DATA PROTECTION NEWS REPORT

Pritchetts

PRITCHETTS LAW LLP

7 NOVEMBER 2022

Welcome to our Data Protection News Report!

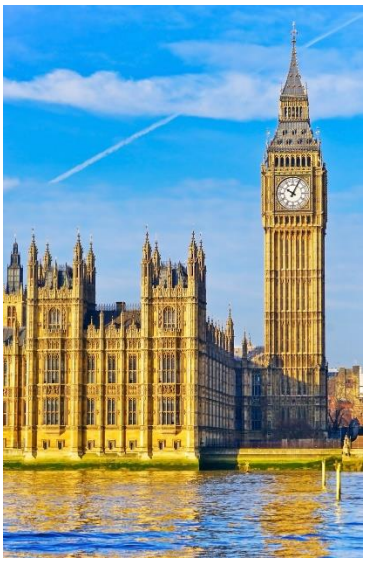
We've rounded up the most important data protection news stories from the last few months.

First, there's our summary of the direction that UK data protection legislation is now heading in, after numerous twists and turns.

Next, check out our take on the biggest enforcement action stories of the year: not just the organisations that have been named and shamed, but also tips on how businesses can optimize their own data protection setup.

Finally, there's an update on fresh guidance from the ICO, including the all-important developments with international data transfers, which we know will affect many of our clients.

We hope that, armed with coffee and biscuits (or is that just us?!), you'll find this a useful summary to digest.



UK Data Protection Legislation: Where Are We Up To?

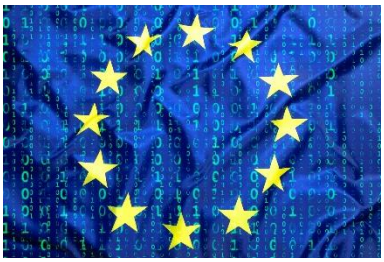
It was as recently as 2018 that we were getting up to speed with the shiny new EU General Data Protection Regulation ("**EU GDPR**") and its UK complement, the Data Protection Act 2018 ("**DPA 2018**"). Then, as we exited the EU, the UK government issued a statutory instrument – the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 under the European Union (Withdrawal) Act 2018. Those regulations amended the DPA 2018 to reflect our exit from the EU, and merged it with the requirements of the EU GDPR to form a data protection regime that now applies in the UK (the "**UK GDPR**").

This year, another major change to UK data protection legislation was launched – apparently to take advantage of our exit from the EU. The Data Protection and Digital Information Bill ("**DPDIB**") was introduced to Parliament in July 2022 and contained many amendments that diverge from the UK GDPR. However, its progress through the legislative process was cancelled after Liz Truss's appointment as prime minister. Subsequently, several spokespeople, from both government departments and the Information Commissioner's Office ("**ICO**"), confirmed that the DPDIB had been officially withdrawn. One said he felt sorry for his colleagues in government, who now have to start all over again.

However, the writing had been on the wall for the DPDIB after a speech by Michelle Donelan, the new digital secretary, at the recent Conservative Party conference. In it, she reiterated the government's intention to move away from the EU GDPR and indicated that the DPDIB was set for further changes. "*We will be replacing GDPR with our own business- and consumer-friendly British data protection system,*" she said. "*Our plan will protect consumer privacy and keep their data safe, whilst retaining our data adequacy so businesses can trade freely.*"

What might come next?

Many data protection professionals and practitioners now await more news with some trepidation. However, the government's stated intention to retain the UK's data protection adequacy from the EU's perspective (so that personal data can flow freely between the EU and UK) gives us hope that any changes will not be as great a threat to adequacy as we might fear.



Let's remember that, in June 2021, the EU ruled that the UK offers an "essentially equivalent" level of data protection to both its EU GDPR and its EU Law Enforcement Directive. However, it also reserved the right to change its mind if the UK diverged too far from EU law.

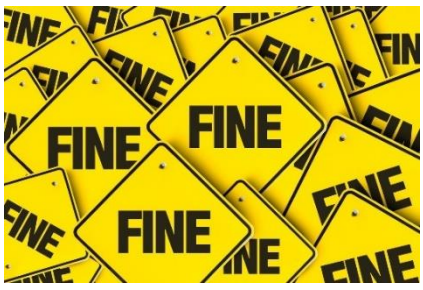
Many practitioners are concerned that the UK government's plans will see that divergence extend too far and risk the UK's adequacy status. Yet Michelle Donelan rejected this in her speech, stating, "*We will look to those countries who achieve data adequacy without having GDPR, like Israel, Japan, South Korea, Canada and New Zealand.*" We imagine that those who had been drafting the now-defunct DPDIB had already been looking at how close they could sail to the wind when seeking inspiration from those other countries. Now, though, it's back to the drawing board, and it remains to be seen if a new course, or just a small turn, will be required.

And what of the promised landfall? Donelan declared, "*I can promise ... that [the new British data protection system] will be simpler and clearer for businesses to navigate. No longer will our businesses be shackled by unnecessary red tape.*"

This sounds commendable if your organisation is only focussed on operations in the UK. However, initial soundings from our clients and contacts reveal concerns that any significant divergence may mean more cost and more, not less, red tape for the many UK organisations conducting business in any part of the EU. They will be forced to comply with at least two divergent data protection regimes. The level playing field for businesses that had been anticipated with the original introduction of the EU GDPR now doesn't seem so level for the UK and anyone doing business with us.

The next general election is currently scheduled to take place no later than January 2025. However, with the recent turbulence we've experienced in UK politics, including Rishi Sunak following the ousted Liz Truss as prime minister, it could well be much sooner. A root-and-branch redraft of the proposed new data protection legislation should be followed by some effective consultation. That will all take considerable time, so the UK legislation may remain in its current state for some time.

Fine-ding Out the Hard Way



The current game of legislative hot potato (see above) could make organisations think that now might be a good time to sit tight and hold off on data protection compliance activities until the situation is clearer. Guess what, though? Recent enforcement news indicates that this would not be the right approach!

Fines and enforcement

The ICO – the UK data protection regulator – and its European counterparts have issued numerous fines and enforcement actions this year. Despite Brexit, EU activity is still noteworthy to many of our multinational client organisations and may also signal potential regulatory approaches in future similar cases here in the UK. We've summarised a few of the key decisions below and offered some learning points.

- **Vulnerability to cyberattacks.** On 24 October 2022, the ICO issued a whopping £4.4 million penalty to Interserve Group, a construction company, for failing to keep secure the personal data of up to 113,000 current and former employees. The chain of events began with an Interserve employee forwarding a phishing email. Interserve's systems did not block or quarantine the email, and its recipient opened it and downloaded its content. This caused malware to install itself on the employee's workstation. Interserve's systems quarantined the malware and raised an alert, but the company did not investigate thoroughly enough. The attacker retained access to Interserve's systems and went on to disable its antivirus software and compromise 283 systems.

The ICO found that Interserve failed to put in place appropriate technical and organisational measures to prevent unauthorised access. It used outdated software and protocols, didn't provide adequate staff training and carried out insufficient risk assessments.

Lessons to learn

Establishing appropriate technical and organisational measures to protect personal data is one of the central elements of the GDPR. And it's not something that organisations can do once and then leave to one side; it's crucial for them to review their approach regularly so that they can stay protected in an evolving threat landscape.

We've helped many organisations to put in place appropriate technical and organisational measures for their business. We can help you draft policies and procedures, demonstrate accountability, protect yourself from breaches and a whole lot more, so do get in touch if we can help.

- **Non-compliant marketing profiling and calls.** On 6 October, the ICO announced that it had fined catalogue retailer Easylife £1.48 million for breaching UK data protection legislation. It had carried out non-compliant profiling by inferring health information from previous purchases, and had made over one million aggressive, unsolicited marketing calls to vulnerable individuals.

The ICO fined the organisation £1.35 million for using the personal data of 145,000 customers to target them with health-related products without their consent and an additional £130,000 for making well over a million predatory direct marketing calls. During its investigation, the ICO found that Easylife had performed significant profiling of customers, including 'invisible' processing of their health data. (The term 'invisible' reflects the fact that the individuals were unaware that their personal data was being collected and used for marketing purposes.)

The Easylife fine came hot on the heels of fines issued to four home improvement companies for making predatory and non-compliant marketing calls to people registered with the Telephone Preference Service.

Lessons to learn

All five of these cases should prompt organisations to (re!) consider their existing marketing practices and ensure that they have performed an in-depth review of their marketing profiling practices, if relevant. The ICO has recently issued some guidance on direct marketing using live calls, and direct marketing by email as well, so Pritchetts can help with adapting to that guidance too!

- **Non-compliant marketing emails.** Don't forget to check that your marketing emails are being sent in a compliant way: the ICO recently fined Halfords £30,000 for sending unsolicited marketing emails to people without their consent.

Lessons to learn

Under electronic marketing rules, organisations can't rely on what's known as the soft opt-in exemption (whereby organisations can send electronic marketing messages to customers whose details have been obtained during the course of a sale or negotiations for similar services) unless they have previously offered those people a simple way to opt out. Organisations need to have offered this when they first collected people's details, and with each subsequent communication.

Many of our clients came unstuck on this when reviewing their customer databases in the run-up to the GDPR – can you prove that you gave that opt-out when you first collected the data? We regularly work with clients to review risk on marketing databases, and we also offer training specifically aimed at marketing professionals, so do get in touch if you need a hand.

- **Non-compliant handling of subject access requests (SARs).** SARs are regarded as the lynchpin of data protection legislation, and the requirement is usually to respond to a SAR within one month, or three months in some special situations. However, in September, the ICO announced that it had reprimanded seven organisations, across both the public and the private sector, who repeatedly failed to meet this statutory deadline. A reprimand is essentially a public naming and shaming, and a warning that next time, there will be much more serious consequences.

Speaking in connection with this case, the Information Commissioner, John Edwards (newly appointed in January 2022), highlighted that SARs were "*an essential gateway to accessing other rights. Being able to ask an organisation 'what information do you hold on me?' and 'how is it being used?' provides transparency and accountability and allows the person to ask for changes to be made or even for the information to be deleted.*" The organisations 'caught' included Virgin Media, various councils, a police organisation, the Home Office and the Ministry of Defence.

Lessons to learn

Many organisations struggle with handling SARs in a compliant way, so they could easily find themselves being named and shamed in the same way. Those of our clients who have found handling SARs difficult until they come to us often haven't had to deal with many before, so they haven't had processes in place to handle them. The ICO has given some pointers on how to get

the basics right, and here at Pritchetts, we'd love to help you build processes so that your organisation doesn't get caught on the hop!

- **TikTok could be fined £27 million for failing to protect children's privacy.** During its investigation of the video-sharing app, the ICO found that Tiktok may have breached UK data protection legislation between May 2018 and July 2020.

The ICO believes that TikTok may have processed:

- The data of children under the age of 13 without parental consent, and failed to provide proper information to its users "*in a concise, transparent and easily understood way*".
- Special category data – which includes ethnic and racial origin, political opinions, religious beliefs, sexual orientation, trade union membership and genetic, biometric or health data – without legal grounds to do so.

As a result, the regulator has issued a "notice of intent", which is a precursor to a potential fine. If TikTok were fined £27 million, it would be the largest fine ever issued by the ICO, exceeding the £20 million handed to British Airways two years ago after an incident in 2018 that saw the personal details of more than 400,000 customers compromised by hackers.

Lessons to learn

The maximum fine possible under the UK GDPR would be 4% of TikTok's total annual worldwide turnover for the preceding year. The ICO must now consider further representations from TikTok before taking a final decision. Historically, this has been a difficult area for the regulator because big-name organisations throw the full weight of their legal teams behind their defence.

If your organisation needs assistance with reviewing its data processing involving children, and ensuring that this is in line with the ICO's Children's Code, let us know.

Data security considerations

- **Does your organisation allow the use of private email and messaging apps?** The pandemic led to greater use of third-party email and apps as people shifted to remote- and home- working environments. In July 2022, the ICO called for a review of this use within government and officially reprimanded some of the bodies involved.

Lessons to learn

Organisations must assess the data security risks of using such systems. They must also consider how they monitor use and what Bring Your Own Device policies they have in place. Are they consistent with the ICO's guidance? If you need help with reviewing and advising on your use of such systems, please let us know.

- **Are your data security policies and breach-handling processes up to date? What would you do in a ransomware situation?** The ICO and the National Cyber Security Centre have said that they stand together against ransomware payments being made. They suggest that paying the ransom doesn't reduce the risk to individuals because it doesn't guarantee that the information will not be released; also, it incentivises criminals.

Lessons to learn

We've helped many of our clients to review and update their policies and procedures, both pre-emptively and when they've been in the thick of a security breach, so please let us know if your organisation would like some help with this.

Outside the UK...

The ICO isn't the only regulator who's been busy doling out fines. In September 2022, its Irish equivalent – the Data Protection Commission ("**DPC**") – issued Instagram with a record Irish fine of €405 million under the EU GDPR. (This followed Instagram's widespread disclosure of email addresses and phone numbers of children using its business account feature, and a public-by-default setting for children's personal Instagram accounts. These practices have since ceased.)

It's the second highest fine under the EU GDPR since it came into force (the highest being Luxembourg's penalty of €746 million to Amazon). It's also the first EU-wide decision on children's data protection rights. It follows the DPC's previous largest GDPR fine of €225 million, which it imposed on WhatsApp back in September 2021 (a hugely interesting case to read, not least in relation to invisible processing and transparency issues with non-user data that was uploaded).

Fresh Updates to ICO Guidance

Of course, enforcement and fines are only two aspects of the regulator's role. The ICO has also been busy creating new guidance, so what news of that?

- There has been some significant movement this year on **guidance for international data transfers.** On 21 March 2022, three documents came into force:
  1. The international data transfer agreement ("**IDTA**").
  2. The international data transfer addendum to the European Commission's standard contractual clauses for international data transfers ("**Addendum**").
  3. A document setting out transitional provisions.

  This was the result of long-running efforts, including an ICO consultation that we at Pritchetts contributed to back in 2021.

Action points

Organisations must now use the new IDTA/Addendum for new international data transfer arrangements. For any existing arrangements that use the old EU standard contractual clauses ("**SCCs**"), organisations have until 21 March 2024 to adopt the new IDTA/Addendum. In the meantime, the data processing must not have changed and there must not have been a change to the safeguards provided by the old EU SCCs.

That time will fly by, so please get in touch if we can help – we've helped many of our clients to achieve compliant international data transfers. The ICO has promised to provide clause-by-clause guidance on how to use the IDTA/Addendum, and how to complete a

Transfer Risk Assessment on any international data transfers. However, we're not expecting this to be a quick process, so we won't be holding our breath…

- The ICO has published **updated guidance on direct marketing**. Its temporary page contains links to resources, support and guidance to help organisations. Among these is some refreshed guidance on direct marketing by email, which encompasses "*emails, texts, picture messages, video messages, voicemails, direct messages via social media or any similar message that is stored electronically*".

The guidance is a temporary measure before the ICO publishes the formal Direct Marketing Code of Practice – a requirement of the UK GDPR in its current form. Remember: a Code of Practice has additional weight, and must be considered by the ICO and the courts when deciding on whether organisations have been compliant and what enforcement action should be taken. The ICO has said that the guidance that it has published on its website will form the basis of the Code, subject to new data protection legislation coming into force in future.

Action points

Organisations should check that their marketing activities across all channels, and all marketing databases, are set up to assist compliance. Keep an eye out for updates from the ICO, particularly around the time when the new data protection legislation comes into force.

- The ICO has launched a **consultation on guidance for monitoring workers**. It has compiled draft guidance about monitoring at work and prepared an impact-scoping document. The guidance will affect all organisations that monitor their workers, so do check out the draft and get involved in the consultation: it closes on 11 January 2023.

Action points

As ever, it's important to be vigilant about compliance when monitoring your workers, including when using newer devices such as dashcams, body-worn cameras and cameras that record remote working. However, monitoring workers applies to the simpler stuff too, such as monitoring email accounts, internet usage, telephone usage, etc.

We deliver training on monitoring and other HR-related issues, and also help clients to compile data protection guidelines that cover worker and HR issues, so do get in touch if you'd like to know more.

- The ICO has issued **new guidance on the research provisions in UK data protection legislation**. Publication of the guidance follows the ICO's consultation in February 2022. In an opinion piece in September 2022, Ian Hulme, the ICO's Director of Regulatory Assurance, said that the guidance should offer confidence to researchers and research participants. He expressed his belief in the value and importance of research and said, "*The new guidance is practical and speaks to issues that researchers, statisticians and archivists face in their day-to-day lives when it comes to data protection.*"

Action points

We work with lots of organisations whose remit is to carry out research, or who need to do so in their organisations, particularly as technology and innovation grow apace. This new guidance from the ICO, in conjunction with its additional forthcoming guidance (see below), will be imperative to compliance in their future growth.

- The ICO has also been developing its **draft guidance on anonymisation, pseudonymisation and privacy-enhancing technologies ("PETs")**. It had already created some existing guidance on AI and data protection, which it co-authored with the Alan Turing Institute. Now, the ICO is expanding this work by drafting some guidance on anonymisation, pseudonymisation and PETs. The consultation on this is currently open, but is due to close on 31 December.

So far, the draft guidance has been released in separate units for consultation. In September 2022, the ICO published its latest section – draft guidance on the use of PETs – and is now seeking feedback to help refine and improve it.

PETs can help organisations to process personal data responsibly, lawfully and securely. They can minimise the amount of data used and encrypt or anonymise personal information. The ICO points out that financial organisations already use PETs when they investigate cases of possible money-laundering, for example. In addition, the healthcare sector currently uses PETs to provide better health outcomes and services to the public.

The UK and US governments are also actively engaged in exploring the possibilities of PETs. In July 2022, they launched a joint initiative to offer a set of prize challenges to consider the potential of PETs to tackle combat global societal challenges. The ICO is one of several bodies that will be supporting the scheme.

Action points

We've helped several of our clients with issues relating to AI, so if your organisation is likely to be affected by these changes in guidance, do let us know. Of course, if you would like to consult us on your use of AI and new tech more generally, we can help with that too.

- The ICO has made available some **training materials for businesses and organisations** to use – for free! The modules might be too specific for your organisation's requirements, or not detailed enough for your various teams, but they offer a good place to start!

Action points

If the ICO's training materials have highlighted a knowledge gap in your organisation, or you're looking for a more detailed or bespoke package, we're experts in delivering data protection training. We offer modules that we develop with you to tailor them to your organisation's needs, and also more general data protection training courses, with a range of dates to choose from. Both types of course are delivered by our two expert data protection lawyers, so do get in touch if you think this might be what you're after.

- There's been some movement recently on **the EU–US data transfer framework**. On 7 October, US President Joe Biden signed an executive order to implement the framework that was announced back in March 2022. On the same day, Michelle Donelan, the new UK digital secretary, met with US Secretary of Commerce Gina Raimondo to discuss digital priorities. Donelan announced, "*The US shares our democratic values, digital priorities and commitment to high standards of data privacy.*"

  It is hoped that the implementation of the EU–US data transfer framework will end the uncertainty that many organisations have faced following the ruling by the European Court of Justice in the Schrems II case. Many practitioners – and the European Commissioner for Justice, Didier Reynders – have expressed their view that a fresh legal challenge is highly likely, but it is hoped that there will be real improvement from the previous EU–US Privacy Shield.

  The process of approval, followed by the EU issuing its adequacy decision, is expected to take about six months, so there should be some developments by Spring 2023. No doubt we will hear further news of UK/US adequacy discussions before long.