



# General Data Protection Regulation (GDPR) services









A bespoke service catering to all types of alternative investments

## Ensure that you're compliant with the new data protection regulation.

The GDPR outlines Europe's baseline expectations for how EU citizens' personal information should be processed as we continue through the digital revolution. Any organisation that processes the private information of EU citizens is in scope.

From an alternative investment perspective, this involves AIFMs, management companies of funds (including SOPARFIs if they have individual directors and/or employees), and others. Organisations will have to design a GDPR governance strategy that contains the project plan and a roadmap showing which measures will be undertaken to implement this strategy. The entity will also have to nominate a data protection officer whose role is to implement guidelines and structures for data protection.

## Overview of some of the main changes to the regulation

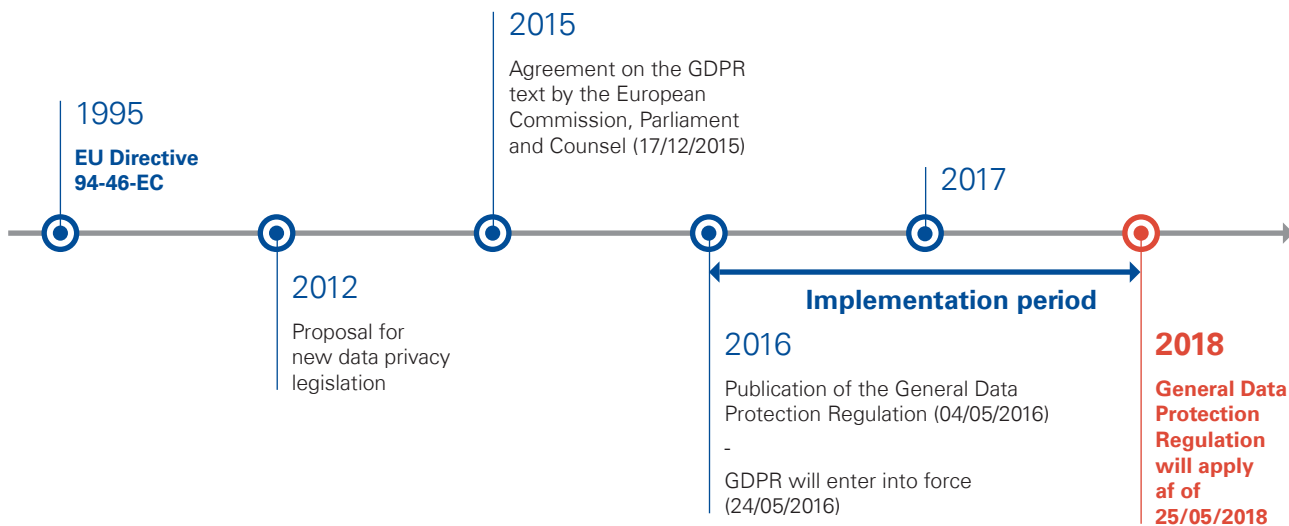
	EU Data Protection Directive	GDPR
 <b>Fines</b>	Fines vary by jurisdiction (e.g. €600k).	A tiered fining structure depending on infringement. Level 1 is 2% of global turnover or €10m (whichever is higher). Level 2 is 4% of global turnover of €20m (whichever is higher).
 <b>Data protection officer (DPO)</b>	Generally no requirement to appoint a DPO.	A DPO is required for "government bodies" and organisations conducting mass surveillance or mass processing of special categories of data.
 <b>Supervisory authorities (SA) enforcement powers</b>	SAs have limited powers under national law.	SAs will be given wide-ranging powers.
 <b>Inventory</b>	No requirement to maintain a personal information inventory.	Generally speaking, organisations will need a personal information inventory.
 <b>Breach notification</b>	Generally there are no obligations to report breaches.	Requirement to report privacy breaches to the regulator within 72 hours and potentially to the data subject too.
 <b>Security</b>	Vague requirement around security (i.e. "adequate level").	Explicit requirements around monitoring, encryption, and anonymisation.

## Detailed features

### Our GDPR service offers you:

- analysis of your organisation's readiness status, including data protection gaps with a data protection assessment
- clear and workable recommendations for improving your overall data protection governance
- advice towards pragmatic, flexible, and scalable data protection management from our proven approach
- a view of industry data protection practices based on real-time benchmarking
- governance, risk management, and compliance (GRC) tools for conducting assessments and for (continuous) monitoring
- cost efficiency by combining this activity with other certifications and assurance activities

### General Data Privacy Regulation - timeline



For contact details please go to: [www.kpmg.lu/alternativeinvestments](http://www.kpmg.lu/alternativeinvestments)

