fieldfisher

This is Going to Hurt: Secret Diaries of the ICO (or, a Song of Enforcement and Fining)

Once upon a time, in a land far away, data protection regulatory risk was not a priority concern for businesses. The intricacies of data protection law remained the realm of only the keenest privacy advocates. The UK Information Commissioner's Office ("**ICO**"), the UK data protection regulator, was handcuffed, able only to impose maximum fines of £500,000 for breaches of data protection law (and indeed, rarely imposed fines even approaching this amount). The data protection regulatory world slumbered as, around it, the scope and complexity of real-world technology shifted. And then, the wind changed.

Today, under the General Data Protection Regulation ("**GDPR**"), the enforcement landscape in the UK looks very different to the earlier lands of yore. We have all heard the cries of the new era ("Fining powers of up to 4% of global annual worldwide turnover, or EUR 20 million, whichever is the higher!"). Businesses like British Airways and Marriott International have been the first to feel the might of the ICO's new armoury, poised to suffer potential fines of approximately £183 million and £99 million respectively (for more on this, see our earlier post here).

But what other powers does the ICO have under the Data Protection Act 2018 ("**DPA 18**"), the UK's updated data protection law? Where is the ICO guidance page on its enforcement powers under this new regime? What is happening elsewhere in the world? And, finally – the most dreaded of all – what impact would Brexit have for us?

ICO enforcement powers under the DPA 18

Firstly, please be aware that the following powers do not just relate to breaches of GDPR. They also relate to breaches of the DPA 18. This means that, as relevant, they can relate to breaches of:

- "General Processing" (Part 2 of the DPA 18: processing under the GDPR)
- "Law Enforcement Processing" (Part 3 of the DPA 18: processing by competent authorities – or their processors - for law enforcement purposes);
- "Intelligence Services Processing" (Part 4 of the DPA 18: processing by the intelligence services).

(*For most businesses, however, Part 2 of the DPA 18 is the salient part.*)

The ICO doesn't currently have a guide to its enforcement powers under the DPA 18 on its website, however it does make available its Regulatory Action Policy, which can be found here.

For those of you searching for a pithier tome, read on. The ICO's powers to enforce for breaches of all these Parts of the DPA 18 are set out in Part 6 of the DPA 18, as follows:

Section	Enforcement Power	What you should know
Investigative Powers		
142	**Information Notices.** the ICO may require a controller or a processor to provide the ICO with information that the ICO reasonably requires to carry out its functions, or where the ICO reasonably requires this information to: Investigate a suspected failure under s149(2) (i.e. failure to comply with specified obligations under the GDPR), or a suspected offence under the DPA 18; or Determine whether the relevant processing is carried out for the purposes of a purely personal or household activity ("household exemption").	All information notices must contain information about the consequences of failing to comply with the notice and the right to appeal the notice. An Information Notice can be directly served on a controller's or processor's representative and it will operate as though it has been served on that controller or processor. Certain restrictions apply to the ICO's ability to issue Information Notices (i) in relation to personal data processed for special purposes (journalism, academic purposes, artistic purposes and literary purposes); (ii) where such notice would involve an infringement of the privileges of either House of Parliament, (iii) in relation to information that is protected by legal advice or litigation privilege; or (iv) where the information would reveal evidence of an offence. The GDPR does not apply to processing that is carried out under the household exemption.
145	**Information Orders.** The ICO can obtain an order from the court to compel the disclosure of information by a person to the ICO if that person has failed to comply with an Information Notice.	
146	**Assessment Notices.** The ICO can require a controller or a processor to permit the ICO to carry out an assessment of whether that entity has complied with (or is complying with) data protection legislation. An Assessment Notice may require the entity to: enable the ICO to enter specified premises, direct the ICO to specific documents, assist the ICO with viewing such information, explain such information, or make available to the ICO certain individuals for interview (amongst other rights).	The Assessment Notice must specify the time periods for compliance. All Assessment Notices must contain information about the consequences of failing to comply with the notice and the right to appeal the notice. Certain restrictions apply to the ICO's ability to issue Assessment Notices (i) in relation to personal data processed for special purposes (journalism, academic purposes, artistic purposes and literary purposes); (ii) where such notice would involve an infringement of the privileges of either House of Parliament, (iii) in relation to information that is protected by legal advice or litigation privilege; or (iv) in relation to certain bodies under the Freedom of Information Act 2000 or the Office for Standards in Education, Children's Services and Skills.
Corrective Powers		
149	**Enforcement Notices.** Where the ICO is satisfied that a person has failed to comply with specific sections of the GDPR, it may give that person written notice to: (i) take the steps stated in the Enforcement Notice; or (ii) refrain from taking the steps stated in the Enforcement Notice. These steps could include a ban on all processing of personal data, or a ban on specified categories of personal data (by reference to the description of the data, the purpose or manner of the processing, or the time when the processing took place).	This power does not explicitly refer to undertakings, however the end result is essentially the same. An Enforcement Notice can only impose requirements that the ICO considers appropriate for the purpose of remedying the identified failure. When deciding whether to give an Enforcement Notice under s149(2), the ICO must consider whether the failure has caused or is likely to cause any person damage or distress. The Enforcement Notice must specify the time periods for compliance. All Enforcement Notices must contain information about the consequences of failing to comply with the notice and the right to appeal the notice.

Section	Enforcement Power	What you should know
	If the Enforcement Notice relates to the rectification or erasure of personal data, the ICO can also require the relevant person to take further steps (for example, to notify third parties of the erasure or rectification; or to supplement such data with a statement of the true facts relating to the matters, which is approved by the ICO).	Certain restrictions apply to the ICO's ability to issue Enforcement Notices (i) in relation to personal data processed for special purposes (journalism, academic purposes, artistic purposes and literary purposes); (ii) where such notice would involve an infringement of the privileges of either House of Parliament; or (iii) in relation to joint controllers under Part 3 or 4 of the DPA 18.
154	**Powers of entry and inspection.** The ICO has various powers of entry and inspection as set out in Schedule 15 of the DPA 18.	The ICO is required to obtain a warrant for such entry/ inspection in advance.
155	**Penalty Notices.** The ICO can issue a written notice requiring a person to pay a specified amount in sterling if that person has failed to comply with an Information Notice, an Assessment Notice or an Enforcement Notice; or if that person has failed (or is failing) as described in s149(2), (3), (4) or (5). When issuing the penalty amount, the ICO must refer to the GDPR and the matters listed in s155(3). These matters include: (i) the nature, gravity and duration of the failure; (ii) the intentional or negligent character of the failure; (iii) any mitigatory action taken to reduce the amount of distress or damage suffered by data subjects; (iv) the degree of responsibility of the relevant entity; (v) previous failures; and (vi) the degree of cooperation with the ICO, amongst others.	The Secretary of State can also broaden the ICO's powers to impose a penalty notice for other failures of data protection legislation. Certain restrictions apply to the ICO's ability to issue Penalty Notices: (i) in relation to personal data processed for special purposes (journalism, academic purposes, artistic purposes and literary purposes); (ii) where such notice would involve an infringement of the privileges of either House of Parliament; (iii) related to processing by the Crown Estate Commissioners, or a person who is a controller under section 2009(4) (controller for the Royal Household); or (iv) in relation to joint controllers under Part 3 or 4 of the DPA 18. Under Schedule 16 of the DPA 18, the ICO must issue a "Notice of Intent" before imposing a Penalty Notice.
S158	**Fixed penalties for non-compliance with charges regulations.** The ICO must produce and publish a document specifying the penalty for failure to comply with the registration charges regulations.	The maximum amount that may be specified as a penalty is 150% of the highest charge payable by a controller in respect of the financial year in accordance with the charging regulations. Currently, this is: • £400 for Tier 1 organisations • £600 for Tier 2 organisations; and • £4000 for Tier 3 organisations. The ICO also reserves the right to increase this amount to the statutory maximum of £4,350 in certain cases.

It's all about penalties—but what are the relevant amounts?

As a starting point, the ICO is required to adhere to the fining thresholds set out in the GDPR. However, the DPA 18 adds further specificity, as follows:

1. If there is an infringement of the **GDPR**, the maximum amount that can be imposed under a Penalty Notice is:
   a. The amount specified in Article 83 of the GDPR; or
   b. If an amount is not specified, the "standard maximum amount".
2. In relation to an infringement of **Part 3** of the DPA 18, the maximum amount that can be imposed under a Penalty Notice is:
   a. The "higher maximum amount" for breaches of sections 35-37, 38(1), 39(1), 40, 44-49, 52-53, 73 -78; or
   b. Otherwise, the standard maximum amount.
3. In relation to infringements of **Part 4** of the DPA 18, the maximum amount that can be imposed under a Penalty Notice is:
   a. The higher maximum amount for breaches of sections 86-91, 93 – 94, 100 or 109; or
   b. Otherwise, the standard maximum amount.

The "**higher maximum amount**" is:

a. For an undertaking, 20 million Euros or 4% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is the higher; or

b. In any other case, 20 million Euros.

The "**standard maximum amount**" is:

a. For an undertaking, 10 million Euros or 2% of the undertaking's total annual worldwide turnover in the preceding financial year, whichever is the higher; or

b. In any other case, 10 million Euros.

The amount must be calculated in sterling using the spot rate of exchange set by the Bank of England on the day on which the Penalty Notice is given.

What else does the ICO need to bear in mind before taking Enforcement action?

While the UK remains part of the European Union, it is required to bear in mind the cooperation and consistency mechanisms under the GDPR. This means that the ICO (along with other EU supervisory authorities) should bear in mind EU-level guidance when it taking enforcement action in their own jurisdictions, particularly in relation to the setting of administrative fines.

The Article 29 Working Party ("**WP 29**") Guidance 17/EN WP 253 ("**Guidance**") in particular sets out guidelines on the application and setting of fines under GDPR. The WP 29 highlights that consistent enforcement of the GDPR is central to a harmonised data protection regime; and that administrative fines are the central element of the new enforcement regime introduced by the GDPR. The Guidance is therefore intended to be used by supervisory authorities to ensure better application and enforcement of the GDPR across the EU.

Importantly, the WP 29 highlights that infringement of the GDPR in any member state should lead to the imposition of "equivalent sanctions". Like all corrective measures, WP 29 states that any administrative fine should adequately respond to the nature, gravity and consequences of the breach and that a supervisory authority must assess all the facts of a case in a manner that is consistent and objectively justified. Any corrective measure must be "effective, proportionate and dissuasive". When it comes to imposing a fine which relates to cross-border processing, the European Data Protection Board ("**EDPB**") will have the final say in relation to disputes by supervisory authorities as to the level of the relevant fine.

So, what Enforcement action has been taken in the rest of Europe?

We are still in the early days of enforcement action under the GDPR. The first major GDPR infringement case came from the CNIL (the French supervisory authority) against Google, where the CNIL imposed a EUR 50 million fine on Google for breaches of its transparency and consent obligations under GDPR (see: here)

However, in recent weeks, the German supervisory authorities, acting under the auspices of the DSK (a joint coordination body) has reportedly set out a new model for calculating fines under the GDPR. According to the International Association of Privacy Professionals, the DSK's calculation starts with the aggregate global annual revenue of the relevant undertaking (which, for corporate groups, includes the revenue of the entire group). The DSK then uses this number to calculate a "daily rate" (by dividing the global annual revenue by 360), which can be multiplied by a number of factors (decided by reference to Article 83(2) of the GDPR) to calculate the total fine amount.

The DSK's model sets out five levels of multiplier factors that would be applied to the "daily rate":

- Minor infringement: multiplier of 1 to 4
- Average infringement: multiplier of 4 to 8
- Severe infringement: multiplier of 8 to 12
- Very severe infringement: multiplier of 12 to 14.4.

This amount would then reportedly be further modified to take into account the nature of the offence and its consequences in accordance with additional criteria, such as the duration of the infringement, the nature, extent and purpose of the unlawful processing, the number of data subjects involved and the extent of the harm suffered. The supervisory authority could then further fine-tune the fine by reference to any other relevant criteria under Article 83(2) of the GDPR, or to reflect any further aggravating or mitigating circumstances.

Initial outputs of the DSK model have allegedly resulted in significantly higher fines that those imposed to date by the German data protection authorities under GDPR. In addition, the DSK has reportedly presented its model to the "Task Force for Fining" of the EDPB. If approved, there is a chance that the model could be adopted as the baseline for calculating regulatory fines across the EU – with the result that businesses should expect to see higher regulatory fines for GDPR breaches, including in the UK.

What about Brexit?

If the UK leaves the EU without a deal, we will no longer be required (as a matter of law) to take into account the subsequent rules or decisions of the rest of the EU when it comes to enforcement actions for data protection law breaches. As a practical matter, however, to demonstrate our "adequacy" (i.e. that we can be trusted with the processing of personal data to the

same standard as the rest of the EU), we may still ultimately refer to EU-wide enforcement decisions and guidance when it comes to deciding our local enforcement.

However, one big change will be that businesses operating in both the UK and the EU will not be able to benefit from a "one-stop shop". Instead, a business that infringes both UK data protection law and the GDPR could find themselves hit with double the fines: one from an EU regulator (a one-stop shop would still apply within the EU, for example if a business had multiple operations across the EU), one from the ICO. This would reflect that the same breach had occurred: (i) under EU law; and (ii) under English law. Not a happy result.

Conclusion

Enforcement action under the GDPR is heating up in the UK and in the rest of the EU. Businesses should expect to see increasing penalties issued by supervisory authorities under the GDPR, including by the ICO.

In addition (although not covered in this article), this is a trend that seems to be increasing across the globe. Authorities outside Europe are also starting to take breaches of data protection law more seriously. In the US, the Financial Trade Commission has reportedly agreed to fine Facebook $5bn to resolve Facebook's privacy issues in relation to the Cambridge Analytica scandal of 2018. In addition, the Attorney General for California ("**AG**") has recently released its anticipated proposed regulations governing compliance with the California Consumer Privacy Act ("**CCPA**"), which are open for consultation until 6 December. **On the current timetable, the AG will be able to bring enforcement action against businesses that breach the CCPA from 1 July 2020.**

As such, this is no time to be slaying dragons. Given the current climate, businesses should focus instead on resolving their compliance gaps to prevent a supervisory authority using GDPR enforcement as an opportunity to take a nasty bite.

Contacts

Amy Lambert
Associate
amy.lambert@fieldfisher.com
+44 (0) 207 861 4294

Amy is an associate in Fieldfisher's London Technology, Outsourcing and Privacy team. See here for further information.