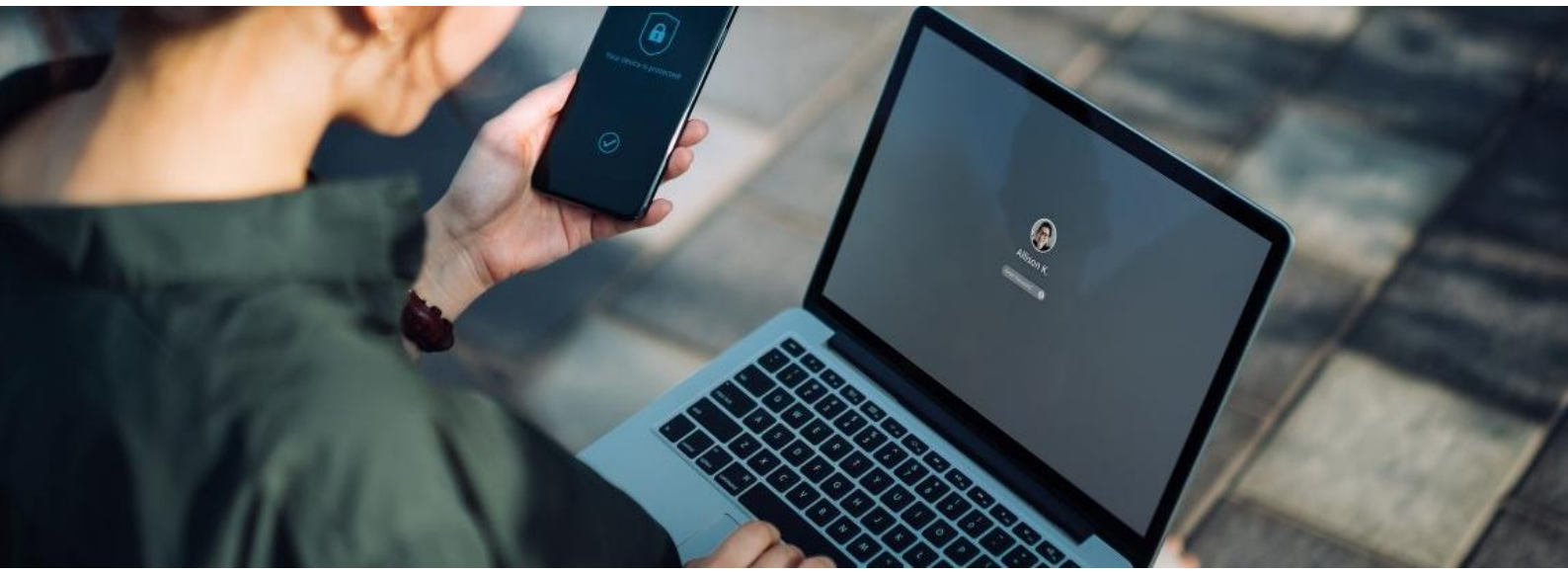

Data protection newsletter

Issue 16

There have been a number of news stories in recent months: TikTok has been fined €345m over its processing of children's personal data; the EU and US have agreed on a new transfer mechanism; a case for non-material damage in Ireland has provided some insight into how courts will calculate damages; our recent Artificial Intelligence survey has provided some interesting findings and a major breach in the PSNI has considerable consequences for employees.

TikTok fined over how it processed children's data

The Data Protection Commission (DPC) adopted its final decision on September 1, 2023, following an inquiry into TikTok Technology Limited's handling of children's personal data.

An investigation was launched into TikTok in September 2021 examining how they processed children's data between 31 July and 31 December 2020. The DPC examined how TikTok processed children's data by looking at the platform's settings for child users, age verification and transparency information for children.

The inquiry found the following points:

- Profile settings for child users were set to public by default, allowing unrestricted access to their content.
- The family pairing feature allowed the child to direct message users aged sixteen and above.
- TikTok failed to provide adequate transparency information to child users.

- TikTok implemented ‘dark patterns’ which encouraged users towards privacy- intrusive options.

The DPC’s decision found that TikTok had infringed a number of GDPR articles, such as failing to implement appropriate technical and organisational measures to ensure data protection by design and default, failing to ensure the safety and security of child users’ personal data, as well as failing on their transparency obligations. The DPC has ordered TikTok to bring their processing into compliance within three months and pay an administrative fine of €345m.

Key action: Companies must ensure when implementing new projects that they consider data protection by design and default.

Ensuring adequate data protection for EU-US transfers

On July 10, 2023, the EU adopted its adequacy decision for the EU-US Data Privacy Framework (DPF). The adequacy decision concludes that under the new framework, the US ensures an adequate level of protection, comparable to that of the European Union for personal data transferred from the EU to US companies. As such, personal data can flow safely from the EU to US companies participating in the framework, without having to put in place additional data protection safeguards such as Standard Contractual Clauses (SCCs) and Data Transfer Impact Assessments (DTIAs).

The DPF is the successor to the Privacy Shield, which faced concerns regarding US surveillance practices and the need for better protection of our personal data. To address these concerns, reforms to US national security and surveillance laws were passed through President Biden’s Executive Order.

Key changes

- Establishment of a new Data Protection Review Court to handle and resolve complaints from individuals relating to access to data by US authorities.
- The introduction of binding safeguards by the DPF introduces strict limitations on US surveillance agencies’ access to EU personal data. It limits access to what is necessary and proportionate for national security purposes.
- Significant limitations on the ability of US authorities to engage in bulk collection of data.
- The requirement for US companies to self-certify.

Benefits of the framework

- Adequate protection of European data.
- Safe and secure data flows.
- Reliable legal basis.
- Competitive digital economy and economic cooperation.
- Safeguarding the data flows that underpin €900bn in cross-border commerce every year.

Where do SCCs stand?

The DPF does not automatically apply to any US company. Banks, airlines, insurers and, in certain cases, telecommunications

providers will not be eligible to join the DPF. Therefore, these industries will need to rely on SCCs, DTIAs and/or other safeguards.

Key action: Check if your vendor is signed up to the DPF. If they are not, continue to rely on SCCs and DTIAs. .

Landmark judgment in non-material damages claim

In July, we saw the first judgment on non-material damages in Ireland. The introduction of the GDPR brought with it the possibility of claiming damages for non-material loss arising from breaches of data subject rights. Although not defined under the GDPR, non-material loss means non-economic loss such as inconvenience and anxiety that may arise from a breach, as opposed to a financial or economic loss.

The case in question involved a plaintiff, who was employed by the defendant company as a supervisor in a factory in Co. Dublin. CCTV footage was shown to other employees of the defendant as part of a training exercise. The training exercise was required in order to address instances of poor food safety practices and to highlight food quality and safety issues at the factory. The plaintiff was identifiable in one of the clips shown, though he was not present at the session. The plaintiff claimed that the use by the defendant of CCTV footage amounted to unlawful processing under the GDPR and as a result of this unlawful processing, he suffered non-material damage. He claimed that he had suffered damage and distress in the form of anxiety, embarrassment, humiliation and loss of sleep due to remarks made by work colleagues about him following the unlawful processing of his personal data.

Factors considered by the court:

1. A mere violation of the GDPR is not sufficient to warrant an award of compensation.
2. There is not a minimum threshold of seriousness required for a claim for non-material damage to exist, but compensation for non-material damage does not cover “mere upset”.
3. There must be a link between the data infringement and the damage claimed.
4. Non-material damage must be genuine and not speculative.
5. Damage must be proved and supporting evidence is strongly desirable.
6. An apology where appropriate may be considered in mitigation of damages.
7. Delay in dealing with a “data breach” by either party is a relevant factor in assessing damages.
8. A claim for legal costs may be affected by these factors
9. Even where non-material damage can be proved and is also not trivial, damages in many cases will probably be modest.

Without supporting medical reports, the court was satisfied that the damage suffered by the claimant "went beyond mere upset". He was awarded €2,000 for non-material damages suffered following the infringement.

Key Action: Consider both material and non-material damages when assessing data breaches.

Four key Insights from our AI survey

We recently conducted a brief survey on Artificial Intelligence (AI) to gauge current sentiments and preparedness for the upcoming AI Act.

Here are four of the key findings:

1. 100% of financial services firms have adopted or are likely to adopt AI in the next three years

Financial services is an area where there has already been strong adoption of AI as it has a number of key use cases such as fraud detection, AML and KYC solutions. However, access to credit is an area of high risk in the AI Act.

2. 70% of firms that are currently using AI or will use it in the next three years do not have an AI policy
3. Nearly two-thirds of those who have heard about the AI Act are waiting for more clarity before progressing with the compliance programme

Combining these two bullet points demonstrates that respondents may not be fully aware of the impact that the AI Act will have on their organisation and the use of the technology. It will be relevant to any system that is available in the EU or where the output impacts EU citizens at the time of coming into force, meaning that any AI being used now will have to be compliant.

4. Respondents felt that AI will have the largest impact on:
    - Operations and services.
    - Sales and marketing.
    - Customer service.

AI use cases at the moment tend to focus on processes that are repetitive in nature. Content generation is another area that is front of mind for many organisations, such as chatbots, copy for marketing material, and recommender/next best action systems in the sales cycle. However, organisations need to be aware of the risk level that these systems might have under the AI Act.

Key action: Establish if your organisation is or will plan to use AI and ensure that you understand the impacts that this will have on the organisation and the compliance requirements associated. Read our article on Responsible Artificial Intelligence & EU AI Act Compliance for more detail or get in touch

mazars

Police Service of Northern Ireland data breach

The Police Service of Northern Ireland (PSNI) was responsible for the accidental disclosure of information relating to all of its 10,000 staff members. The data breach occurred during a response to a Freedom of Information (FOI) request from a member of the public. The request concerned statistical information about the number of officers serving in the PSNI. While fulfilling this request, a clerical error resulted in the source data being published alongside the statistical data on the PSNI's website. The source data contained the surname, initials, roles and departments of every member of the PSNI, including civilian employees.

The existing FOI procedure within the PSNI only requires approval or review from a senior member where the request is seeking sensitive information. In this scenario, statistical information was not deemed to be sensitive, so a check was not carried out, resulting in the error not being caught prior to release. The PSNI has vowed to review this procedure.

Half of the police officers whose personal data was exposed in this leak have been in contact with the Police Federation to enquire about potential damages cases after the data breach. It is possible these police officers may be awarded compensation under the GDPR for non-material damages stemming from the stress and upset related to having their data disclosed publicly. It is difficult to quantify how much this data breach may cost the PSNI, but it's estimated to be in the tens of millions. As a result, the PSNI has suffered severe reputational damage which may result in some of the workforce leaving or reduce the willingness of new recruits to join.

While investigating this breach, it was discovered that a smaller data breach had also occurred a month prior, exposing the details of 200 officers and civilian staff. This breach occurred when a laptop, police radio and documents were stolen from a superintendent's private vehicle.

Key Actions: When information is being provided, ensure non-relevant data is sufficiently redacted or removed. Also, when working remotely, ensure personal data is stored securely and never left unattended.

Contacts

Liam McKenna, Partner
T: +353 (01) 449 6454
lmckenna@mazars.ie

David O'Sullivan, Manager
T: +353 (01) 449 6444
DOSullivan@mazars.ie

Lisa Clarke, Assistant Manager
T: +353 (01) 512 5533
lisa.clarke@mazars.ie

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 42,000 professionals – 26,000 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.
*where permitted under applicable country laws.

www.mazars.ie

mazars