The evolution of a data protection regulator

The new age of data protection: what Boards need to know about the ICO

Building a better working world

"Change is coming. It is inevitable. Progress, however, is optional.

So, I'm looking around the room and wondering where you're at. This time last year – whether you were in this room, following the conference on Twitter or just getting on with your day job – do you feel you've moved on? Has your mindset shifted? We at the ICO have certainly changed. And we're progressing."

Elizabeth Denham,
Information Commission[1]

[1] Elizabeth Denham's keynote speech, screened at the Direct Marketing Association's Data Protection 2018 event on Friday, 23 February 2018 in London

Introduction

Data protection is making the headlines – it is in the press and has been debated in Parliament. The Information Commissioner's Office (ICO) is centre stage in the fight to protect individuals' personal data: and that fight has evolved into high profile investigations and the type of regulatory response that is akin to bigger regulators such as the Financial Conduct Authority (FCA).

This EY Regulatory & Public Policy briefing looks at the evolution of the ICO, the changing dynamics in the way in which it operates, including its new powers and expectations regarding firms' data protection governance and culture and some of the key messages Boards need to know about the ICO. We have also included some questions that Boards could usefully ask themselves about their organisations' relationship with the ICO, and data protection in general, as we move into the new age of data protection regulation.

Recent events involving the ICO enforcing data protection legislation have demonstrated how far the ICO has come as a regulator but also the limits that still remained on its ability to act (or act in a timely manner). Unlike the FCA, which can make a swift and unannounced visit to a firm if serious regulatory breaches are suspected, the ICO had to make an application to court for a warrant to search premises, which could be slow and public.

However, change is coming. The EU General Date Protection Regulation (GDPR), came into effect on 25 May 2018. The GDPR is described, by the Information Commissioner, as "a game changing piece of legislation [which] will reshape the data protection landscape." Under GDPR, responsibility sits squarely with the Board of directors of both data controllers and data processors – in other words, all UK organisations – to monitor compliance and manage breaches. Going forward the ICO will be focussing not just on organisations' systems and controls but on what steps the Board is taking. This briefing aims to highlight some of the key changes for Boards and provide some pertinent questions to ask your organisations.

GDPR also brings changes for the structure, capacity and resourcing of the ICO, which has become the UK supervisory authority for data protection. The new UK Data Protection Act 2018 (DPA 2018), creates a new statutory footing for the ICO and equips the ICO with additional powers over and above those in the GDPR. For more information on the changes to data protection legislation see Appendix I.

As discussed in their blog 'New regulatory powers for the digital age' the ICO has "worked with government to strengthen our powers so we can issue information notices to individuals as well as organisations, we can issue urgent notices to be complied with within 24 hours. We have the ability to inspect and assess compliance without notice and it will be a criminal offence for an organisation to destroy or alter information we wish to pursue a warrant to remove".[2] The ICO has also published a draft Regulatory Action Plan for consultation, on 4 May, that sets out how it intends to use its new powers.[3] For further information on the evolution of the ICO see Appendix II.

So with an enhanced international role (which will become more complex after Brexit) and a 'new regulatory landscape [that] calls for a more pivotal and complex ICO', the ICO is set to become a larger and better resourced regulator with a more proactive approach to regulation and a more extensive enforcement toolkit. As the Information Commissioner said, the "25 May will merely mark the end of the beginning of a very long journey for the data protection community" and the moves to reshape the ICO "so that we are the relevant, future-focussed regulator that you need us to be" are clear for all to see.[4] Now really is the time for Boards to ensure they understand their responsibilities under the GDPR, how the ICO is changing, including its expectations, powers, and how to engage proactively.

Under GDPR, responsibility will sit squarely with the Board of directors of both data controllers and data processors to monitor compliance and manage breaches. Going forward the ICO will be focussing not just on organisations' systems and controls but on what steps the Board is taking.

So with an enhanced international role (which will become more complex after Brexit) and a "new regulatory landscape [that] calls for a more pivotal and complex ICO", the ICO is set to become a larger and better resourced regulator with a more proactive approach to regulation and a more extensive enforcement toolkit.

[2] https://iconewsblog.org.uk/2018/05/04/new-regulatory-powers-for-the-digital-age/

[3] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-consults-on-how-it-will-use-increased-powers-under-upcoming-data-protection-reform/

[4] Elizabeth Denham's keynote speech at the IAPP Europe Data Protection Intensive 2018, London, 18 April 2018 – https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/04/iapp-europe-data-protection-intensive-2018/

Questions to ask?

In addition to ensuring their companies are monitoring the data protection and e:privacy legislative and regulatory developments during 2018 – and responding to opportunities to provide input to policy makers and regulators – here are a few of the data privacy and ICO-related questions which Boards could be asking themselves:

- Does the Board understand their obligations under the new legislation and the need to invest in safeguards to build and retain customer trust in data privacy?
- Compliance with GDPR is now a Board level responsibility: is data privacy on the main Board agenda and how will we demonstrate to the ICO the steps taken to comply?
- Are we able to evidence: our reporting structures; risks assessments and mitigation measures; and who is responsible for what within the business? Are these records up-to-date, accurate and comprehensive?

  How quickly will we be able to make this information available for the ICO if an incident occurs? Do we have a clear notification process?
- How do we move to and develop a more proactive engagement strategy with a regulator we may not have been prioritising on the same level as regulators such as the FCA?
- Do we understand the ICO's focus and priorities? If we don't, how do we engage with the ICO and how do we enhance our understanding?
- The GDPR requires prior consultation with the supervisory authority (e.g., article 36), are we clear about when consultation with the ICO is needed? What does 'consultation' mean in practice and what information will the ICO require?
- If we operate in a sector with high processing or use of personally identifiable information (PII) what assurance can be provided to stakeholders and the ICO that our risks are appropriately managed and/or mitigated (e.g., have we requested an ICO advisory visit or consensual audit)?
- If we are developing 'novel, technological approaches that present a high degree of intrusion into people's privacy', how are we engaging with the ICO to socialise our approach to data protection as part of our process development?
- Are we appropriately engaged with industry data protection, privacy and cyber security working groups? How do we ensure we stay current on best practice and emerging risks?
- Have we assessed the implications of the GDPR for any group companies outside the EU that may be offering goods or services to EU citizens or monitoring their behaviours? In addition to ensuring compliance, how do we link them into our UK ICO engagement strategy?

A changing data protection culture

By now Boards should have received very clear messages that the ICO means business, the GDPR is about changing the culture towards personal data and there is an inextricable link between data protection and cyber security. As the Information Commissioner explained: "I'd encourage you to use these new regulations as an opportunity to focus on data protection and data security. Ensure your board of directors understand the new obligations under the laws, the need to invest in safeguards to build and retain customer trust."[5] The DPA 2018 consolidates and modernises UK data protection legislation, facilitating the move to a joined up regulatory approach to data protection and security. However, whilst the ICO is operating akin to regulators such as the FCA, arguably more may need to be done to link it fully into the UK regulatory framework.

How the ICO will work with the FCA, the Financial Reporting Council (FRC) and other regulators and agencies is an important operational issue to resolve. Will the ICO have sufficient resources to monitor organisations proactively or can it rely on the work of other regulators or an assurance framework that is extended to data privacy (if so, what would it look like)? Other legislation may well be needed to establish firmly the evolved ICO and provide for appropriate levels of mutual cooperation.

That said, there are visible signs that the ICO and FCA are working in closer collaboration. In February 2018, they published a joint update on GDPR: "Compliance with GDPR is now a board level responsibility, and firms must be able to produce evidence to demonstrate the steps that they have taken to comply. The requirement to treat customers fairly is also central to both data protection law and the current financial services regulatory framework."

Furthermore, the FCA has been clear that "Whilst the ICO will regulate the GDPR, complying with the GDPR requirements is also something the FCA will consider under their rules, for example, the requirements in the Senior Management Arrangements, Systems and Controls (SYSC) module. As part of their obligations under SYSC, firms should establish, maintain and improve appropriate technology and cyber resilience systems and controls."

The FCA and ICO will also be reviewing their 2014 MoU[6] to ensure it is 'still fit to address future collaboration'. So financial services firms, in particular, should be mindful that breaches of GDPR requirements could also amount to a breach of the FCA rules, exposing them, in serious cases, to multiple enforcement action as well as loss of reputation and customer trust.

As regards cyber security, the ICO is committed to working with the National Cyber Security Centre (NCSC) and the Government 'to provide more certainty, assurance, and guidance to businesses for cyber security legislation.' The NCSC, whose parent body is GCHQ (the Government Communications Headquarters), was established in 2016 to manage national cyber security incidents, carry out real-time threat analysis and provide tailored sectoral advice. Organisations of all sizes should ensure they are monitoring NCSC guidance and, in particular, threat reports.

Under the GDPR "Businesses will need to be able to show reporting structures, risks assessments and mitigation measures, who is responsible for what within the business and these records need to be up-to-date and accurate and comprehensive. They need to be available for the ICO if an incident occurs." The ICO now has the power, under the DPA 2018, to compel disclosure of information when investigating breaches.

> "I'd encourage you to use these new regulations as an opportunity to focus on data protection and data security. Ensure your board of directors understand the new obligations under the laws, the need to invest in safeguards to build and retain customer trust."

[5] Elizabeth Denham talked about how cyber security and data protection are inextricably linked in her speech at the CBI Cyber Security Conference on 13 September 2017

[6] https://www.fca.org.uk/publication/mou/mou-fca-ico.pdf

Conclusion

Data protection will undoubtedly continue to hit the headlines. From multinationals to charities, some organisations may struggle to be fully 'GDPR compliant', particularly given the volumes of personal data already collected. As well as changing existing practices, there is also the continued risk of cyber-attack and whilst such attacks may be inevitable, the ICO will want answers when personal data is compromised. Organisations which are complacent about data protection and data security are unlikely to have a defense.

The ICO has stressed that "whilst fines may be the sledgehammer in our toolbox, we have access to lots of other tools that are well-suited to the task at hand and just as effective. Like the DPA, the GDPR gives us a suite of sanctions to help organisations comply – warnings, reprimands, corrective orders. Whilst these will not hit organisations in the pocket – their reputations will suffer a significant blow."[7]

We have already seen the ICO take high profile steps in the market to enforce data protection regulation but we have not yet seen the ICO operating for long UK supervisory authority under the GDPR. It is inevitable that the regulatory response to new legislation may evolve over time (as we have seen with the UK Bribery Act 2010) so the ICO will continue to evolve even though it has taken on its new responsibilities and powers. Market incidents are also defining the future of UK data protection regulation: including the ability of the ICO to respond with appropriately sharp teeth.

Organisations should expect the ICO to be proactive this year at defining higher risk organisations and practices, setting expected standards of behaviour and taking action to reduce the risk of future incidents.

The ICO is evolving and, as discussed in Appendix III, adapting to the impact of technological change on data privacy rights. The question is, has your company evolved its approach to data protection and its relationship with the ICO?

> "Compliance with GDPR is now a board level responsibility, and firms must be able to produce evidence to demonstrate the steps that they have taken to comply."

[7] https://iconewsblog.org.uk/2017/08/09/gdpr-sorting-the-fact-from-the-fiction/ ICO Blog: GDPR Sorting out the fact from the fiction

Appendix I: The new age of data protection – an overview

The GDPR brings EU data protection legislation into the new digital age. After over four years of detailed negotiations amongst the 28 EU Member States, the GDPR was finally adopted by the EU Parliament and European Council in 2016 and came into force on 25 May 2018. The GDPR updates and harmonises privacy across the EU, replacing the 1995 Data Protection Directive (DPD) and introducing a tougher enforcement regime. An Economist article in *The World in 2018* quotes Christopher Kuner, from the Free University of Brussels, as saying that GDPR "is still the most complex piece of regulation the EU has ever produced"[8].

As discussed in the R&PP Point of View, *'Regulatory consequences of living in a digital world'*[9], the regulatory landscape is changing as a response to the risks to personal data created by developments such as machine learning, the Internet-of-Things and robotics. Regulation is playing catch-up to technological evolution and whilst the GDPR modernises EU legislation, technology is not standing still and neither should legislation.

Amongst the changes, the GDPR introduces the protection of EU individuals' personal data wherever the processing is carried on. This is likely to result in greater use of enterprise risk management to address the risks. In contrast to the DPD, which applied to data processing within the EU, the GDPR applies when the personal data of EU citizens is processed in connection with goods or services that are offered to them or, in connection with the monitoring of behaviour of individuals within the EU.

Much has already been written about GDPR. In the blog 'GDPR – sorting the fact from the fiction', the Deputy Information Commissioner stressed that 'GDPR is an evolution in data protection, not a total revolution. It demands more of organisations in terms of accountability for their use of personal data and enhances the existing rights of individuals. GDPR is building on foundations already in place for the last 20 years.

If you are already complying with the terms of the Data Protection Act, and have an effective data governance programme in place, then you are already well on the way to being ready for GDPR.'

> "The new GDPR regime represents a step change, rather than a leap into the unknown."

So why the degree of concern? Perhaps because individuals may feel they have lost control of their personal data, particularly online, and in many cases the consent to collect their data has been ambiguous and non-specific. Faced with the huge volumes of data already collected, firms may now struggle to locate and consolidate data, especially unstructured data, for example, when individuals exercise their enhanced rights under GDPR, such as the right to be forgotten. In these circumstances, companies may also risk holding personal data for longer than needed, contrary to GDPR Principle (e): Storage limitations.

The fines under the GDPR of up to 4% of annual global turnover or €20 million (whichever is greater) for serious offences, whilst not the norm, will certainly focus minds.

[8] New EU data rules will get tough on privacy by Ludwig Siegele http://www.theworldin.com/edition/2018/article/14563/new-eu-data-rules-will-get-tough-privacy

[9] http://www.ey.com/Publication/vwLUAssets/ey-regulatory-consequences-of-living-in-a-digital-world/$FILE/EY-Regulatory-consequences-of-living-in-a-digital-world.pdf

There is still debate about the intended and unintended consequences of the GDPR within the EU (e.g., will it stifle innovation and could the fines, if used disproportionally, put companies out of business). However, the reality is that the GDPR is here and, ultimately, it is about rebuilding trust and doing the right thing.

As the ICO blog: "Whatever the size of your organisation, GDPR is essentially about trust. Building trusted relationships with the public will enable you to sustainably build your use of data and gain more value. Through changing their data handling culture, organisations can derive new value from customer relationships.

Failing to get data protection right is likely to damage your reputation, your customer relationships and, ultimately, your finances. That goes way beyond increased fines — think brand damage and a subsequent loss of custom."

GDPR will now be followed, as agreement could not be reached in time, by a Regulation on Privacy and Electronic Communications (the ePrivacy Regulation) which will apply to new forms of electronic communication — including instant messaging and machine-to-machine communication in the Internet-of-Things.

The ePrivacy Regulation will, amongst other things, focus on the need for valid consent. The original plan was for GDPR and the ePrivacy Regulation to come into force at the same time, but the complexity of the negotiations have resulted in a delay — possibly until later in 2018 or even 2019.

The Network and Information Systems (NIS) Directive, which was required to be transposed into UK law by 9 May 2018, seeks to raise the levels of security and resilience of network and information systems and includes reporting requirements in the event of breaches. In the UK the DPA 2018 modernises the UK statute book, consolidates four data protection regimes and, amongst other things, extends the scope of the GDPR to other areas of processing (e.g., the processing of unstructured manual data by public authorities).

The Information Commissioner described this changing landscape as 'a new frontier for privacy and information rights regulation' and speaks of her office 'working in the new age of data protection'.

Appendix II: The evolution of a regulator

The ICO is an independent public body with a mission to uphold information rights for the UK public in the digital age and its vision is to increase the confidence that the UK public have in organisations that process personal data and those which are responsible for making public information available. Its responsibilities are set out in the DPA 2018, the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

The ICO has five Strategic Goals:

1. To increase the public's trust and confidence in how data is used and made available.
2. Improve standards of information rights practice through clear, inspiring and targeted engagement and influence.
3. Maintain and develop influence within the global information rights regulatory community.
4. Stay relevant, provide excellent public service and keep abreast of evolving technology.
5. Enforce the laws we help shape and oversee.

The DPA 2018 became the statutory footing for the ICO after 25 May 2018: it is intended to, amongst other things, provide the ICO with the additional functions required under the GDPR and other new legislation and increase the maximum level of fines in the UK to be consistent with the GDPR. In particular, Part 5 and Schedule 12 of the DPA 2018 make provision to allow the Information Commissioner and her office to continue to operate under the UK's new data protection laws. It describes the Information Commissioner's functions, duties and powers which are discussed in the ICO's draft Regulatory Action Policy.

The ICO we see today, though, with some 400 staff and multiple offices is vastly different to how it was born. In July 1984, the ICO was set up, with a Commissioner and a small number of staff, to oversee the Data Protection Act 1984 DPA and set up a register of data users and company bureau with powers that were limited to issuing notices to enforce compliance[10]. Since April 2010, the maximum ICO fine for serious breaches of the DPA had been £500,000. As discussed previously, under the GDPR the ICO is able to fine both data controllers and data processors up to 4% of annual global turnover or €20 million for serious breaches.

However, it would be wrong to focus on the size of the fines under the GDPR. As the Information Commissioner said in her blog 'GDPR – sorting the fact from the fiction'

"This law is not about fines. It's about putting the consumer and citizen first. We can't lose sight of that. Focusing on big fines makes for great headlines, but thinking that GDPR is about crippling financial punishment misses the point. And that concerns me."

The ICO has committed to continuing to guide, advise and educate organisations about how to comply with the GDPR 'We have always preferred the carrot to the stick.'

> "... it's scaremongering to suggest that we'll be making early examples of organisations for minor infringements or that maximum fines will become the norm."

[10]History of the ICO https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/

However, the message is clear "for those that flout the law – those that play fast and loose with the personal data that's been entrusted to them."[11] In particular, the ICO will reserve its strongest sanctions "for breaches involving novel, technological approaches that present a high degree of intrusion into people's privacy".[12]

As the powers available to the ICO have evolved over the years, so too has its focus: from managing citizens' rights and a focus on the public sector to a wider focus on the protection of data by both private and public sector organisations. A pivotal moment came in 2015 when the law was changed to enable the ICO to take action against nuisance callers without having to prove substantial damage or substantial distress, which was proving difficult. Now the ICO's list of enforcement action contains public bodies, including county councils, police authorities and a central government department and also numerous private companies and individuals.

In particular, in January 2018 the ICO fined a company £400,000 after serious failures placed customer and employee data at risk. Was this (and other high-profile action) a warning and foretaste of things to come? Whilst the ICO is debunking the fear factor with regard to ratcheting up of fines under the GDPR, organisations which are not taking reasonable steps to protect and secure personal data should be clear that the ICO means business.

The ICO is now involved in reviews of incidents such as the May 2017 cyber-attacks on the NHS. In May 2017 the Information Commissioner also opened a formal investigation into the use of data analytics for political purposes[13], one strand of which came to public attention in March 2018.

> "A matter of great concern is that the Information Commissioner has to go through what sounds like a laborious process to get the warrant needed to conduct an investigation that is obviously in the public interest. When we secure, for example, emergency injunctions to stop the publication of material that people do not want published, or when magistrates issue search warrants, most of us with experience of this at a local level would observe that such warrants are often issued in a much faster and less high-profile way than the process the Information Commissioner appears to have to go through."
>
> **Liam Byrne,** MP[14]

It is clear, however, that the evolution of the ICO is not yet complete and that further legislative change will be needed. The ICO has been given extra powers to deal with complex investigations.

"For those that flout the law – those that play fast and loose with the personal data that's been entrusted to them." In particular, the ICO will reserve its strongest sanctions "for breaches involving novel, technological approaches that present a high degree of intrusion into people's privacy."

[11] Elizabeth Denham's speech at the Association of Chief Executives and Public Chairs' Forum joint event, on Friday, 2 February 2018
[12] Elizabeth Denham's keynote speech, screened at the Direct Marketing Association's Data Protection 2018 event on Friday, 23 February
[13] https://iconewsblog.org.uk/2017/05/17/information-commissioner-elizabeth-denham-opens-a-formal-investigation-into-the-use-of-data-analytics-for-political-purposes/
[14] See Hansard, 20 March 2018 https://hansard.parliament.uk/Commons/2018-03-20/debates/a63a34d7-d41c-44bf-ac8a-e497c3b79808/DataProtectionBill(Lords)(SixthSitting)?highlight=Information%20Commissioner#contribution-879AC413-94E2-4DC4-9792-7BD9FC1A1494

Appendix III: To 2021 and beyond

In April 2017 the ICO published its first Information Rights Strategic Plan 2017-2021. The plan sets out the Information Commissioners mission to increase public trust (including by creating a culture of accountability within organisations) and is designed to make sure the ICO maintains its position as the forefront of data protection and stays relevant.

One of the strategic priorities in the plan is to develop a new Technology Strategy that outlines the ICO's "means of adapting to technological change as it impacts information rights." The Technology Strategy 2018-2021 was published by the ICO on 1 March 2018. The strategy has eight technology goals and how the ICO intends to achieve them. These include engaging with other regulators, international networks and standards bodies on technology issues relevant to data protection, providing effective guidance to organisations about how to address data protection risks arising from technology (for example, a report on "lesson learnt" from reported cyber breaches). The ICO also has a goal to support and facilitate new research into data protection risks and data protection by design solutions, including through the use of an ICO Grants Programme and research and investigations into new and emerging technologies to inform future priority areas.

Work on technology will be carried on by the ICO's new Technology Policy Department. The ICO has also committed to establishing a regulatory sandbox, drawing on the Financial Conduct Authority (FCA) process. Organisations should note that technology priority areas for 2018-2019 are cyber security, AI, big data, machine learning and web and cross device tracking. Another clear message is that organisations, particularly those investing in innovative areas, should work with the ICO: "The ICO appreciates the challenges organisations are working under today because we face the same challenges.

Budgets are tight, technology is moving fast and there's the race to keep up with competitors. But data protection law needn't be onerous if you adopt privacy by design and sound cyber security at the outset of a project. Don't treat them as an afterthought. Don't bolt them on.

You will find the ICO to be a proactive, reasonable regulator aware of business and the real world."

The ICO's four-year Resource and Infrastructure Strategic Plan complements the Information Rights and Strategic Plan by setting out how the ICO will be resourced and the infrastructure it will have in place to 'establish the foundations essential to provide the UK with a strong and expert privacy and information rights regulator' over the period October 2017 to September 2021. Highlights from the plan include:

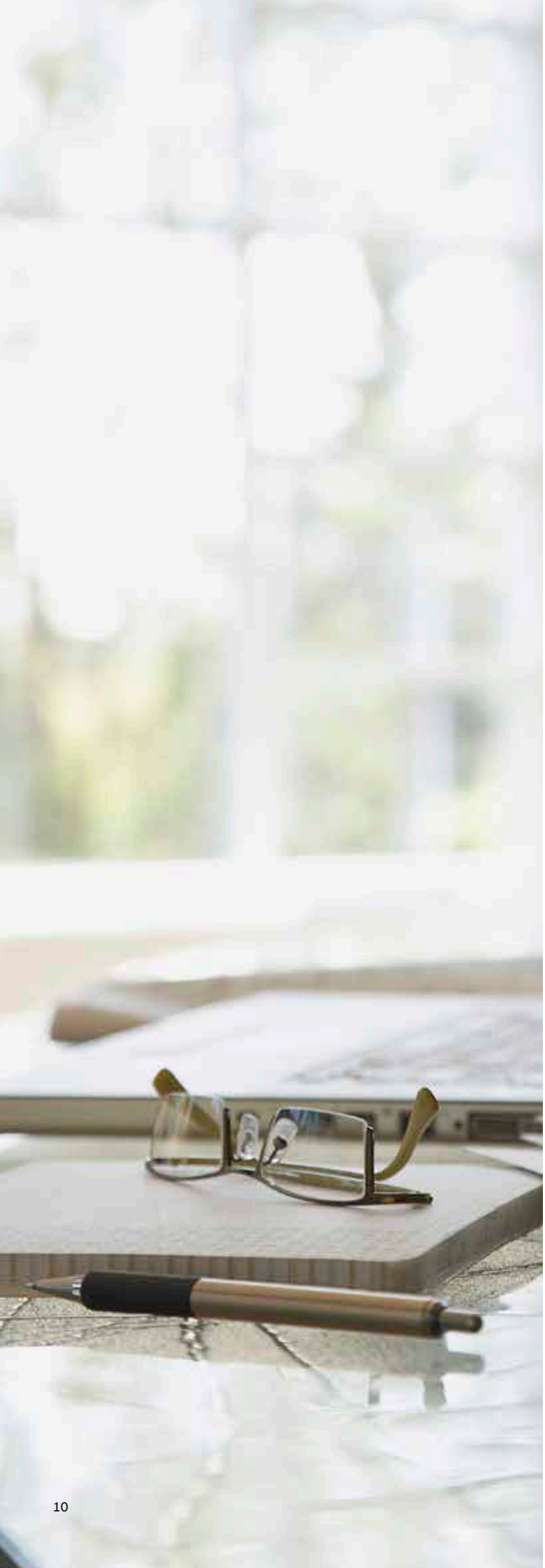
- Introducing new roles to enable the ICO to remain productive, efficient and effective as its regulatory brief becomes more complex
- An anticipated increase in headcount to 'in excess of 600 FTE by April 2020'
- A new funding model

The ICO's data protection work was funded through fees levied on organisations that process personal data, unless they were exempt. This was done under powers granted in the Data Protection Act 1998.

When the GDPR came into effect on 25 May 2018, it removed the requirement for data controllers to pay the ICO a fee, The Government has, therefore, set out a new funding structure in the Data Protection (Charges and Information) Regulations 2018, which is based on the relative risk to the data that an organisation processes. Under the structure, data controllers' fees are in three tiers based on the relative risk to the processing of personal data, with the fees for larger companies rising from £500 per annum to £2,900 per annum. ICO fines will, however, continue to be returned to Government.

For further details see https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/02/new-model-announced-for-funding-the-data-protection-work-of-the-information-commissioner-s-office/

HM Treasury has also given the ICO flexibility on its salary costs for the next three years, which will help the ICO to recruit and retain the right people to drive forward its progress and organisation, and we should expect to see this translated into increasing levels of proactivity.



For further information, please contact a member of the Regulatory & Public Policy Team or Security, resilience and privacy team.

Eamonn McGrath
Partner

T: +44 20 7951 2082
M: +44 7771 945 494
E: emcgrath@uk.ey.com

Pragasen Morgan
Associate Partner

T: +44 20 7197 7831
M: +44 7341 078 673
E: pmorgan@uk.ey.com

Loree Gourley
Director

T: +44 20 7951 2000
M: +44 7717 388 926
E: lgourley@uk.ey.com

John Jarrett
Director

T: +44 20 7951 7364
M: +44 7391 585 044
E: john.jarrett@uk.ey.com

Jane Hayward Green
Associate Director

T: +44 20 7783 0881
M: +44 7788 356 021
E: jgreen4@uk.ey.com

Notes

Notes


Ctrl

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP

The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.

Ernst & Young LLP, 1 More London Place, London, SE1 2AF.

ED None

EY-000067514.indd (UK) 06/18. Artwork by Creative Services Group London.

In line with EY's commitment to minimise its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/uk