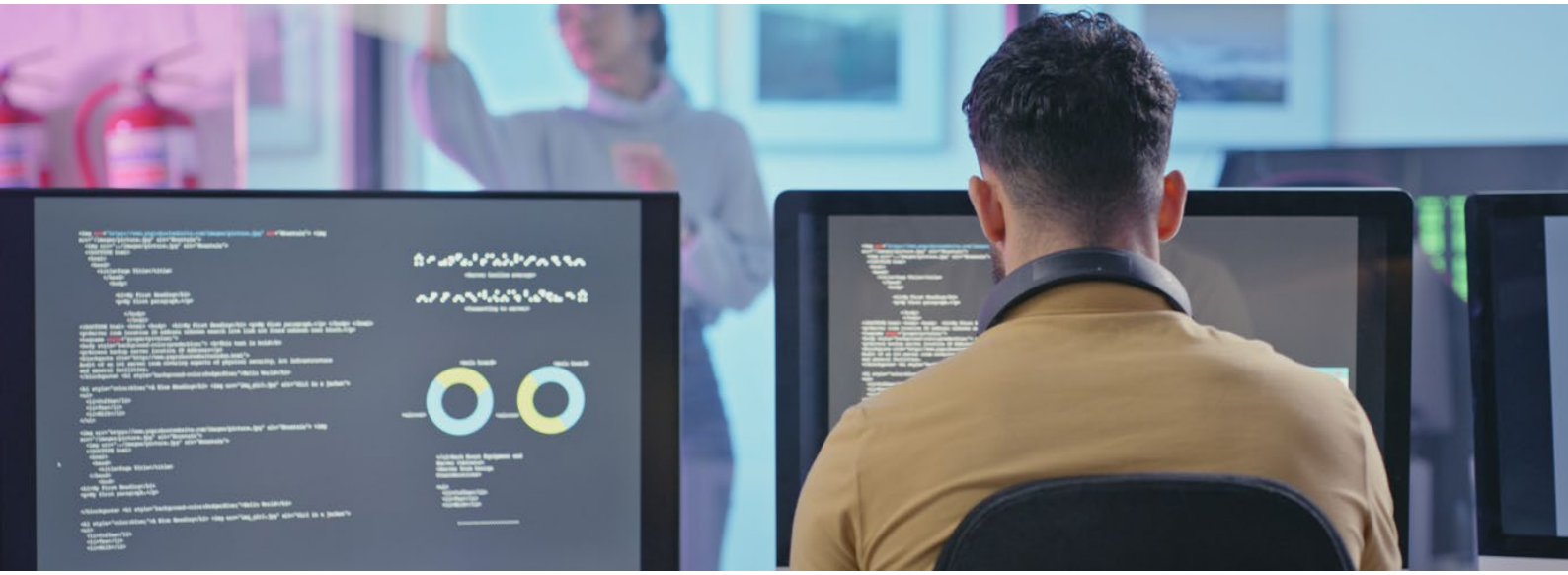

Data protection newsletter
Issue 15

It has been five years since the GDPR came fully into force. We now have a good idea of how data protection will be interpreted and should be applied. We also understand that it's always a moving target with internal organisation changes, external guidance, sanctions, and judgement needing to be understood and addressed.

In this issue, we discuss the AI Act, ChatGPT and large language models, the implications of the €1.2bn fine for Facebook, certification as an enabler to international transfers, and DPC guidance on records of processing activities.

AI Act

The European Parliament has voted on the EU AI Act and has passed it with an overwhelming majority. The draft Act was updated in May. The changes are extensive and include changes to the definition of AI, obligations for deployers and developers of foundational models and generative AI, and the introduction of 6 principles:

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity, non-discrimination and fairness
6. Social and environmental wellbeing

Any organisation that is considering, or is already using, AI should take these principles into account. Doing so will ensure that you do not fall into the prohibited use of AI and be subject to fines of up to €40 million or 7% of global turnover.

Establishing the right level of governance should be the first step for organisations considering adopting AI. It will require a cross-functional team to identify the legal, ethical, technical, and organisational impacts on the organisation and stakeholders.

Key action: Identify activities that meet the definition of AI early and understand the additional obligations imposed by using AI.

ChatGPT and large language models

ChatGPT has become a household name in the last couple of months. The Italian data protection authorities banned the artificial intelligence chatbot in late March, which it lifted when Open AI addressed the Italian supervisors' concerns over consent capture and transparency. Many other large technology companies have also announced their own large language models (LLM), such as Google's BARD and Microsoft's Bing AI.

Organisations that do not control their or their employees' use of tools such as ChatGPT are carrying several risks associated with their use:

- **AI hallucinations:**
  This is where the LLM has not been trained on the up-to-date data set and, as such, attempts to fill in the gaps itself. There are several academic examples where ChatGPT has made up references and published papers. There is a risk that an employee uses an LLM to generate content that is shared with a client or the public and is then found to be incorrect. Naturally, this will have different impacts depending on the role and industry. No one wants a doctor or a lawyer to make such mistakes.
- **Privacy:**
  Many of the LLMs in use learn from the inputted data and the material it generates. If employees use personal or company-sensitive data, then the LLM will use this to learn and may incidentally share it with others. If inputting personal data, do you have a lawful basis for that data sharing?
- **Malicious use and cyber security:**
  Some users have used ChatGPT to produce convincing phishing and social engineering emails. The ability to quickly generate large numbers of realistic attacks will increase the risk of cyber-attack for all businesses.
- **Transparency:**
  You should inform individuals whenever they are interacting with or reading content generated by an AI system. People will interact differently with an AI chatbot or with AI content than with human-generated content. As such, they must be aware of the context. It is worth noting that it is very likely that doing so will be a requirement under the upcoming AI Act.

Given the scale of the use of ChatGPT, the European Data Protection Board (EDPB) has launched a task force to foster cooperation and the exchange of information on possible enforcement actions between the European data protection authorities. At the same time, many regulators and industry bodies are sharing their guidance and whitepapers.

Key action: Ensure to develop and implement a company-wide policy for using generative AI technologies and large language models.

mazars

Record-breaking fine for international transfers

The Data Protection Commission (DPC) has fined Meta a staggering €1.2 bn for breaching article 46 (1), which relates to international transfers based on appropriate safeguards, which it was found that Meta did not have in place. This has been the largest fine to date under the General Data Protection Regulation (GDPR). Meta has been ordered to suspend future transfers of personal data to the US within five months and stop unlawful processing, including the storage of personal data in the US, within six months.

Following an inquiry, the DPC found that Meta was basing the transfer of personal data to the US on the 2021 Standard Contractual Clauses (SCCs), along with several additional supplementary measures. However, it was found that these measures were not adequate. The DPC outlined that the laws in the US do not provide a sufficient level of protection equivalent to that afforded by the GDPR. Neither the 2010 nor 2021 SCCs would effectively address or compensate for the inadequate protection provided to individuals by US law.

More organisations than just Meta fall within the scope of US laws, particularly FISA 702. Therefore, this decision has far-reaching impacts on many businesses that transfer data to the US.

In issue 14, we discussed the proposed EU-US Data Privacy Framework, which is expected to be adopted later this year. The US has committed to providing more safeguards concerning US surveillance activities, strengthening the protection of EU citizens' personal data. We will likely see this new framework being challenged, so organisations would be wise not to wait for its adoption to allow data transfer to the US. Alternative arrangements will need to be put in place until it becomes effective.

Key action: Review your SCCs and Data Transfer Impact Assessments (DTIAs)

Certification as a data transfer tool

Where organisations transfer data outside of the European Economic Area (EEA), an appropriate safeguard must be in place. From the above DPC fine, we have seen that transfers to the US where FISA 702 applies to an organisation, the SSCs and the additional supplementary measures are inadequate.

In February, the European Data Protection Board (EDPB) adopted certification guidelines as a transfer tool. Europrivacy is the first approved GDPR certification scheme. It can be used to replace SCCs and DTIAs as a data transfer mechanism. Data exporters must ensure that their transfers outside of the EEA are compliant and offer the same protection to data subjects as the GDPR. These transfers can be challenging to manage, as seen from the Meta fine. Data exporters should rely on the Europrivacy certification that the data importer achieves to demonstrate their compliance. It provides accredited third-party assurance over the adequacy of safeguards in mitigating risks, thus ensuring the same level of protection for data subjects as enjoyed in the EU.

The benefits of Europrivacy certification for data importers include:

- Improve customer trust and enable a competitive advantage.
- It enables you to identify and reduce legal and financial risks. Certifications are to be acknowledged by supervisors and will lead to a reduction in the scale of any fines.
- Support interaction with supervisory authorities.
- Demonstrate GDPR compliance to internal stakeholders such as senior management and boards through independent third-party assessment.
- It is recognised by all the supervisory authorities across the EEA.
- Enables or prepares the importer for compliance with data protection obligations in their jurisdiction and demonstrates the same.

Key action: Look at alternative transfer mechanisms, such as certification, to support data transfers outside the EEA.

Records of Processing Activity guidance

The DPC 2022 conducted a sweep of some organisations' Records of Processing Activity (RoPA). Article 30 of the GDPR sets out a number of elements required in a RoPA, but there has been no industry standard set as to what additional information should be captured. The RoPA is a key document for data controllers and processors, so ensuring a robust RoPA is in place is very important.

The DPC guidance gives insight into what additional information should be captured in the RoPA outside the article's 30 requirements. Organisations now have a benchmark for their RoPAs to ensure it adequately defines their processing of personal data.

The document identifies key 'do's' and 'don'ts' when completing and maintaining a RoPA. These include:

Do's

- Break it down into each individual business unit or function, e.g. Finance, HR etc.
- Include meaningful and granular information, e.g. retention periods should be specific. Clearly set out what information is mandated under Article 30 and what information is additional.

- Inactive processing activities should be removed from the active processing activities list, but a record of inactive activities should be maintained.
- It should be regularly reviewed as it is a living document.

Don'ts

- If requested, it should not be difficult to produce the RoPA for the DPC. It should be ready to go.
- Out-of-date material should not be recorded in the RoPA, e.g. Privacy Shield.
- More than general information is required. The RoPA should contain specific details, especially when outlining the technical and organisational measures. It is not enough to simply state they are in place; organisations need to outline what exactly is in place.
- Hyperlinking other documents to obtain more information is not sufficient. The RoPA should be a complete and accurate document.

Key action: review your RoPA template and ensure it incorporates guidance provided by the DPC.

Our five-year anniversary data protection survey

- For those that have not yet reviewed the results of our annual data protection survey, which, this year, also includes views from the public, you can access the survey results on our website

Contacts

Liam McKenna, Partner
T: +353 1 449 6454
lmckenna@mazars.ie

David O'Sullivan , Senior Manager
T: +353 1 449 6444
DOSullivan@mazars.ie

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory and tax services. Operating in 95+ countries and territories around the world, we draw on the expertise of more than 47,000 professionals – 30,000+ in Mazars' integrated partnership and 17,000+ via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

www.mazars.ie

mazars