ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The controller/processor dilemma: EDPB consults on guidance

One of the first questions an organisation must ask itself when considering its data protection compliance responsibilities is: "Are we controller or processor?" By **Emma Erskine-Fox** of TLT.

These concepts are by no means new, but the General Data Protection Regulation 2016 (GDPR) has caused organisations to think more carefully about their own roles and those of the third parties they exchange data with. The assessment is often not as straightforward as one might hope.

On 7 September 2020, the European Data Protection Board (EDPB) released draft guidelines on the

Continued on p.3

Enforcement guidance: ICO says it will not shoot to kill

Marta Dunphy-Moriel and **Alexander Dittel** of Kemp Little assess the guidance which was issued immediately before the much reduced BA and Marriott fines.

If we had taken a bet last year, most people would have been convinced that the ICO would issue huge GDPR fines. These would have been calculated based on turnover even if the issue had been caused by a malicious cyber attack. Evidence of this approach was the ICO's announcement of its intention to issue the extraordinary fines of £183.39 million to British Airways[1] and £99 million to Marriott International[2] in

Continued on p.5

New PL&B resources

- PL&B's Data Protection Clinic: Book a 30 minute consultation to help resolve your Data Protection issues. The clinic will support you in identifying your key priorities and much more.

www.privacylaws.com/clinic

- PL&B's *Privacy Paths* podcasts are available at www.privacylaws.com/podcasts and from podcast directories. Topics include controller-processor agreements and success stories from the ICO's regulatory sandbox.

Issue 112 **NOVEMBER 2020**

PL&B Services: Conferences • Roundtables • Content Writing
Recruitment • Consulting • Training • Compliance Audits • Research • Reports

ICO... from p.1

2019. However, for those ever sceptical amongst us, this image did not quite sit with the ICO's reputation or normal business practice. And that is a good thing, because it is our experience that being an assertive, reasonable and professional regulator is the best way to influence market practices.

A REASONABLE AND PRAGMATIC REGULATOR?

The ICO has long branded itself as a reasonable and pragmatic regulator. While 2019 made us doubt that, we now know that a measured approach has prevailed as the ICO reduced the British Airways fine to £20 million[3] and the Marriott fine to £18.4 million[4]. The turnover-based calculation was abandoned, the new starting figures were much lower and they were further reduced on account of economic hardship and the impact of the pandemic.

The ICO's primary focus is in keeping personal data safe. Some of its most significant fines related to information security failings including the then maximum of £500,000 imposed on Dixons and the same on Cathay Pacific in 2019. Previously, the TalkTalk fine of £400,000 in 2016 (*PL&B UK* September 2016 p.10) for information security failings took the top spot. Even the first ever ICO GDPR fine related to information security. Doorstep Dispensaree was fined £275,000[5] for persistently failing to cooperate but importantly, for leaving approximately 500,000 documents with medical records in unlocked containers in a backyard, exposed to the elements and malicious actors. The ICO's message is clear: Get your information security in order!

The ICO has been investigating market sectors such as the adtech industry. But instead of issuing fines, it has been working with the industry to understand and improve data processing practices. Other than the Bounty fine of £400,000[6] imposed under the old regime for illegally sharing personal information belonging to more than 14 million people, the ICO has not issued any significant fines in relation to intrusive profiling, invisible processing and data sharing. Having said that, the ICO's updated marketing code of practice for consultation[7] and its recent review of the broking sector,[8] perhaps herald the beginning of more enforcement in this field.

Unlawful marketing practices dominate the ICO's fines each year, which is likely due to reports from members of the public. The fines typically do not exceed £200,000 which is reserved for high volume offenders.[9] However, even in this area the ICO will be robust in case of intentional large scale for-profit contraventions as was the case with CRDNN which received the maximum fine of £500,000 under the e-Privacy Regulations (PECR)[10] in relation to 63.5 million automated calls.[11]

WHAT DO OTHER REGULATORS DO?

Looking at cases in other European countries, we see a real mixture of regulatory focus. For example, the Italian *Garante* which has been topping the GDPR fine charts this year seems to award the highest fines for direct marketing malpractice affecting large number of people. €27.8 million was awarded against telecommunications operator TIM,[12] €16.7 million against telecommunications operator Wind Tre S.p.A.[13] and €11.5 million against *Eni Gas e Luce*.[14] Each fine related to marketing. Perhaps the intentional and large scale nature of these breaches warrant these fines, but this is where the ICO's enforcement is not comparable as its hands are still tied by a £500,000 maximum under PECR.

On the other hand, the German authorities investigate more fundamental contraventions. For example, the Berlin authority fined *Deutsche Wohnen* €14.5 million[15] for its unjustified retention of tenant data. The Hamburg regulator recently surprised observers with a €35 million fine imposed on H&M[16] for intrusive profiling of hundreds of its employees.

The Belgian regulator seems to dish out fines for a variety of contraventions, such as the relatively high fine of €50,000 for an arguably harmless DPO conflict of interest.[17] The Belgian, Spanish and French authorities have also issued fines in relation to cookies, despite the ongoing discussion at European legislative level about how cookies should be regulated in future. The French regulator also made headlines when imposing a €50 million fine on Google for profiling,[18] which remains the highest GDPR fine to date.

In contrast to some of its European counterparts, the ICO's enforcement does seem more focused and consistent. However, it is difficult to compare approaches as each fine is decided on its facts and the realities in each member state.

WITH GREAT POWER COMES GREAT RESPONSIBILITY

According to the ICO, in protecting the rights and freedoms of individuals in the digital age, it will be as robust as necessary in upholding the law whilst ensuring clarity about enforcement and consistency. Businesses should be able to operate and innovate efficiently without red tape or concern about disproportionate sanctions. Indeed, the ICO tends to enforce data protection obligations which are clear and sufficiently established as good practice.

The ICO's new *Statutory guidance on our regulatory action* provides a good deal of clarity about enforcement. It relates to powers under the Data Protection Act 2018, but much of the language is borrowed from the existing 'Regulatory Action Policy 2019-2021' which covers the ICO's wider powers. Helpfully, the proposed guidance expands on the methodology of calculating fines, and the offending organisation's turnover is now a consideration rather than a determining factor.

WHEN AND HOW WILL FINES BE IMPOSED?

Fines will be reserved for serious breaches by a controller or processor, such as intentional or negligent acts, repeated breaches or particularly harmful breaches. As a general rule, each fine will be a fair and proportionate sanction to punish the offending organisation but also an effective deterrent that will promote future compliance.

The ICO's risk-based approach means that its focus is on the areas of highest risk and harm. A fine may be appropriate for high volume breaches, lack of lawful basis or transparency, sensitive processing capable of causing distress or embarrassment as well as a failure to comply with an investigation or previous recommendations, and failure to mitigate.

In setting the penalty, the ICO clarified nine steps:

- Step 1 is an assessment of seriousness

by considering the nature, gravity and duration of the contravention but also the offender's cooperation, mitigation and how the contravention came to light.
- Step 2 is about assessing the degree of culpability looking at the offender's practices and safeguards as well as any processor failures.
- Step 3 will determine the turnover or equivalent.
- In step 4, the ICO will calculate an appropriate starting point based on turnover or fixed maximum. According to the British Airways penalty notice,[19] turnover may but will not always be the starting point for the calculation of fines. A percentage will be applied to that amount, fixed according to the degree of seriousness and culpability.
- Step 5 considers aggravating and mitigating factors, such as illicit financial gain, intent, response time, and whether or not special category data was affected. These factors helped reduce the British Airways and Marriott fines.
- In steps 6 and 7 the fine will be reduced to lessen any undue financial hardship and to promote economic growth, which also helped reduce the British Airways and Marriott fines.
- Step 8 is a final review of the proposed fine's effectiveness, proportionality and dissuasiveness.
- In step 9 a 20% early payment discount will be applied if the controller does not appeal.

Organisations will be reassured that the ICO will always consider all these factors. The offender will have 21 days to comment on a notice of intent. In rare cases, representations can be made verbally. Generally, the Information Commissioner or another senior officer will decide on the final penalty. For significant penalties, an advisory panel may be consulted.

Anything else in the ICO's enforcement toolbox?

Information notices: The ICO will often send informal information requests. However, if there is a need to test responses or take urgent action to secure evidence, a formal information notice will be served. For example, Doorstep Dispensaree[20] was served an information notice only after two failed attempts to obtain information two months into the investigation. In rare cases, the ICO can request that information be provided within 24 hours.

Assessment notices: An assessment notice will require access to premises, documentation or equipment for the ICO to assess compliance. It will be served where evidence suggests a lack of compliance or raises doubts about compliance. In a recent example, the ICO served assessment notices on credit reference agencies Experian, Equifax and TransUnion during its investigation into analytics for political campaigns.[21]

The ICO will consider the burden of an inspection on the audited party and will accommodate reasonable requests on how it should be carried out. However, in urgent cases, access may have to be granted within just seven days or even without notice if there are reasonable grounds to suspect an ongoing contravention or an offence being committed.

The ICO will inspect and examine materials and interview individuals. Interviews will be conducted to understand the underlying working practices or awareness but questions will not be framed as a test or to catch people out.

The ICO may access both manually and electronically stored data, data on mobile devices or media. The ICO may access privileged information except for privileged information relating to data protection legislation. The ICO may take data off site.

The resulting audit report will explain conclusions with reasoning and recommendations. Following its assessment, the ICO may decide that no further formal action is needed. Alternatively, it may commence formal enforcement action.

Search warrants: Court orders will be used where a party fails to comply with any notices. A search warrant will be used in rare cases where the party fails to respond or where required to preserve evidence. For example, the ICO executed a search warrant to access CRDNN Limited which was making automated calls using calling line identity numbers which were concealed as international calls. The ICO seized emails that indicated the directors' awareness of PECR requirements.

Enforcement notices: Enforcement notices compel the offender to remedy any repeated failures, serious ongoing infringements, transfers to third countries, or other contraventions. Timing is often dictated by feasibility. For example, following a two-year investigation Experian was recently given nine months to act on the ICO's recommendations.[22]

Where appropriate, the ICO may share a preliminary enforcement notice for comments by the offender.

Fixed penalties and prosecutions: The ICO can also issue fixed penalties ranging from £400 to £4,350 for a lack of cooperation or non-compliance with notices.

Prosecutions: Every year the ICO prosecutes individual offenders who commit criminal offences under the Data Protection Act 2018. Examples include offenders who steal their employer's data for illicit gains[23] but also staff who delete data to prevent disclosure.[24] The ICO has the power to prosecute under the Computer Misuse Act 1990 which may carry a custodial sentence.[25]

Where does this leave us?

The proposed guidance is reassuring for those organisations which find themselves investigated despite their best efforts to comply. In settling the extraordinary fines announced in 2019 at a more explainable level, the ICO has confirmed its standing as a reasonable and pragmatic regulator. The good news is, organisations that have invested in GDPR compliance and show they have done everything they reasonably could in the circumstances will likely receive support instead of punishment.

AUTHORS

Marta Dunphy-Moriel is Commercial Technology Partner and Alexander Dittel Commercial Technology Senior Associate at Kemp Little LLP.
Emails:
Marta.Dunphy-Moriel@kemplittle.com
Alex.Dittel@kemplittle.com

 © 2020 PRIVACY LAWS & BUSINESS

REFERENCES

1 Intention to fine British Airways £183.39m under GDPR for data breach, 8 July 2019 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/
2 Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach, 9 July 2019 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/
3 ICO fines British Airways £20m for data breach affecting more than 400,000 customers, 16 October 2020 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/
4 ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/
5 Doorstep Dispensaree Ltd, 20 December 2019 ico.org.uk/action-weve-taken/enforcement/doorstep-dispensaree-ltd-mpn/
6 Bounty UK fined £400,000 for sharing personal data unlawfully, 12 April 2019 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/04/bounty-uk-fined-400-000-for-sharing-personal-data-unlawfully/
7 Consultation on the draft direct marketing code of practice, 4 March 2020 ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-direct-marketing-code-of-practice/
8 Investigation into data protection compliance in the direct marketing data broking sector, October 2020 ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf.
9 London company fined after 14.8m spam texts sent, 13 December 2018 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/12/london-company-fined-after-148m-spam-texts-sent/
10 The Privacy and Electronic Communications (EC Directive) Regulations 2003 www.legislation.gov.uk/uksi/2003/2426/contents/made
11 CRDNN Limited, 2 March 2020 ico.org.uk/action-weve-taken/enforcement/crdnn-limited-mpn/
12 Marketing: dal Garante privacy sanzione di 27 milioni e 800 mila euro a Tim, 1 February 2020 www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9256409
13 Ordinanza ingiunzione nei confronti di Wind Tre S.p.A., 9 July 2020 www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9435753
14 Il Garante privacy sanziona Eni Gas e Luce per 11,5 milioni. Telemarketing indesiderato e attivazione di contratti non richiesti, 17 January 2020 www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9244351
15 Berliner Datenschutzbeauftragte verhängt Bußgeld gegen Immobiliengesellschaft www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2019/20191105-PM-Bussgeld_DW.pdf
16 Bußgeld wegen Datenschutzverstößen bei H&M datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren
17 Inspectieverslag over verantwoordelijkheid bij gegevenslekken en positie functionaris gegevensbescherming www.huntonprivacyblog.com/wp-content/uploads/sites/28/2020/05/Besli ssing_GK_18-2020_NL_-1.pdf
18 The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC bit.ly/3ldQury
19 Penalty notice, British Airways plc, 16 October 2020 ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf
20 17 December 2019
21 ICO takes enforcement action against Experian after data broking investigation, 27 October 2020 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/
22 ICO takes enforcement action against Experian after data broking investigation, 27 October 2020 ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/
23 Former recruitment consultant prosecuted for stealing personal data from his old employer ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/former-recruitment-consultant-prosecuted-for-stealing-personal-data-from-his-old-employer/
24 The case of Nicola Young ico.org.uk/action-weve-taken/enforcement/nicola-young/ related to obligations under the Freedom of Information Act. However, the Data Protection Act 2018 establishes the same offence in relation to data subject requests.
25 Six month prison sentence for motor industry employee in first ICO Computer Misuse Act prosecution ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/six-month-prison-sentence-for-motor-industry-employee-in-first-ico-computer-misuse-act-prosecution/