issue we assess developments in biometrics (p.19 and p.22), and the emerging Children's Code which still needs Parliamentary approval but will signify a shift in attitudes and practice (p.1). A different kind of dilemma is the interface between anti-money laundering and data protection laws. Can there ever be common ground? Perhaps, suggests our correspondent on p.14.

The ICO is considering its role in the data ethics debate with a view to launching a public consultation in the second quarter of 2020. Read my interview with Ellis Parry, who is the ICO's newly appointed Data Ethics Adviser, Technology and Innovation. The ICO is again expanding its horizons to new areas (p.7).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

privacylaws.com/reports

"*PL&B* reports are one of the best sources of data protection information available today, especially the articles written by experienced practitioners who generously share insights and knowledge. In terms of quality, *PL&B* reports are in a league of their own."

Lucy Inger, Director, Lawmatrix

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.