

The General Data Protection Regulation

Are you prepared?

You have until
25 May 2018 to
be compliant with
the GDPR

Sharp Teeth

Article 83 introduces tough new penalties of fines up to €20 million.

Applies to any organisation

The Regulation is broad and extraterritorial in scope. Applies to you if your organisation touches personal data on EU citizens, even if your organisation does not collect that data itself.



Broader definition of personal data

Now includes identifiers such as social identity, economic, cultural, physical, mental and genetic, and extends consumer rights across access, consent, correction, data portability and erasure.

Evidence

You must not only comply with the six general principles (lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, retention, integrity, and confidentiality), but you must be able to demonstrate you comply with them



Storage limitation

You cannot keep personal data for longer than is necessary for the purpose for which it's processed.



Breach notification

You are to report a notifiable breach to the Information and Data Protection Commissioner (IDPC) within 72 hours of you becoming aware of it.



'Privacy by design'

Data protection is to be built into products and services, rather than being tackled as an afterthought. You need to design compliant policies, procedures and systems at the outset of any product or process development.

Right to be forgotten

Your client can request the deletion or removal of personal data when there is no compelling reason for its continued existence.



Risk is mentioned over
60 times
in the GDPR.

Liabilities on data processors

If you are a data processor, under the GDPR you can now be held directly liable for the protection of personal data. If there is a breach, as a data processor you must notify the company you are working for, that is the controller, 'without undue delay'.



About 63% of all data breaches involve third parties

Too often, third parties are your weakest link. Third parties represent your biggest threat to data security. You need to review your contracts with third parties to make sure these are compliant to the GDPR.