Data protection

GDPR One year on

ico.
Information Commissioner's Office

GDPR: One year on

This update

The purpose of this update is to reflect on our experiences over the past year and share what we have learnt about the GDPR and its impact a year after its implementation.

We describe some of the work we have undertaken to deliver the six goals set out in our Information Rights Strategic Plan. This includes supporting the public to use their new rights, working with organisations to provide support and guidance and using our new enforcement and investigation powers. The report also covers how we are working to stay relevant and foster innovation and ensuring we are a well-resourced, influential regulator on the national and international stage.

As well as describing what we have delivered in the first year of the new regime and some of our ongoing work, we look ahead to our priorities and focus for the year ahead.

We describe a year of:

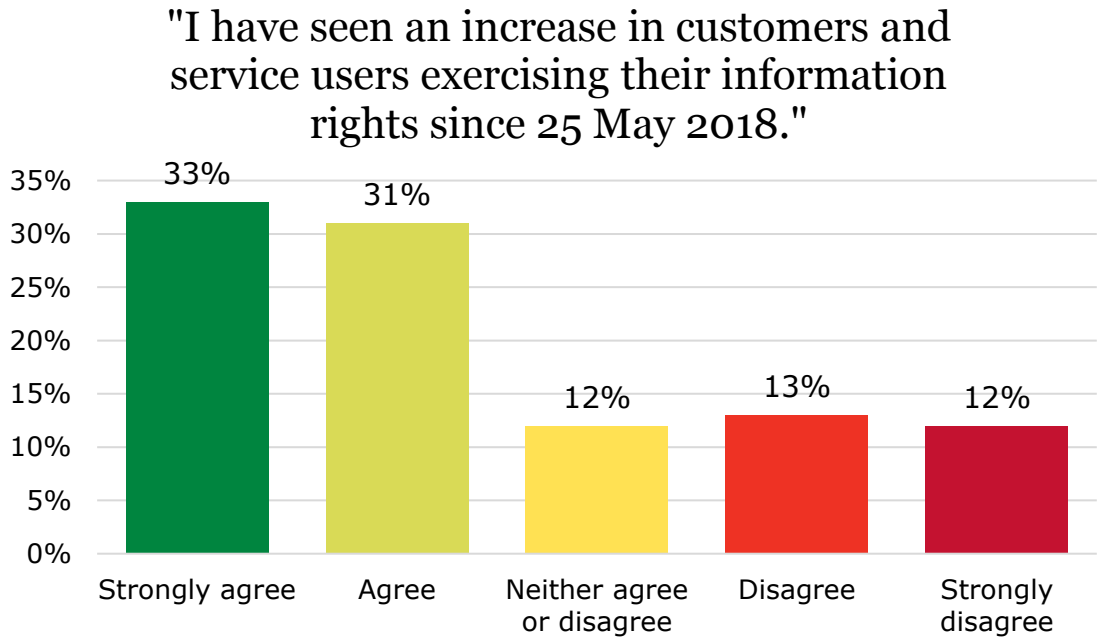
Supporting

The public

The first year of the GDPR has seen people realise the potential of their personal data. There is a greater awareness of the law, in particular the data rights of individuals, and a greater awareness of the role of the regulator where rights aren't being respected.

Research conducted for us in July 2018 found one in three (34%) people have high trust and confidence in companies and organisations storing and using their personal information – significantly up from the 21% stating this in 2017.

In March we surveyed DPOs, and 64% stated that they either agreed or strongly agreed with the statement 'I have seen an increase in customers and service users exercising their information rights since 25 May 2018'.



Note: These figures have been formatted so that they are rounded to the nearest whole number.

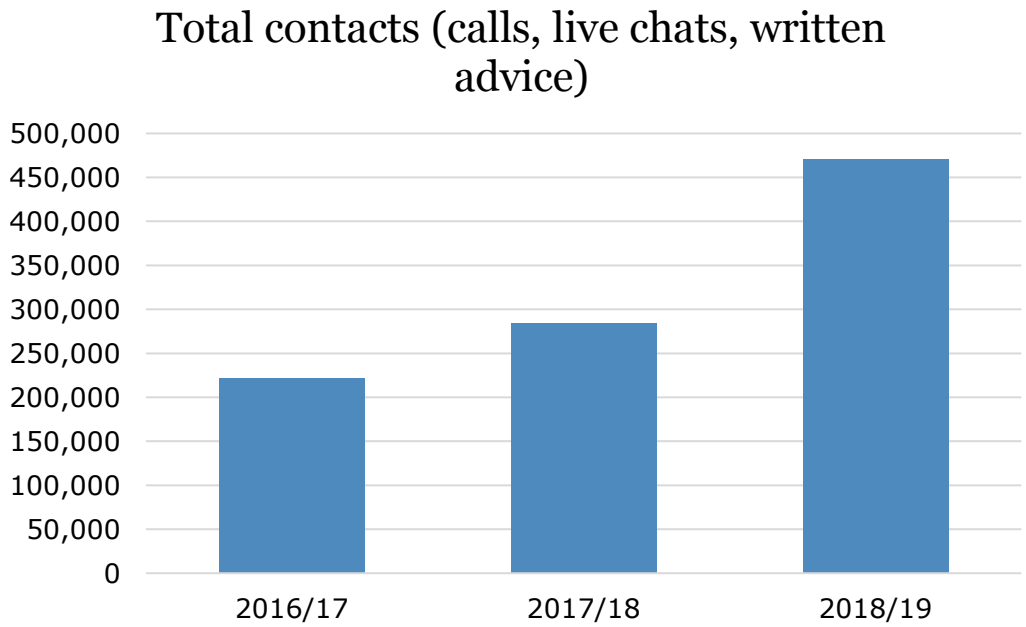
This increase in awareness has been supported by the ICO's Your Data Matters campaign. This campaign aims to increase awareness of the enhanced data protection rights individuals have under the GDPR, highlighting how people can exercise these rights and promoting our online guidance products. This campaign has led to a 32% (over 2.5 million) increase in individuals accessing our website.

We've been working to support the public throughout. This may have been direct through one of our many expanded public facing services or through an organisation using one of the various tools we have made available for companies, small or large, to explain the new laws and rights. We have also launched a number of investigations to highlight and address otherwise opaque or invisible processing of personal information so the public are aware how their data is being used.

Data Protection Officers

At the same time, the push to be ready for the GDPR prompted organisations to make significant changes. They determined the legal basis under which they collected personal data, inventoried the data they held, examined how data was used in their supply chains and refreshed their consents.

This heightened engagement and understanding of the rights and responsibilities in the new regime has been reflected in the volume and nature of our contact and engagement with businesses, organisations and individuals. Our helpline, live chat and written advice services received over 470,000 contacts in 2018/19, a 66% increase from 2017/18.



In larger organisations, the GDPR has placed a significant responsibility on DPOs, bringing with it the ongoing challenge of normalising the new regulations.

Nominations received for this year's Practitioner Award for Excellence in Data Protection demonstrated the creative and dynamic way this community of privacy professionals has responded to this challenge.

At our annual Data Protection Practitioners' Conference (DPPC) in April 2019, we presented the award to Mikko Niva of Vodafone Group Services Ltd. Mr Niva delivered a pioneering privacy compliance programme for Vodafone - not just in the UK, but across 21 different countries. He also took a leadership role outside of Vodafone, speaking on privacy at a range of conferences during the year. Mr Niva's award follows on from the 2018 winner, Esther Watt, Data Protection Officer at North Kesteven Council. Ms Watt led a programme for the council to ensure a smooth and positive transition towards GDPR compliance.

Many other examples of similar work across all industries were showcased throughout the nominations for this award, including:

- demonstrating the future benefits of GDPR compliance to the business;
- producing guidelines and training modules, tailored to the needs of each business, to help to make the GDPR understandable to their organisation;
- running specific companies which aid SMEs or charities with GDPR compliance;
- embedding privacy by design and Data Protection Impact Assessments (DPIAs) by default for all new work processes;
- developing GDPR action plans to embed data protection principles throughout organisations;
- awareness raising and cultural change by emphasising that the GDPR is a company-wide responsibility. In some organisations, this has included making every employee accountable for the information they work with; and
- working with other organisations within their sector to provide support and best practice at a sector level.

This award helps to demonstrate some of the work being done throughout the UK to embed the principles of the GDPR into organisations.

It also shows the importance of an embedded DPO with the right support. The challenges faced every day by DPOs means that having the seniority

and engagement from board level is critical to their success. Resourcing these roles should be a key priority for both public and private sector organisations.

When we surveyed DPOs as part of the DPPC 2019, the responses showed that the majority of DPOs felt that they received great support from within their organisation. The importance of culture was considered to be one of the biggest issues for implementing the GDPR and so it is encouraging to see that at least two-thirds of all respondents were satisfied with their senior leadership support. More than 90% of DPOs had an accountability framework in place and 61% reported that their framework is well understood in their organisation. Overall, three quarters of DPOs said that their information rights messages were getting through to their senior leadership team, and they felt supported in developing a framework to embed these rights in their organisation.

Clearly this is positive progress in under a year, but maintaining momentum will be key. There is still a long way to go to truly embed the GDPR and to fully understand the impact of the new legislation – in our survey nearly 50% of respondents faced unexpected consequences as a result of the GDPR.

To help, we have continued to produce guidance and blogs to support organisations, building on the success of our early 'myth-busting' advice and our comprehensive guide to the GDPR, published in the run-up to 25 May 2018. Businesses around the world used this guidance in the run-up to 25 May and beyond: between 1 April 2018 and 24 May 2019, it had 16.6 million views on our website.

SMEs

Beyond the DPO community, we recognise that it hasn't been easy for small organisations to become GDPR compliant. Legal bases for processing, data auditing and privacy policies take time to understand and there are no quick fixes for making sure people's personal data is being processed legally. For sole traders this has been particularly difficult.

To help this vital community understand their responsibilities, we provided a suite of resources, support and guidance on our website tailored to the needs of sole traders and small organisations, including toolkits and checklists, podcasts and FAQs. For further help and advice, we offered a dedicated helpline and live chat service and held advisory

sessions attended by hundreds of SMEs. In addition to these services we will also soon be establishing within the ICO a one-stop shop for SMEs, drawing together the expertise from across our regulatory teams to help us better support those organisations without the capacity or obligation to maintain dedicated in-house compliance resources.

All organisations

To help organisations understand their obligations we have produced a Guide to the GDPR, which also integrates content related to the DPA 2018. We have also produced an interactive tool to help organisations to understand the lawful bases for processing, as well as a tool to assist with the continued flow of data in the event of a no-deal Brexit.

We have also produced an in-depth Guide to Law Enforcement Processing for those who have day-to-day responsibility for data protection in organisations with law enforcement functions. Supporting those covered by the new Law Enforcement Directive has also been a key service in the year after its implementation.

We have put comprehensive guidance in place – our aim is now to focus on where existing guidance still needs to be updated and ensure we continue to provide a clear and comprehensive guide to the law. We will also continue to provide new areas of support for organisations, such as codes of conduct and certification, and to continue to bust myths – with blogs covering some misconceptions about topics as wide-ranging as data sharing, personal data flows after Brexit and to offer our annual festive reassurance that the GDPR won't affect Christmas.

Alongside our guidance, we also have responsibility for creating four statutory codes for data sharing, direct marketing, age-appropriate design and data protection and journalism. These codes are being developed and will play an important part in supporting the implementation of the GDPR in these areas.

Age appropriate design code

A key concept of the GDPR is that children merit special protection. This code, known colloquially as the children's code, aims to help achieve that. The children's code sets out 16 standards of age-appropriate design which we expect providers of online services and apps to meet when their apps are likely to be used by children or when they process children's personal data. This is a key example of how important and effective data

protection by design can be. The code builds on Parliament's set of minimum standards to be taken into account.

The consultation on the draft code closes on 31 May 2019. It was created following a call for views from June to December 2018, which included a survey for parents, carers or children to give their views.

Data sharing code

The data sharing code will update our existing data sharing code of practice, which was published in 2011 under the DPA 1998. Data sharing brings important benefits to organisations, citizens and consumers, making their lives easier and helping with the delivery of efficient services.

One of the myths of the GDPR is that it prevents data sharing. This isn't true. The GDPR aims to ensure that there is trust and confidence in how organisations use personal data and ensure that organisations share data securely and fairly. To achieve this, it is important that data controllers have clear guidance on data sharing so that individuals can be confident that their data is shared securely and responsibly.

A call for views on the data sharing code closed in September 2018. We are currently considering the views presented to develop a draft code for formal consultation. We expect to launch that consultation in June 2019 and for the code to be laid before Parliament in the autumn.

Direct marketing code

The direct marketing code aims to ensure that direct marketing continues to be a useful tool for organisations to engage with customers to grow their business or publicise and gain support for causes. It must also avoid being intrusive and ensure that all activities are compliant with the GDPR, DPA 2018 and the Privacy and Electronic Communications Regulations (PECR).

A call for views closed in December 2018 and we are currently considering the feedback. This will inform a draft code; we expect to launch a formal consultation on this in June 2019 and to finalise the code by the end of October. We will review the code once the new European Union e-privacy regulation is completed, and update if necessary.

Data protection and journalism code

The data protection and journalism code aims to strike a balance between privacy, respect of individuals' rights, and freedom of expression. The

code will provide clear and practical guidance on what the law requires to achieve this. This builds on guidance we produced under the Data Protection Act (DPA) 1998 in response to the Leveson Inquiry. We will also be working with the press regulators to ensure that the code fits within the wider framework for the industry.

The call for views was published on 29 April 2019 and closed on 27 May 2019. Following this, we will review the views presented and develop a draft code for formal consultation. We expect to launch that consultation in June 2019 and lay the code before Parliament in the summer.

Political parties

In July 2018 we published our Democracy Disrupted? report. This report emerged from our investigations under the DPA 1998 into the use of personal data in political campaigns. While we have produced guidance on political campaigning, the investigation demonstrated the need for a wider code of practice, as parties and campaign groups now increasingly use personal information and data analytics to target and influence voters.

A code of practice is vital to retain the trust and confidence of the electorate, ensuring that all personal data used in political campaigns is used in a way which is transparent, understandable and lawful. The code will explain how to do that.

The code will apply to all organisations who process personal data for the purpose of political campaigning, ie activity relating to elections or referenda.

Under the GDPR, the Commissioner has the power to produce codes of practice. However, it is our position that it would be preferable for this code to be given statutory footing under the DPA 2018, so that it has the same legal status as the other four codes. We have called on the Government to legislate to this end.

A call for views on this code closed on 21 December 2018. We are currently considering the views presented to develop a draft code for formal consultation. We expect to launch that consultation in July 2019.

Taking action

Enforcing

Whilst providing support and guidance to organisations is a key part of the ICO's role, we will not hesitate to act in the public interest when organisations wilfully or negligently break the law. Enforcing the GDPR is not just about big fines; it's about using all the tools set out in our Regulatory Action Policy. In this policy we set out our objectives for regulatory action:

- We will respond swiftly and effectively to breaches, focusing on those involving highly sensitive information, adversely effecting large groups of individuals or those impacting vulnerable individuals.
- We will be effective, proportionate, dissuasive and consistent in our application of sanctions, targeting our most significant powers on organisations and individuals suspected of repeated or wilful misconduct or serious failures to take proper steps to protect personal data.
- We will support compliance with the law, including sharing information in relation to and otherwise contributing to the promotion of good practice and providing advice on how to comply with all aspects of legislation.
- We will be proactive in identifying and mitigating new or emerging risks arising from technological and societal change.
- We will work with other regulators and interested parties constructively, at home and abroad, recognising the interconnected nature of the technological landscape in which we operate and the nature of data flows in the expanding digital economy.

The policy also sets out how we will use our enhanced powers to pull back the curtain on processing where the public have concerns, for example social media companies, political parties, data brokers and the use of new technologies by law enforcement agencies.

We are increasingly using our powers to change behaviours. We have tools at our disposal and will use these to ensure individual rights are upheld and organisations comply with the law. Our recent action against HMRC for failing to get consumer consent to use their voices in

recognition software resulted in us issuing HMRC with an enforcement notice and ordering them to delete the records of five million individuals.

Under the GDPR we are able to issue formal assessment notices to any organisation either public or private. Under the DPA 1998 the Commissioner only had compulsory audit powers in respect of central government and health organisations. These new powers of inspection have enabled us to proactively respond to concerns raised by the public about unsolicited marketing communications and fair and unlawful processing. We have issued 15 assessment notices under the new law in conjunction with our investigations into data analytics for political purposes, political parties, data brokers, credit reference agencies and others.

We have also issued organisations with warnings and reprimands across a range of sectors including health, central government, criminal justice, education, retail and finance. We have issued 11 information notices which have allowed us to progress our investigations and inform our action.

To make sure our enforcement work is targeted in the right areas, we use the information we receive from the public and other sources to inform our strategic threat assessment and support our investigations and enforcement work. This includes information from personal data breach reports, concerns reported to us by the public and working with other regulators.

CASE STUDY

Use of powers in our high profile investigations – the changing landscape

In May 2017 we launched a formal investigation into the use of data analytics for political purposes after allegations were made about the 'invisible processing' of people's personal data and the micro-targeting of political adverts during the 2016 EU referendum.

The inquiry eventually broadened and has become the largest investigation of its type by any data protection authority, involving social media online platforms, data brokers, analytics firms, academic institutions, political parties and campaign groups.

Our investigation was conducted under both the previous and new legislation. In order to seize evidence as part of the investigation we requested a warrant which meant it took 17 days from the outset to gain access to Cambridge Analytica's premises. Our powers have broadened and we now have greater control and flexibility over powers to help this type of situation. 'No-notice' assessment notices mean we should be able to have access to companies' data protection practices faster than under the previous legislation.

We issued the first enforcement notice under DPA 2018 to Aggregate IQ, a Canadian data broker and one of the organisations that formed part of the investigation. It ordered the company to delete certain personal data it held about UK citizens.

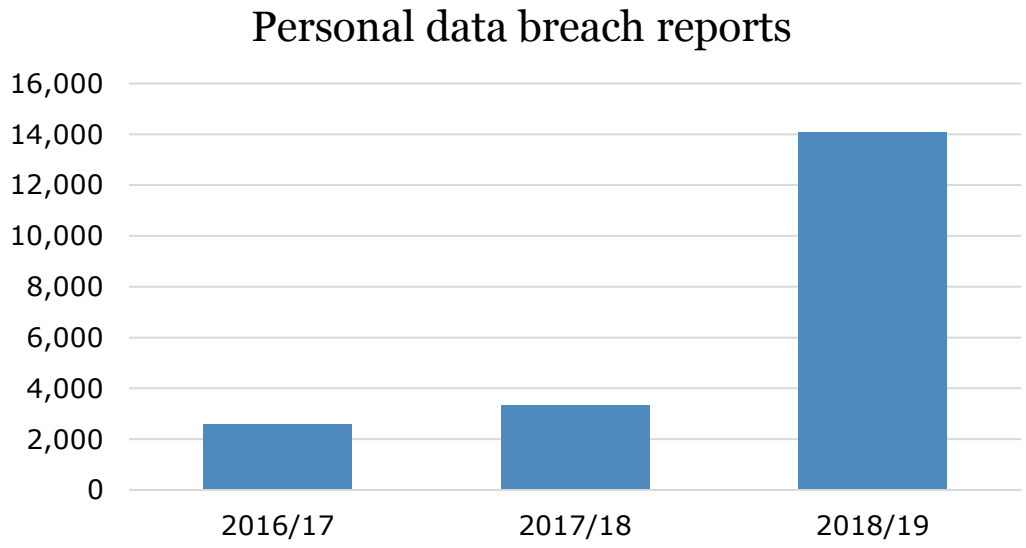
Under the previous legislation we issued Facebook with a £500,000 fine because of the timing of the breaches. As we have stated in the past, the fine could have been higher under the new legislation.

Before 25 May 2018, most companies had to agree to an audit. Now we have the power to issue assessment notices - and we did so soon after the introduction of new laws in order to understand how the three credit reference agencies and three main data brokers collect and use people's personal data for direct marketing.

Information notices have continued to be issued before and after the introduction of the GDPR, but we now have the ability to issue 'urgent' information notices which will assist with all fast-moving investigations.

Acting on personal data breaches

We received around 14,000 PDB reports from 25 May 2018 to 1 May 2019. For comparison, we received around 3,300 PDB reports in the year from 1 April 2017.



We closed over 12,000 of these cases during the year. Of these, only around 17.5% required action from the organisation and less than 0.5% led to either an improvement plan or civil monetary penalty. While this means that over 82% of cases required no action from the organisation, it demonstrates that businesses are taking the requirements of the GDPR seriously and it is encouraging that these are being proactively and systematically reported to us. These figures also show that it remains a challenge for organisations and DPOs to assess and report breaches within the statutory timescales. We recognise this and provide support and guidance to help organisations to meet the requirements to report.

The personal data breaches reported to the ICO have resulted in a range of outcomes.

An example of a breach reported where no further action was required:

A nursery produced Father's Day cards for the children to take home. Within the card was a photo of the child. There were two children with the same name at the nursery, which accidentally put child A's photo in child B's card and vice versa. No further action was required and our view was that this breach was not reportable – it is unlikely individuals' rights and freedoms would be impacted by the wrong photo being sent out. We provided advice to the nursery about reporting thresholds.

An example of a breach that did require further action from the organisation, but did not require formal action from the ICO:

An organisation was late submitting two reports to us, but one didn't meet the reporting threshold. Advice had been given previously and some

steps taken to make improvements to the breach reporting process, so the ICO sought further assurances about future improvements to practices and reporting.

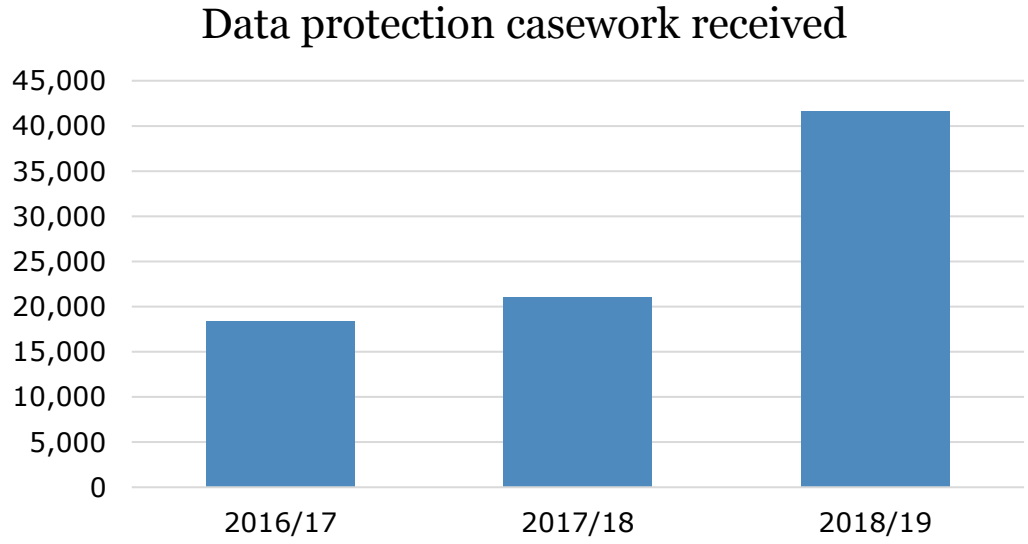
An example of a breach where the ICO took formal action:

As a result of administrative errors, an organisation disclosed personal data to incorrect recipients. Our investigation determined that whilst this was not a systemic failing, it nevertheless demonstrated that established policies and procedures were not always being followed. The organisation was therefore issued with a reprimand to take certain steps to improve compliance with the GDPR, including ensuring that all staff attended mandatory training; that policies and procedures be enforced and reiterated to staff on a regular basis; and that contact details be checked on all correspondence.

Responding to public concerns

Greater awareness of individual rights has meant that we have seen a significant impact on the numbers of concerns raised with us by the public. From 25 May 2018 to 1 May 2019, we received over 41,000 data protection concerns from the public. The figure for 2017/18 was around 21,000.

Subject access requests remain the most frequent complaint category, representing around 38% of data protection complaints we received. This is similar to the proportion before the GDPR (39%). In fact, the general trend is that all categories of complaint have risen in proportion with the overall increased number of complaints since the implementation of the GDPR.



We also see that some sectors are responsible for higher numbers of breach reports and data protection concerns. The health sector, for example, accounts for over 16% of PDBs and 7% of data protection complaints. Local government accounted for 8% of PDBs and 9% of data protection complaints. Lenders accounted for 6% of data protection complaints. This intelligence helps us to target our guidance, support and action in the areas where there is the greatest regulatory risk.

Working with others

In the modern world, data truly has no borders. The GDPR has an international impact, applying to every company which does business in Europe. Our international strategy commits us to maintaining the strong links we have in Europe and beyond. It also sets out a clear vision of where we need to develop our capacity to share investigatory information and to share best practice from international exemplars.

EU Data Protection Board figures indicated that from 25 May 2018 to 1 May 2019, there were around 240,000 cases across the EU (data protection complaints, data breaches, proactiveinvestigations or other similar issues). We received over 55,000 of these (roughly 23%). Where the data protection cases reported have cross-border implications throughout the EU, these are reported to a lead EU data protection authority. The UK is currently the lead supervisory authority on 93 of these cases.

In addition, the UK is working on behalf of UK citizens to uphold their information rights in 58 other cases where other EU data protection authorities are the lead supervisory authority, and the UK is a concerned supervisory authority.

We continue to grow and strengthen our links with the EU supervisory authorities to support ongoing data protection work, protecting the information rights of UK citizens. On a wider global stage, in October 2018 the Information Commissioner was elected as chair of the International Conference of Data Protection and Privacy Commissioners (ICDPPC), which brings together around 120 data protection offices across the world.

This role gives the UK an ability to not just share policy and enforcement experience, but to take on a leadership role within the global privacy and information rights community.

On a national level we have continued to develop and build relationships with other regulators including joining the UK Regulator's Network (UKRN). These relationships not only support our enforcement and operational work, but also enable us to ensure that data protection and information rights are a key topic across sectors.

Enabling innovation

Developing Sandbox

The GDPR requires businesses and organisations to focus on comprehensive data protection, embedding sound data governance in all processes. As organisations meet this challenge, we will encourage innovation through our approach to engagement and regulation.

In March 2019 we opened the beta phase of our regulatory sandbox, a new service designed to support organisations using personal data to develop products and services that are innovative and have demonstrable public benefit.

The Sandbox will enable participants to work through how they use personal data in their projects with our specialist staff to help ensure they comply with data protection rules. We expect that many of the products that will come into the Sandbox will be at the cutting edge of innovation and may be operating in particularly challenging areas of data protection where there is genuine uncertainty about what compliance looks like.

Delivering the Grants Programme

In 2018 we introduced a Research Grants Programme to promote good practice and support independent, innovative research and solutions, focused on privacy and data protection issues, to help to deliver long-term improvements to information rights. This gives the UK research community a stronger voice in how information rights evolve and to find solutions for privacy and data protection issues. We have earmarked £1m of funding for this programme over four years.

In 2018, we awarded grants to four organisations:

- Open Rights Group: Development of a digital tool to help individuals protect and enforce their information rights, particularly in the insurance and banking sectors. As part of the research a website,

Data Rights Finder, was created to make contents of privacy policies more understandable. This allows a better understanding of how personal data is collected and used and what people can do about this. This also increases clarity about how personal data is being used for near-instant decisions for financial products.

- Imperial College London: Development of an online tool for the public and organisations to evaluate the risk of re-identification of pseudonymised data.
- Teeside University: Development of a prototype software tool for healthcare professionals to capture patient privacy preferences to allow sharing medical information securely to support research (as part of the Great North Care Record). Data sharing can lead to better outcomes for patients, as well as data-sharing for research leading to major advances for treatments. The research included evaluation of the tool with focus groups on ease of use, which also allowed patients to see the effect on the availability of their data. The tool captures privacy directives in fine and coarse-grain detail and providesreat benefits to privacy. It could be adapted for existing healthcare systems.
- London School of Economics: A project looking at children's information rights and privacy, with the intention of it leading to the production of an accessible online toolkit for children, parents and teachers to increase their awareness and competency around online privacy. This research particularly looked at children's capacity to consent, children's understanding of privacy and the potential risks related to this. This research work has clear links to our work to keep children safe online, which is also being progressed through our age-appropriate design code.

We also selected four innovative research projects to receive a total of over £275,000 in funding for Phase 2. These initiatives were:

- Connection at St Martin's in the Field: A project to engage with homeless people in London to better understand their knowledge and awareness about how their personal information is used. As well as providing an effective means of informing homeless people of their data rights and how to enforce them, the project will create an outreach process that can be taken up by other organisations.
- Oxford University: A study of six smart homes to study current privacy preferences and to prototype new tools, interfaces, and

approaches to smart home privacy. The project team will also gain an understanding of how these alternative design approaches might be integrated into processes and disseminate the resulting best practices.

- PHG Foundation: A project researching the nature of pseudonymised genomic data, its function as personal data under the GDPR, uses in medical research and how any potential associated risks may be mitigated.
- Cardiff University: A project to develop a training programme for researchers working with a wide range of routine public sector data.

Growing the ICO

Our people

The work outlined above has created challenges for the ICO in how we deliver our new powers and responsibilities, as well as meeting the growth in demand for our services as a result of the DPA 2018 and the GDPR.

During 2018/19, our workforce grew from 505 to more than 700. As demand for, and interest in, our work continues to increase into 2019/20, we are anticipating further increases to our workforce, eventually taking the ICO to an anticipated 825 full-time equivalent in early 2020/21. That will mean the ICO has almost doubled in size over three years.

As might be expected, training and developing our new staff has been a key feature of the past year.

We have appointed significant numbers of new staff to specialised roles: we doubled the size of the Data Protection Complaints Directorate, which was already our largest department, and we more than doubled the size of our Customer Contact department. At the same time, we have reviewed our structures, processes and use of technology to ensure we are delivering our services in an efficient and effective way, with a new service excellence programme continuing to guide our expansion plans.

To meet the challenges of the GDPR it was vital to recruit and retain staff with the right mix of skills and experience. A review of our pay arrangements helped to mitigate the risks posed by uncompetitive pay. We have also developed different ways of attracting the right

people, including developing secondments, apprenticeships and research fellowships.

Keeping pace with developments in technology and cyber security is fundamentally important to our work. The challenges are as real for the ICO, as a regulator, as they are for those we regulate. As well as expanding our capacity to deal with the increased work, we have needed to increase our capability to deal with more complex areas.

Some of the most significant data protection risks to individuals, including cyber attacks, AI, cross-device tracking and machine learning, are now driven by the use of new technologies.

Last year we produced our Technology Strategy, which set out our plans in this area. During 2018/19, we took some significant steps to increase our technology capability and deliver that Technology Strategy. We also established a new Executive Directorate for Technology Policy and Innovation.

This increased capability in technology has already been hugely beneficial, contributing heavily to our Age appropriate design code to protect children from harm online. It has also allowed us to establish a Regulators and AI forum, which will let regulators share best practice on regulating AI.

These changes, together with the accompanying expansion of physical and technical infrastructure, were key to the ICO being able to meet the demand from DPA 2018, and was affordable because of the associated changes to our funding model.

Our resources

As the profile, responsibilities, powers and size of the organisation have increased, the ICO's funding has been reviewed to ensure it is well resourced to deliver its vital role.

Under the previous funding model, organisations with fewer than 250 employees paid a data protection fee to the ICO of £35. Under the new model, organisations with ten or fewer staff and charities pay a fee of £40, while organisations with between 11 and 250 staff pay £60. Large organisations with over 250 staff previously paid a fee of £500, butnow pay £2,900.

In the past year the number of organisations paying the Data Protection fee increased by 16%, compared to a historic average yearly increase of 6%. However, due to the funding model change, this meant that our fee income increased by 86% in 2018/19 compared to 2017/18.

In the short term, it is vital that we continue to be adequately resourced to deliver against our responsibilities under the DPA 2018. We will continue to grow the numbers of organisations paying the fee and push for every single organisation required to pay the fee to do so.

In November, we issued our first penalty notices for non-payment of the data protection fee. Up to 30 April 2019, we issued over 3,800 notices of intent to fine for failure to pay the fee, and of these we received nearly 2,300 payments totalling around £627,000. For the same period, over 300 Final Penalty Notices were issued for non-payment of fees, resulting in nearly £100,000 in fees and penalties. In 2019/20, we will continue to investigate where companies have not paid the fee, particularly large companies.

An increase in the number of organisations paying the fee will not mean we have unlimited funding. We will resource ourselves according to our goals. If the income from fees consistently outstrips our needs, it will bring the potential to reduce the fee for all organisations, reducing the burden for every organisation, but ensuring that burden is shared equally.

Looking forward

As we take stock of all that has changed and been achieved in the year, it is clear there is much left to do. We will continue to strive to deliver regulatory outcomes which support our mission of upholding information rights for the UK public in the digital age and the trust and confidence in how data is used.

We will continue to focus on the areas identified as our regulatory priorities. These include:

- cyber security;
- AI, big data and machine learning;
- web and cross-device tracking for marketing purposes;
- children's privacy;
- use of surveillance and facial recognition technology;

- data broking;
- the use of personal information in political campaigns; and
- freedom of information compliance.

We will focus on ensuring our work is aligned to these priorities, keeping pace with the way the privacy and information rights landscape is changing. As the public's attitudes to how their information is used changes, we have an opportunity to make a real difference.