

Welcome to the Spring issue of our Data Protection Newsletter!



We've looked back over the last three months to round up the most important data protection news stories of the year so far.

It was a relief to see the [new UK Data Protection Bill introduced](#) at the beginning of March, after its predecessor was shelved amid the disorder that followed Boris Johnson's departure from office. We've provided our initial thoughts, with more to follow soon!

AI has been hitting the headlines recently too, especially with the release of ChatGPT and Google Bard. But how can organisations manage the risks associated with using AI? The [ICO has released some new guidance on AI and data protection](#).

Across the Channel, the ECJ has issued an interesting judgement on the [conflicts of interest that may arise when appointing a DPO](#). We give you our view on the interplay between this and the DPDI 2.

There's also been an interesting judgement in the English High Court regarding the [use of private messaging apps in the workplace](#). We've offered some tips on the steps that employers can take.

Finally, as the cost-of-living crisis continues to bite, many are keen to make savings on their energy bills – but at what cost? Read [Energy Suppliers: the Balance Between Cost Savings and Privacy](#).

New UK Data Protection Bill Introduced ... Again

The original Data Protection and Digital Information Bill (“DPDI”) fell victim to the political chaos that followed the ousting of Boris Johnson as prime minister, and was shelved.

Since that original draft in July 2022, we have been awaiting developments with bated breath. Finally, on 8 March 2023, the newly created Department for Science, Innovation and Technology introduced a new version of the DPDI – [the Data Protection and Digital Information \(No.2\) Bill](#) (“DPDI 2”) – for its first reading in Parliament.

In its [press release](#), the government said that the DPDI 2 will “*introduce a simple, clear and business-friendly framework that will not be difficult or costly to implement – taking the best elements of GDPR and providing businesses with more flexibility about how they comply with the new data laws*”. It also emphasised the importance of maintaining data adequacy with the EU, which has been a major concern for businesses since the reform of UK data protection law was announced.

There hasn't been much change between the two versions, but when the DPDI 2 is compared to the existing rules in the UK, there is plenty to unravel. The DPDI 2 is a complicated beast, which makes it difficult to provide a straight answer about what the actual changes are. In summary, the DPDI 2 will

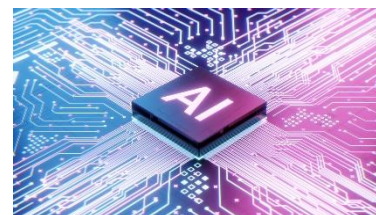




amend the existing UK data protection legislation (which includes the Data Protection Act 2018 (“**DPA 2018**”), the UK’s implementation of the General Data Protection Regulation (“**GDPR**”), and the Privacy and Electronic Communications Regulations (“**PECR**)). It doesn’t simply replace those with one easy-to-read document.

We thought that it would be helpful to analyse the DPDI 2 and summarise its key changes. Our work on this is ongoing (the DPDI 2 alone is over 200 pages long!), but we will publish it as soon as it’s available. Do check back [here](#) regularly to make sure that you don’t miss out!

ICO Releases New AI Guidance



The use of artificial intelligence (“**AI**”) continues to proliferate in many sectors, including healthcare, recruitment and commerce, to name a few. AI can bring many benefits to organisations and individuals, but its use can entail risks too.

On 29 March, the UK government released a policy white paper on its [pro-innovation approach to AI regulation](#). And just prior to that white paper, the UK data protection regulator, the Information Commissioner’s Office (“**ICO**”), had updated its [Guidance on AI and Data Protection](#). Its work results from requests by UK industry to clarify the requirements for fairness in AI. Whether the ICO’s thoughts and government policy are completely aligned remains to be seen.

The ICO’s stated aim is to *“continue to ensure ICO’s AI guidance is user friendly, reduces the burden of compliance for organisations and reflects upcoming changes in relation to AI regulation and data protection”*.

Its updates include:

- ❖ New details on what organisations should assess in their data protection impact assessments (“**DPIAs**”) for AI systems.
- ❖ A new chapter on how the key data protection principle of transparency applies to AI.
- ❖ New information about using AI systems to make inferences, create affinity groups and process special category data.
- ❖ New content on fairness in AI.



The ICO has emphasised that the guidance is not a statutory code. Instead, it provides advice on how to interpret data protection law in relation to AI. It also makes good-practice recommendations for technical and organisational measures that mitigate the risks to individuals that AI might cause. There is no penalty for failing to adopt its recommendations, as long as organisations find another way to comply with the law.

Here at Pritchetts Law, we work with many clients to clarify and resolve data protection issues with their use of AI. If this is something you would like help with, you can find out more [here](#), or [get in touch](#) – we’d love to hear from you.

ECJ Rules on DPOs and Conflict of Interest

The GDPR requires certain organisations to appoint a Data Protection Officer (“DPO”). These include public authorities, organisations that monitor individuals regularly and systematically on a large scale, and those whose core activities involve processing large-scale special category data and data relating to criminal convictions and offences.



Many organisations choose to designate the role of DPO to an existing employee with other roles, rather than establishing a stand-alone figure. This is in line with Article 38 (6) of the GDPR, which states that a DPO “may fulfil other tasks and duties. [The organisation] shall ensure that any such tasks and duties do not result in a conflict of interests”.

And there lies a key problem for organisations ... **how do you assess those conflicts of interest?**

On 9 February 2023, the European Court of Justice (“ECJ”) issued an [important ruling](#) on this area of EU data protection law. Although that ruling won’t directly apply to the UK, courts and the ICO’s views may be persuaded by the decision. The ECJ stated that a conflict of interest may exist where DPOs are entrusted with other tasks or duties that would result in them determining the objectives and methods of processing personal data on the part of the controller or its processor.



So, when organisations select a DPO, they must ensure that they carefully assess whether the employee’s current role(s) might conflict with their duties as a DPO. Their assessment should consider all relevant circumstances, including organisational structure. A useful source of information here is the EDPB’s [Guidelines on DPOs](#), which offers a non-exhaustive list of conflicting positions within an organisation. It says that these may include “senior management positions (such as chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments) but also other roles lower down in the organisational structure if such positions or roles lead to the determination of purposes and means of processing”.

It will be interesting to see what impact the DPDI 2 will have on the state of play with DPOs. As this newsletter is issued, the current proposal is to create a new role of “senior responsible individual” (“SRI”) to replace the DPO. The new role appears very similar to that of the DPO, but some key distinctions are currently proposed:

- ❖ An SRI will only be required where the organisation is a public body, or carries out processing that is likely to result in a high risk to the rights and freedoms of individuals. The previous requirements to designate a DPO if carrying out “regular and systematic monitoring of data subjects on a large scale” or “processing on a large scale of special categories of data” have been removed.
- ❖ The SRI must be part of the “senior management”. This calls into question whether outsourced DPO services will be permitted, and if so, how.

So, if this switch to an SRI is made in the UK, will organisations that work across borders – with EU GDPR obligations or expectations – still retain the higher standard of a DPO?

See above for [New UK Data Protection Bill Introduced](#) and watch this space as the bill moves through the parliamentary process!

Please [get in touch](#) if you need help over time to determine whether you need a DPO or an SRI.



Use of Private Messaging Apps in the Workplace

The recent furore over the leak of more than 100,000 WhatsApp messages that were sent between Matt Hancock and other members of the Cabinet at the height of the Covid-19 pandemic has reignited the debate about employees' use of private email and messaging apps.

It hasn't even been a year since the [Information Commissioner's report](#) on the use of these apps by government staff during the pandemic was published in July 2022. The report concluded that such use presented real risks to transparency and accountability within government, and called for change. In addition, the ICO issued a reprimand under the UK GDPR, requiring that the Department of Health and Social Care improved its practices.

A case in point

However, this issue is not exclusive to government. Recent media stories have exposed the unacceptable use of WhatsApp by police officers, but it is a more general conundrum for employers up and down the country. Earlier this year, the [English High Court refused to strike out a misuse of private information \("MPI"\) claim that a former employee had taken against her employer.](#)

During her separate claim of sexual harassment at work leading to unfair dismissal, the claimant's employer had produced thousands of her WhatsApp messages to undermine her credibility. The employer argued that a significant portion of the messages had been downloaded to a work laptop, but the court did not accept that this meant that they had lost their private character. Its judgement also questioned why the employer had kept the messages and failed to notify its employee when it found them, especially given that no proceedings were underway at the time. A likely outcome is that the employer could struggle to identify an appropriate legal basis for its processing activities in this regard.




So, what should employers do?

For employers more generally, lines have become blurred as employees use private messaging apps such as WhatsApp for personal communications, for interactions with their colleagues and for business purposes. Employers should carefully consider the balance to strike and mitigate the risks by:

- ❖ Keeping in mind their obligations to their employees under data protection law and in terms of their employees' right to privacy.
- ❖ Putting in place a robust set of policies, including on social media, communications and bring your own device ("BYOD").

These should cover the use of private messaging apps during employees' period of employment and information about what will happen to their messages when they leave the organisation. The policies should also define what the employer regards as appropriate and acceptable behaviour, and explain that disciplinary action may result if the policy is not followed.

 We've helped many clients to create [data protection policies, procedures and guidelines](#) that are tailored to their organisation and form part of a cohesive and accessible data protection framework. Why not [get in touch](#) for further details?

- ❖ Training their staff on their policies, and how they should conduct themselves on apps such as WhatsApp, and with communications more generally.

💡 **We offer a range of data protection training courses, with dates available throughout the year. You can find out more and book [here](#), or [contact us](#) so that we can discuss your needs.**



Energy Suppliers: the Balance Between Cost Savings and Privacy

In his Spring Statement on 15 March 2023, Chancellor Jeremy Hunt announced that the annual energy bill for a typical UK household will remain at £2,500 until the end of June, rather than rising to an anticipated £3,000. However, this still constitutes a huge increase in energy prices from a year ago, and businesses and households continue to struggle with the cost-of-living crisis. Therefore, both groups are keen to explore ways to reduce their energy usage and save money.

Many solutions – including smart meters, Internet of Things (“IOT”) devices, smart electric heating systems and electric vehicle (“EV”) charging – are available, but some of them rely heavily on technical processes and the use of customers’ data, much of which is personal data.

Collecting such data can carry considerable risk. For example, for householders, it is likely to be easy to discover their daily routine, so someone viewing the consumption profile might be able to determine whether the property was unoccupied, or whether a child was home alone. Abuse of IOT devices has also been cited in cases of harassment, bullying and coercive control.

However, there are also possible gains from the availability of data from smart meters or domestic IOT devices. For example, for those living in sheltered housing, an out-of-routine activity could act as a warning sign to the care organisations who manage the accommodation.

Privacy by design

Given the potential benefits of collecting data from smart meters and IOT devices, the challenge is ensuring privacy by design. Customers may feel concerned about the control that they are surrendering to a remote, probably automatic source, and the extent to which they will have to part with their data to do so.



Energy companies will need to explain their data collection practices for these devices, and have an appropriate legal basis to support them. When they analyse their practices, they may need to perform a legitimate interests assessment (“LIA”) to prove that they gave everything proper consideration. Doing so will help to bring them in line with the UK GDPR’s accountability principle.

For more on this story, check out our [blog](#). In the meantime, if you’re looking for a pragmatic and commercial approach to balancing privacy requirements with commercial objectives on your own innovative data-led project, please [get in touch](#) to find out how we can help you.