ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Government unveils its plans for the Data Reform Bill

The DCMS says that the law reform does not significantly differ from the GDPR. As data controllers and the ICO face changes, the question about UK adequacy remains. By **Laura Linkomies**.

On 17 June, the government published its long-awaited plans to reform the UK Data Protection Act[1].

The UK proposals, discussed in this article, modify the current accountability framework in terms of suggesting a Privacy Management Programme which would change the requirements on DPOs, Record of Processing Activities (ROPA) and Data Protection Impact Assessments

Continued on p.3

The ICO's take on '*effective, proportionate and dissuasive*' GDPR enforcement action

The ICO's draft policy on fines looks to improve transparency and consistency. By **Emily Morgan** and **Alexander Dittel** of Wedlake Bell LLP.

Even after four years of the General Data Protection Regulation (GDPR) being in force, enforcement action by supervisory authorities in Europe and the Information Commissioner's Office (ICO) in the UK is often received with a sense of surprise. Headlines

Continued on p.5

Co-operate with PL&B on Sponsored Events

PL&B **would like to hear about your ideas for conferences, roundtables, webinars and podcasts (topics, speakers).**

Multiple opportunities for sponsorship deals to build brand awareness with a globally recognised and trusted partner.

Email info@privacylaws.com

Issue 122 **JULY 2022**

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

UNITED KINGDOM
report

ISSUE NO 122 **JULY 2022**

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
Emily Morgan and Alexander Dittel
Wedlake Bell LLP

Sharon Lamb and Michaela Novakova
McDermott Will & Emery

Asher Dresner
lincolnjay.com

Duncan Blaikie, Cindy Knott and Natasha Pappas
Slaughter and May

Sahra Wouters Okeili
Law student, Vrije Universiteit Brussel

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

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2022 Privacy Laws & Business

comment

Data Bill now here for scrutiny

Just as we were going to print, the government announced that it was introducing the Data Protection and Digital Information Bill in Parliament (p.20). While debate in Parliament has to wait until September, we can now study the different aspects of this Bill. The government's thinking has already changed quite a bit from its original position (p.1 and p.15). It remains to be seen how the appointment of a new Data Minister, Matt Warman MP, and indeed a new Prime Minister, will affect the progresss of this Bill.

The DCMS has suggested that, by removing some of the compliance requirements around accountability, the government claims that business and the public sector will benefit from up to £1 billion in costs savings. For organisations, the Bill means more change – on the face of it relatively few will greatly benefit from the proposed reliefs. As very few large organisations process only UK data, companies will still have to ensure that they also comply with the EU GDPR. Smaller firms could benefit – but many are not complying currently and have not made investments into data protection. So change may be minimal for this sector.

The new AI policy paper (p.20), to be followed later on by a White Paper, seeks to give different regulators the opportunity to take a tailored approach to the use of AI.

At *Winds of Change*, PL&B's 35th Annual Conference, 4-6 July, the ICO's Executive Director of Regulatory Futures and Innovation, Stephen Bonner, spoke about how the ICO is responding to technological challenges in AI, biometrics, advertising and other issues (p.9). The ICO is mindful that we need to achieve a 'thoughtful regulatory response' now, as these issues will shape our lives in the decades to come.

The ICO is making some welcome changes to the way it operates – for example, its fining policy (p.1). It is still not easy to get to grips with, but organisations will appreciate more transparency in this field. More innovations are included in the ICO25 three-year strategy (p.20). For the first time, the ICO will also be able to retain some of the monies coming in from monetary penalties (p.11) which will strengthen its enforcement work

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.

ICO fines... from p.1

about seemingly trivial1 or excessive2 fines are often contrasted with reports about apparent regulatory inaction.[3]

However, regulators are not the only show in town. Over the last ten years, privacy advocates have emerged as a driving force seeking to defend people's data protection rights. At the same time, a new generation of data privacy professionals who advise organisations on a daily basis look at regulatory practice for guidance. Understandably, inconsistent regulatory action could lead to conservative and defensive advice, excessive spending on superfluous compliance exercises, misinformation of the public through an opportunist media, and, of course, legal challenges of the regulator at public expense.

With this backdrop, it remains important to ensure consistency of enforcement action and particularly, fines. Issuing a fine is a matter of regulatory discretion and the GDPR does not set a minimum fine. Authorities are free to adopt policy objectives, such as the ICO's aim to "create an environment that protects the public, while ensuring that organisations are able to operate and innovate efficiently in the digital age".[4] However, when issued, fines must be "effective, proportionate and dissuasive".[5]

The ICO's proposed Regulatory Action Policy and Statutory Guidelines[6] and the EDPB's fine calculation guidelines[7] will likely improve transparency and consistency, and help establish appropriate safeguards including due process. However, neither guidance offers certainty to the level of an "exact starting amount" or to "quantify the precise impact of each aggravating or mitigating circumstance". As noted by the EDPB, imposing a fine cannot be a "mere mathematical exercise".

Looking back …

Before the GDPR, the ICO reassured us that it will not take regulatory action in respect of:

- Non-compliance with the data protection principles if the data controller has taken reasonable steps in the circumstances to prevent a breach;
- Single non-criminal breaches by small businesses caused by ignorance of requirements;
- Non-criminal, non-compliance which is not particularly intrusive and has not caused significant detriment; or
- Breaches arising from commercial disputes which are minor in nature, for example those which can be resolved by other means such as a private civil action.

However, times have changed, and the new guidance does not offer any such reassurances. The arrival of the GDPR and the recent proliferation of AI require a different approach. Even a seemingly trivial shortcoming in relation to algorithmic transparency, or wrongful use of input data, could have severe consequences if an AI model is used to make decisions about individuals in future.

A new approach?

The ICO's restarted consultation about enforcement[8] takes account of the change in the ICO's leadership but also the anticipated data reform. If more freedom is to be given to organisations to conduct "responsible processing", perhaps there is a need for more regulatory oversight.

Although not expected to differ significantly from the current draft,[9] the ICO's Statutory Guidance and Regulatory Action Policy will align with the data reform which promises:[10]

- To promote competition, innovation and economic growth;
- Publication of a detailed report each year on the ICO's approach to enforcement and use of its powers.
- Commissioning of technical reports to guide enforcement action.
- Issuing fines within six months of the letter of intent or faster, while preserving the ICO's ability to take additional time where needed.
- Informing the offender of anticipated timelines for each phase of the investigation.

> The ICO promises that in calculating financial penalties it will be fair and consistent.

The ICO's nine steps

In calculating penalties, the ICO follows the five steps under its Regulatory Action Policy.[11] The draft Statutory Guidance clarifies nine steps and includes more detail in comparison to the 2020 draft. The ICO promises that in calculating financial penalties it will be fair, consistent and take all relevant evidence and representations into account.

Step 1 is an assessment of seriousness by considering the nature, gravity, extent and duration of the contravention and processing activity but also the offender's cooperation, previous conduct, mitigation, certifications and how the contravention came to light. A **low**, **medium**, **high**, or **very high** risk rating will be assigned. This assessment will translate into a percentage which is applied to the starting point in Step 4.

Recently, reduced seriousness led to a reduction of the fine by two thirds given that the number of paper documents allegedly stored in an unsafe manner was not 500,000 but 76,000.

In **Step 2**, the offender's degree of culpability is assessed by looking at practices and safeguards as well as any processor failures. This will help determine the exact starting point within the range calculated in Step 4 and any adjustments on account of aggravating and mitigating factors in Step 5.

These will be higher in case of intentional breaches authorised explicitly by top management or contrary to the data protection officer's advice. However, the ICO has not established intent even when an organisation created a fictional policy framework to wrongly treat marketing emails as service communications.[12]

Step 3 will determine the turnover or equivalent to assess the starting range for a penalty.

In **Step 4**, the ICO will apply a percentage of up to 0.5%, 1%, 1.5% and 2% (or up to 1%, 2%, 3% or 4% in respect of higher maximum contraventions) determined by the low, medium, high or very high seriousness

and culpability. However, this is where the ICO and EDPB approaches differ, as shown in the example below.

EDPB's calculation of fines

In contrast, the EDPB's calculation model anticipates three steps. Firstly, the statutory maximum is determined based on the standard or higher maximum under the GDPR. Then a percentage of up to 10%, 20% or 100% is applied to the statutory maximum based on low, medium or high level of seriousness. Thirdly, although not mandatory, another percentage of 0.2% - 2% or 10% – 50% depending on the turnover being below or over €50 million.

Step 5 considers aggravating and mitigating factors, such as illicit financial gain, intent, response time, novel or invasive technology, special category data, implications for critical national infrastructure and others.

It is difficult to provide any quantitative rules for this step. The EDPB says that "increases or decreases of a fine cannot be predetermined through tables or percentages." In both cases of the ICO's recent enforcement action taken against charities Mermaids[13] and HIV Scotland,[14] the processing of special category data was involved and shows that fines were relatively high despite the not-for-profit nature of the offenders.

Openness and cooperation, prompt remedial action, accepting responsibility and other factors will serve as mitigation.

Given the focus on infrastructure, invasive tech and privacy intrusion, it follows naturally that fines may be more severe for high-risk industries, such as utility companies and healthcare service providers.

In **steps 6 and 7** the fine will be reduced to lessen any undue financial hardship and to promote economic growth. Under the data reform, the ICO will have a duty to have regard to competition, innovation and economic growth.

Previously, British Airways challenged the use of its turnover as a "core metric" as being contrary to the promotion of economic growth. However, the ICO considered this view "entirely misguided". The approach of larger companies being issued with larger penalties is "inherently proportionate and cannot pose any risk to economic growth".[15]

Step 8 is a final review of the proposed fine's effectiveness, proportionality and dissuasiveness and application of the statutory standard or higher maximum cap.

In **Step 9** a 20% early payment discount will be applied if the controller does not appeal and pays the fine in full within 28 days.

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

A panel to advise the ICO

Depending on the response to a notice of intent, the ICO may agree to convene a panel in cases where a proposed fine in excess of £5 million is likely to

EXAMPLE – HIGH TURNOVER AND HIGHER MAXIMUM

ICO's approach to the starting point	EDPB's approach to the starting point
Assume £100 million turnover	Assume €100 million turnover
Assume medium seriousness and culpability, i.e. 1 - 2% is applied which comes to a range of £1 million- £2 million, settled at say £1.5 million	Assume higher statutory maximum applies, i.e. the higher of 4% of worldwide turnover or €20 million, which gives a legal maximum of €20 million.
+ / - aggravating and mitigating factors	Assume medium seriousness and culpability, i.e. 10% - 20% is applied to the applicable legal maximum which comes to a range of €2 million - €4 million, settled at say €3 million
+ / - financial hardship and to promote economic growth	Not mandatory. Adjust the amount corresponding to turnover of the undertaking, i.e. 10% for undertakings up to €100 million turnover, which is €300,000 as a starting point
Assume higher statutory maximum applies, i.e. the greater of 4% of worldwide turnover or £17.19 million, which means the penalty must not exceed £17.19 million	+ / - aggravating and mitigating factors
+ / - effectiveness, proportionality and dissuasiveness	Assume higher statutory maximum applies, i.e. the fine must not exceed €20 million
End result is a fine of **£1.5 million** subject to the ICO's further discretions as set out above	+ / - effectiveness, proportionality and dissuasiveness
N/A	End result is a fine of **€300,000** subject to the authority's further discretions as set out above

 © 2022 PRIVACY LAWS & BUSINESS

cause a very significant financial impact on the recipient's business model. This will be considered on a case-by-case basis.

The role of the panel will be to decide whether the proposed fine and enforcement action is effective, proportionate and dissuasive. Drawing on the evidence, consistency and industry reactions, the panel will prepare a report and recommendations to the ICO who will have the final say.

There is no information about how the panel will be appointed. Naturally, conflicts of interest must be avoided. However, it would not be implausible inviting to the table industry experts, consumer protection groups, privacy advocates and data protection professionals.

Conclusion

Organisations will welcome the additional transparency about calculating the starting point for a fine. While the EDPB's methodology seems to produce a lower starting point than that of the ICO, the UK's data reform promises to add greater emphasis on competition, innovation and economic growth which will likely keep the ICO enforcement endeavours in check. However, it is impossible to provide mathematical certainty for this complex process which is only limited to what is effective, proportionate and dissuasive.

The UK's data reform wishes to "improve" the accountability principle under the GDPR making it more flexible and risk-based. However, it could be argued that such an approach will work best with strengthened regulatory oversight and enforcement to maintain the current culture of compliance.

In addition, under a new arrangement with the Department for Digital, Culture, Media & Sport, the ICO will retain up to £7.5 million per year received in monetary penalties. This could have an effect on the ICO's enforcement culture. At the same time, pursuing weak cases against well-resourced offenders may not pay off and the ICO will not be able to please every victim of non-compliance.

While a step in the right direction, given the fact-specific nature of each case and the varying regulatory practice, the ICO and EDPB guidelines will likely not eliminate inconsistencies in enforcement action which are here to stay for the foreseeable future. As for the ICO, there are too many balls in the air to be able to predict the future of data protection enforcement action in the UK.

AUTHORS

Emily Morgan is a Solicitor and Alexander Dittel is a Partner in Technology at Wedlake Bell LLP.
Emails: emorgan@wedlakebell.com
adittel@wedlakebell.com

EXAMPLE – LOW TURNOVER AND STANDARD MAXIMUM

ICO's approach to the starting point	EDPB's approach to the starting point
Assume £5 million turnover	Assume €5 million turnover
Assume low seriousness and culpability, i.e. 0 - 1% is applied which comes to a range of 0 - £50,000 as a starting point, settled at say £10,000	Assume standard statutory maximum applies, i.e. the greater of 2% of worldwide turnover or €10 million, which means the penalty must not exceed €10 million
+ / - aggravating and mitigating factors	Assume low seriousness and culpability, i.e. 0% - 10% is applied to the applicable legal maximum which comes to a range of €1,000,000, settled at say €500,000
+ / - financial hardship and to promote economic growth	Not mandatory. Adjust the amount corresponding to size of the undertaking, i.e. 0.4 % for undertakings up to €10 million turnover, which is €2,000 as a starting point
Assume standard statutory maximum applies, i.e. the greater of 2% of worldwide turnover or £8.59 million, which means the penalty must not exceed £8.59 million	+ / - aggravating and mitigating factors
+ / - effectiveness, proportionality and dissuasiveness	Assume standard statutory maximum applies, i.e. the fine must not exceed €10M
End result is a potential fine of **£10,000** subject to the ICO's further discretions as set out above	+ / - effectiveness, proportionality and dissuasiveness
N/A	End result is a potential fine of **€2,000** subject to the authority's further discretions as set out above

REFERENCES

1 €2,000 fine in relation to subject access request (Spanish DPA, March 2020) www.aepd.es/es/documento/ps-00237-2021.pdf
2 €100M issued to Google in relation to cookies following by another €150M a year after (CNIL, January 2022)www.cnil.fr/en/cookies-google-fined-150-million-euros ; CNIL, December 2020 www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland
3 The ICO has not issued a fine in relation to a credit referencing agency leveraging its statutory status to monetise the data of the nation (ICO, October 2020) ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/.
4 Draft Statutory guidance on our regulatory action, ICO, ico.org.uk/media/about-the-ico/consultations/4019213/statutory-guidance-on-our-regulatory-action-2021-for-consultation.pdf
5 Article 83(1) of GDPR.
6 As above.
7 Guidelines 04/2022 on the calculation of administrative fines under the GDPR Version 1.0 Adopted on 12 May 2022 edpb.europa.eu/system/files/2022-05/edpb_guidelines_042022_calculationofadministrativefines_en.pdf
8 ICO consultation on the draft Regulatory Action Policy; statutory guidance on our regulatory action; and statutory guidance on our PECR powers ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-rap-statutory-guidance-on-our-regulatory-action-and-statutory-guidance-on-our-pecr-powers
9 ICO publishes regulatory action policy and guidance, Mick Gorrill, Wedlake Bell LLP wedlakebell.com/ico-publishes-regulatory-action-policy-and-guidance/
10 Data: a new direction - government response to consultation, 23 June 2022 www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultationk
11 Regulatory Action Policy, ICO ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
12 Amex fined for sending four million unlawful emails ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/05/amex-fined-for-sending-four-million-unlawful-emails/
13 Mermaids ico.org.uk/action-weve-taken/enforcement/mermaids/
14 HIV Scotland ico.org.uk/action-weve-taken/enforcement/hiv-scotland-mpn/
15 Penalty notice, British Airways plc, 16 October 2020 ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf

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 Versions
We will email you the PDF edition which you can also access in online format 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

"I've always found *PL&B* to be a great resource for updates on privacy law issues, particularly those with a pan-EU focus. It strikes the right balance for those in-house and in private practice. The content is clear, well presented and topical."

Matthew Holman, Principal, EMW Law LLP

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 36th 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.