

# Are you ready for **GDPR**?

## Does the GDPR apply to my organisation?



You process personal data by automated means or through a filing system



You're a data controller or processor with an establishment in the EU, and you process the personal data of EU citizens.



You're a data controller or processor based outside of the EU, but process the personal data of EU citizens or monitor behaviour of EU data subjects.

## What do I need to do to achieve compliance?

**#1**

Implement the appropriate technical and organisational measures to ensure and be able to demonstrate that processing is performing in accordance with this Regulation (Article 24)

**#5**

Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, e.g. pseudonymisation, encryption. (Article 32)

**#2**

Implement technical & organisational processes to demonstrate that you have considered and integrated data protection into your processing activities. "Data protection by design". (Article 25)

**#6**

Notify the supervisory authority of a personal data breach without undue delay - not later than 72 hours after having become aware of it. (Article 33)

**#3**

Maintain a record of processing activities. (Article 30)

**#7**

Where a type of processing, in particular using new technology, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall carry out a Data Protection Impact Assessment prior to processing. (Article 35)

**#4**

Cooperate with the supervisory authority in the performance of its tasks. (Article 31)

**#8**

Appoint a Data Protection Officer to inform and advise on GDPR obligations monitor compliance, manage data protection activities, train staff and conduct internal audits and be the first point of contact for supervisory authorities. (Article 37-39)

## What could happen if I don't comply with the regulations?



Issue warnings.



Demand you fix things to a strict deadline



Carry out audits.



Demand you erase data



Tier 1: Up to €10m or 2% of global turnover.



Financial penalties.



Stop data transfers to other countries.



Tier 2: €20m or 4% of global turnover.