KPMG
Law

Key data privacy considerations for asset managers

kpmglaw.ie

The protection of personal data is governed by the General Data Protection Regulation (GDPR). The GDPR sets out what organisations need to do to comply with the law, and also outlines the rights that all individuals have in respect of their personal information.

GDPR applies to all organisations and is relevant to every organisation which has employees. Whilst the application of GDPR to asset management companies may not be initially obvious, there are a number of key privacy considerations that will be relevant to many asset management companies.

Readiness for dealing with data subject access requests

All individuals have the right to request access to the personal data that an organisation holds about them. This can be particularly relevant where an employee ceases their employment with an organisation. In some cases involving significant amounts of personal data, a data subject access request (DSAR) made under the GDPR can bring the daily operations of a business to a standstill. The scope and complexity of DSARs can vary greatly, and the request can originate from different data subjects such as employees or customers.

Where, for example, an access request comes from an employee with many years of service, it might involve retrieving, reviewing, and redacting high volumes of data. Further, as prescribed by the GDPR, this must be done to an accurate standard and within the statutory deadline of 30 days (extendable to up to 60 additional days).

Failure to comply not only violates regulatory requirements but also exposes businesses to significant legal and financial risks, as well as potential reputational damage. In responding to a request, often an all-hands-on-deck approach is necessary: input from the HR team, the IT team, in-house legal, and senior management may all be required. Proactive data management strategies are therefore essential for minimising the impact of DSARs on business operations.

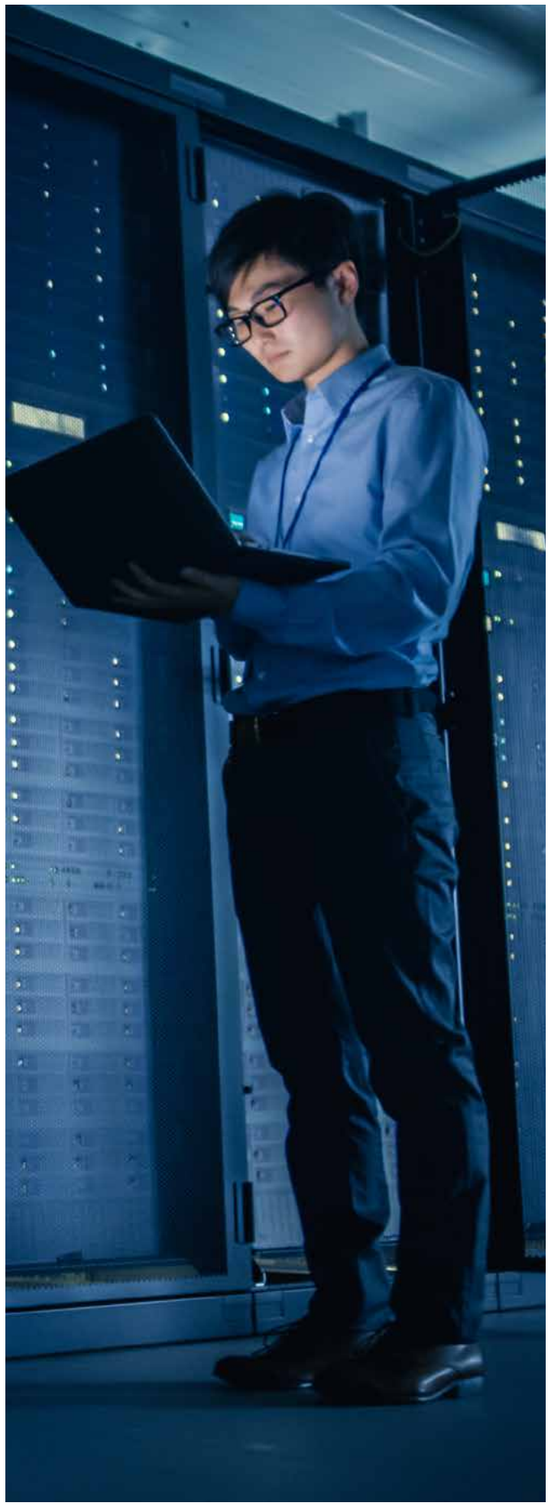
Storing personal data for too long

Many organisations struggle to set up a specific retention period for the personal data they process. It is not uncommon to encounter companies that seem to follow the "just in case" approach, storing their personal data for longer than required and, in certain circumstances, "forever". This approach is not only a breach of the GDPR, but it can also lead to many risks if the data is mishandled.

Retaining data for longer than it is needed carries financial and reputational risks for an organisation. The most obvious risk relates to data breaches and data subject access requests. The more personal information an organisation holds and retains, the greater its exposure and potential liability if that information is disclosed or requested by a data subject.

Excessive data retention also has significant financial impacts for organisations. Storing, managing and maintaining redundant data and systems across an organisation can incur significant costs. By imposing constraints on data retention, organisations will be able to mitigate the risks including unauthorised access, misuse, or breaches of sensitive information.

Adherence to data retention obligations is paramount for organisations to ensure compliance with the GDPR and demonstrate accountability in their data processing activities.



International Data Transfers

A stated aim of the GDPR is the free flow of personal data between EEA Member States. The transfer of personal data to countries outside the EEA however requires special consideration – this is particularly relevant to organisations which operate on a global basis. In essence, a European organisation cannot send an individual's personal data outside of the EEA – it's prohibited, unless one of the exceptions to this general rule applies.

Transfers outside the EEA require:

i. An adequacy decision to be in place in the country the personal data is being transferred to; or

ii. Appropriate safeguards must be in place to secure the transfer of personal data; or

iii. Reliance on a derogation, as set out in the GDPR.

Trust is key when it comes to data transfers internationally. Organisations must map where personal data goes, and if it leaves the EEA, the organisation must illustrate where the personal data travels to and ensure that the correct transfer mechanism is in place to safeguard the individuals' rights.

If there is no adequacy decision, 'appropriate safeguards' may be used to legally transfer personal data internationally. Appropriate safeguards are legal tools designed to ensure recipients of personal data outside the EEA process and protect personal data to the same standard as Europe. All the safeguards require prior approval from a supervisory authority.

Training your staff

For most organisations, data privacy is considered a "top-10" organisational risk. We know that keeping up with all data privacy requirements can be challenging.

Privacy training is one of the key factors to ensure all employees in an organisation understand their obligations under the GDPR and any other applicable privacy regulations. A lack of training increases the risk of human error when employees are dealing with personal data (e.g. failure to safeguard personal data, or sharing data with unauthorised persons). This can lead to breaches and potentially fines and reputational damage.

Training should be tailored to the different roles and responsibilities of each employee to ensure it is relevant and in line with the processing activity. It should also be an ongoing activity to guarantee that all employees, including new joiners and contractors, understand the importance of processing personal data in a compliant manner.

How can KPMG Law help?

Our aim in KPMG Law is to help our clients succeed in their privacy journey. Together with our specialised service providers across KPMG, we can offer invaluable support in navigating the complexities of DSARs, data retention, international data transfers, and training your staff.

We know every business is unique, and our solutions and services are scalable to suit your needs.

Keep an eye on our website for further insights.

Contact us

Emma Ritchie
Head of Data Protection & Privacy
KPMG Law LLP Ireland
e: emma.ritchie@kpmglaw.ie

Jorge Fernandez Revilla
Head of Asset Management
KPMG Ireland
e: jorge.revilla@kpmg.ie

Nicole Walsh
Director
KPMG Law LLP Ireland
e: nicole.walsh@kpmglaw.ie

David McMunn
Director
KPMG Law LLP Ireland
e: david.mcmunn@kpmglaw.ie

Daniela Mejuto Pita
Associate Director
KPMG Law LLP Ireland
e: daniela.mejutopita@kpmglaw.ie

kpmglaw.ie

Produced by: KPMG's Creative Services. Publication Date: May 2024. (10360)