

Welcome to the February edition of the Data Protection and Privacy newsletter.

2023 was another busy year for data protection, and this edition of the newsletter explores some of the key issues and developments we have seen businesses navigate, and the upcoming changes we can expect to see.

In this issue we cover:

- Sharing Data with law enforcement authorities
- New ICO Guidance for Organisations
- Legislation Update : DPDI
- The EU AI Act
- The Online Safety Act
- A round up of recent enforcements

Our Data Protection and Privacy Team are always on hand to help with any of your data protection compliance needs. If you have any feedback on the newsletter, issues you would like us to cover or any queries, please contact us at: dataprotection@prettys.co.uk.

Emma Loveday-Hill
Head of the Data
Protection and Privacy
Team



eloveday-hill@prettys.co.uk

Sharing data with law enforcement authorities

Sharing personal data is one of those potentially difficult areas of data protection where, in certain circumstances, companies do it without necessarily realising that's what they are doing. This is particularly true of when law enforcement authorities ask for information, for example, if they want to see CCTV footage. Complying with such a request is, unfortunately, not as straightforward as it might initially seem.

The Information Commissioner's Office (ICO) has provided guidance on "Sharing Personal data with law enforcement authorities" which sets out when data can be shared with competent authorities. It is important to note that if a company wishes to share the data, it still needs to identify a lawful basis to do so under Article 6 of the UK GDPR. If the data includes sharing special category data, then an Article 9 lawful basis will also need to be identified. In addition, if a company wishes to share criminal offence data, then the relevant schedules of the Data Protection Act 2018 will also need to be complied with.

So, what does this mean? If a company has received a request for data, if there is a crime to report, or if the police wish to investigate a crime, the company, as the data controller, must ensure that it thinks about the reason for sharing the data. Although it might seem that there is a legal obligation to share personal data, this may not always be the case. Even though the law enforcement authority may be insistent that the personal data is shared, the usual data protection principles need to be considered before any data is disclosed. This includes consideration of:

- whether the processing of the personal data is necessary and proportionate;
- how the amount of personal data shared could be minimised;
- what the Article 6 lawful basis for processing personal data will be (this will often be legitimate interest or legal obligation, however, this should be considered on a case-by-case basis);
- whether an Article 9 condition will be required if special category data is being processed;
- whether a condition in schedule 2 of the Data Protection Act 2018 has been met;
- how records will be kept and whether the Written Record of Processing Activities (RoPA) will need to be updated;
- whether any assessments need to be completed, for example, a Legitimate Interest Impact Assessment or Data Protection Impact Assessments to help justify the processing; and
- whether the personal data is being used for its original intended purpose.

We recommend that all companies put a process in place to ensure that any requests are dealt with consistently, and in accordance with the data protection legislation. In some cases, it may be clear that a request is likely to need to be complied with, for example if there is a warrant requiring it. However, in other cases it may not be so clear, and businesses should always consider asking for further information if needed, and this could include, narrowing the scope of the request to a certain time frame or a specific type of information.

If there is no legal requirement to provide the personal data, then of course a company may still decide that it is able to do so, for example, if it is in the legitimate

interests of the business and being used for the prevention and detection of crime.

This is also likely to be a permissible reason under Schedule 2 of the Data Protection Act 2018.

As we have said, it is not always straightforward. If you would like any further advice or guidance on this, please do contact us.



New ICO Guidance for Organisations

The Information Commissioner's Office (ICO) has released two new pieces of draft guidance for businesses relating to 'Recruitment and Selection' and 'Keeping Employment Records'. These two documents offer clarity and much-needed certainty to businesses to ensure they are compliant when processing records about candidates and employees. This guidance updates and replaces the 2011 Employment Practices Code, which was deemed no longer fit for purpose due to the subsequent changes in data protection laws and the ways people work in a post-pandemic world.

The updated guidance sets out what businesses are obliged to comply with during the recruitment process. It also helps to clarify obligations when using a recruitment agency.

Most interesting of all, the guidance provides advice on the use of automated decision making and profiling in recruitment – a crucial read for any business which uses or hopes to integrate AI as part of its recruitment process. It clarifies the risks that even partial automation of this process can have and provides suggestions for integrating AI in a way which avoids inadvertent discrimination and unfair treatment through meaningful human involvement.

It is important to remember if your business wishes to incorporate the use of automated decision making into your recruitment process you must be transparent and make candidates aware of its use. The best way to do this would be through a privacy information notice for candidates. If your business is using automated decision-making, then you should ensure that a Data Protection Impact Assessment (DPIA) is completed and regularly reviewed to ensure that it does not affect the individual's rights and freedoms.

The guidance on 'Keeping Employment Records' supplements the existing guidance on information about workers' health and employee monitoring. It outlines the legal requirements around employment records and explains what must be done, what should not be done and matters of best practice to help businesses to understand their data protection obligations to its employees.

Both pieces of guidance are still subject to change based on feedback received. Consultation on both documents will close on 5pm on 5 March 2024. They can be found at the following link, alongside other useful resources.

<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/>

Legislation update: The Data Protection and Digital Information Bill

The Data Protection and Digital Information (No.2) Bill (the Bill) is finally getting closer to receiving Royal Assent. The Bill is currently awaiting the Committee stage in the House of Lords after the conclusion of the second reading on 19 December 2023.

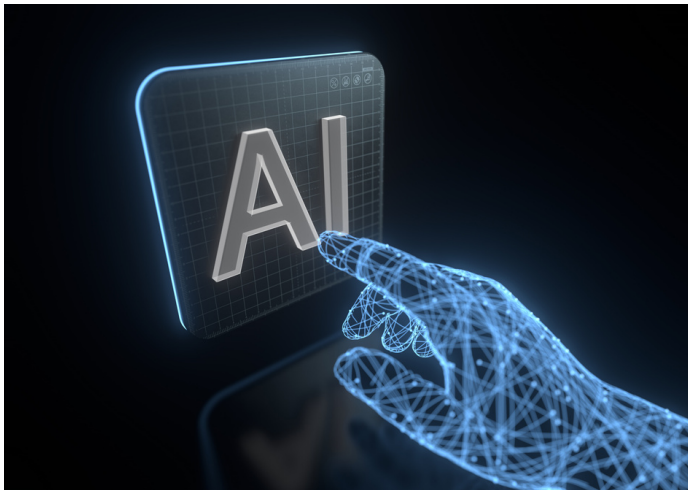
During its second reading, several key issues were debated while concerns were raised and areas for amendments highlighted. This included issues such as the use of AI, automated decisions making and the differences between data protection legislation in the UK versus in the EU.

The Bill looks to reform the UK's data protection regime by providing businesses with greater flexibility over the use of personal data. The Bill also aims to reduce the burden on UK businesses to comply with UK data protection laws and importantly means that businesses will



not (in theory) have to take any new additional steps to comply. However, the Bill does suggest reforming the Information Commissioner's Office (ICO) and changes to the Data Protection Officer (DPO) role to that of a Senior Responsible Individual (SRI). This could result in some substantial changes to the data protection legislation when the Bill comes into effect.

It is never too late for businesses to think about reviewing their data protection compliance, even with the expected changes to the data protection legislation, it is important that policies, assessments, and Records of Processing Activities (RoPA) are kept up to date. If your business needs assistance with its data protection compliance, our data protection team are happy to help.



Artificial Intelligence (AI)

Artificial Intelligence (AI) continued to dominate the headlines towards the end of 2023, and we have seen a development in the legislation surrounding it:

EU AI Act – why is it relevant?

The EU AI Act (the Act) provides a regulatory framework for AI in the EU. It was first proposed in 2021 and has since been subject to scrutiny and a number of amendments to reach an agreement which could be accepted by both the European Parliament and The European Council. In December 2023, we finally saw a provisional agreement reached and we are now awaiting the final legislation to be approved.

The Act looks to ensure that all AI systems used within the EU are safe, transparent, and non-discriminatory, as well as ensuring an element of human involvement to avoid negative and harmful outcomes. The European Parliament wants AI to encourage the innovation use of the technology and its development but regulate it to promote better conditions.

Part of the Act looks to assign a 'risk' to AI systems and any that are deemed to be of an unacceptable risk, meaning they are considered a threat, will be banned. Other risks will be assessed and will need to comply with transparency requirements under data protection legislation.

The Act will apply to individuals who are residing within the EU, therefore international businesses, including those in the UK who are developing AI systems that will affect those within the EU, will need to ensure their systems are compliant with the Act. This will have a similar territorial scope to that of the

GDPR. It may be beneficial for businesses to establish which 'risk' their AI systems will fall under when the Act comes into force to help further understand future compliance requirements.

The exact expected publication date is still unknown, however, it is likely that we will see the Act become law during 2024 and then businesses in the EU will have two years before the Act comes into effect in 2026.

Artificial Intelligence (Regulation) Bill

In November, we saw the introduction of the Artificial Intelligence (Regulation) Bill to Parliament. The Private Members Bill, starting in the House of Lords, aims to establish a central AI authority to regulate the approach to AI. The Bill takes its lead from the AI white paper we saw last year and introduces the role of AI officers to oversee AI compliance.

A Private Members Bill is introduced by member of Parliament and peers who are not government ministers. More often than not, these types of bills are unsuccessful, although they may influence future legislation.

In the "A Pro-innovation approach to AI Regulation" whitepaper, it was said creating legislation which regulates AI could hinder the pace at which this technology can develop. It will be interesting to watch if the Artificial Intelligence (Regulation) Bill goes any further and whether opinions have changes since to release of the whitepaper. There has not currently been a date set for any further reading of the bill, and we will have to see what happens next.

The Online Safety Act – A Safer Digital Landscape?

The UK Government has taken a significant step towards ensuring the safety of users online by recognising the need for a more robust regulatory framework to tackle the challenges created by today's digital landscape.

The Online Safety Act (the Act), which received Royal Assent in October 2023, introduces a new framework to regulate illegal and harmful online content, but what does the Act mean for users and digital platforms? New legal requirements are now in place for those who provide the following services:

- User-to-user services which allow users to encounter content that has been generated, uploaded, or shared by other users (such as social media platforms).
- Search services which enable users to search multiple websites and databases; and
- Internet services that publish or display pornographic content.

User-to-user services extend beyond social media platforms. Services which enable users to interact with content from other users (even if the interaction is not a material function or aim of that service) will be caught by the Act. There are, however, several exemptions that may apply.

While it may seem that large 'tech' businesses, online social media platforms, and search engines such as Google are likely to be most affected, the Act is also likely to capture thousands of smaller companies or platforms, including websites and forums where content can be shared, who promote via advertising, and platforms which allow users to interact with one another.

Some businesses which meet certain thresholds, will also be subject to additional duties, though this will depend on various factors, such as their size and functionality, as well as other factors. The Act also has a wider extra-territorial scope, meaning that businesses that operate outside of the UK, but provide certain services will also be caught by the Act.

What will businesses be required to do?

The cornerstone of the Act is the imposition of a "duty of care" on online platforms. The duty requires platforms to take reasonable steps to ensure the safety of their users and prevent harm caused by content on their services. Businesses will be expected to:



- Take steps to mitigate and manage harm to users. This will include removing illegal content, preventing it from being made available in the first place and preventing children from accessing illegal and harmful content.
- Putting in place systems and processes which enable certain types of content to be reported as appropriate.
- Establish complaint procedures for users. The procedure will need to be transparent and easy to use and appropriate action will need to be taken in response to each complaint. Some businesses will also be expected to comply with fraudulent advertising requirements.

What are the risks of non-compliance?

Ofcom is responsible for ensuring that those businesses that fall under the scope of the Act comply with the relevant requirements. Ofcom's enforcement powers means that it can issue monetary penalties of up to 10% of annual global turnover or £18 million (whichever is higher). Ofcom can also issue notices of contravention (to both service providers and individuals), which will set out which enforceable requirements must be complied with.

What next?

Businesses should now be thinking carefully about whether they will be required to comply with the new requirements and what practical steps to take to prepare for the new framework

This should include:

- Carrying out a risk assessment of current operations and platforms.
- Assessing if the business falls within the categories mentioned above and whether the extra obligations will apply.
- Reviewing internal systems and reporting procedures.
- Reviewing internal complaints procedures and terms of service.

While the Act has gathered support for its efforts to regulate the digital landscape, it has not been without its share of criticisms. Critics argue that the Act may inadvertently lead to over-censorship and suppress free speech. Striking a balance between protecting users and upholding freedom of expression remains a difficult challenge. Smaller platforms may also find it challenging to comply with the new regulatory requirements.

As the digital landscape continues to evolve, the effectiveness of the Act will need to be closely monitored as will whether its aim of making the UK the safest place to be online has been achieved.

For further information, or a copy of our webinar covering this subject, please do get in touch.

Recent enforcement

At the end of 2023, we saw a shift in the Information Commissioner's Office (ICO) enforcements away from data breaches and back to businesses who are breaching the Privacy and Electron Communication Regulations (PECR), especially in relation to direct marketing.

The ICO has started 2024 with enforcements already being issued for direct marketing breaches. This includes fining the food delivery company, HelloFresh. They have been fined £140,000 for send seventy-nine million spam emails and one million spam texts over a seven-month period.

While HelloFresh claimed users had opted into direct marketing, during the ICO's investigation, it was established that their opt in statement stated "Yes, I'd like to receive sample gifts (including alcohol) and other offers, competitions, and news via email. By ticking this box, I confirm I am over 18 years old". This not only fails to reference text messaging marketing but also combines age verification which could confuse and incentivise customers into agreeing to the statement. This not only affected current customers, but also those who had deactivated their subscriptions.

Enforcement action has already been taken against Poxell Ltd, a home improvement company, who have been fined £150,000 for making 2,647,805 unsolicited marketing calls. They came on the ICOs radar after they received 413 complaints from individuals who had received these calls after they had registered with the Telephone Preference Service (TPS). Complaints included calls being made to those with serious illnesses as well as referencing aggressive sales techniques. Poxell did not help with the ICOs investigation, and they continued to make these calls until their phone lines were stopped.

Another home improvement company, Skean Homes Ltd, have also been fined by the ICO for unsolicited marketing calls for people on TPS. Skean made over 600,00 calls in 2 months, the ICO found following their investigation after receiving thirty-one complaints. This resulted in Skean being fined £100,000 and issued an enforcement notice to prevent calls being made to those on the TPS in future.

What does this mean for organisations?

It is important to ensure your business complies with the UK Data Protection Legislation and the Privacy Electronic Communication Regulations (PECR). PECR imposes strict rules on when electronic marketing can be carried out, particularly when marketing is directed at individuals rather than companies. It is therefore important that marketing teams are trained in relation to direct marketing, and understand the requirements, including how to obtain valid consent and when the soft opt in can be used.

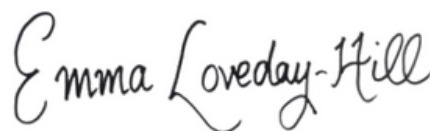
It is also useful to regularly carry out exercises to regularly cleanse mailing lists to ensure those who have unsubscribed or have joined services like TPS are removed.

If you need assistance with training your teams on direct marketing, we can provide online or in person training that is tailored to your business. Please do get in touch if you would like further information on how we can help.

Conclusions

I hope you have found this round-up useful. If you need any help with any of the issues covered, or anything else related to your data protection compliance, then please do get in touch. We have packages of documents available (for example, to assist with your AI compliance), and can also provide you with more bespoke advice on any particularly tricky issues you might be facing.

You can sign up to our data protection hub for our latest legal updates, articles, and invitations to our exclusive events at <https://www.prettys.co.uk/join-data-protection-hub>.



Emma Loveday-Hill
Head of the Data Protection and Privacy Team

THE DATA PROTECTION & PRIVACY TEAM



Matthew Cole, Partner
Emma Loveday-Hill, Head of Data Protection & Privacy Team
Maria Spencer, Solicitor
Bethan Moore, Data Protection Assistant

CONTACT US

dataprotection@prettys.co.uk