ICO Fines

for non-compliance with the GDPR.

In the UK the The Information Commissioner can issue a monetary penalty for failing to comply with Part 3 of the Act. There are two tiers of penalty – the higher maximum and the standard maximum.

Standard Maximum

Fine: Up to €10 million or 2% of turnover for failing to:

* Obtain consent from a child
* Implement data protection by design & default (e.g. failing to design a product that protects the user's privacy)
* Properly apportion risk in a data sharing situation (i.e. where two or more organisations – including different companies in the same group - use the same data, they must all properly manage the risk between one another via a data sharing arrangement)
* Appoint a DPO or Representative when required to do so
* Comply with requirements concerning the appointment of data processors
* Maintain proper records of data processing
* Co-operate with supervisory authority
* Implement appropriate security measures
* Notify personal data breaches to supervisory authority and/or data subjects when required to do so
* Conduct a DPIA and/or address any risks identified by a DPIA

Higher Maximum

Fine: Up to €20 million or 4% of turnover for failing to:

* Comply with data protection principles
* Fulfil requirements for obtaining valid consent
* Fulfil requirements for processing special category personal data
* Fulfil obligations re data subject's rights
* Transfer personal data to third country in accordance with rules
* Comply with any Member State obligations re specific processing situations
* Comply with order of/co-operate with a supervising authority
* 'Bring processing operations within GDPR'
* Communicate personal data breach to supervising authority/data subjects

Want more detail?

For the relevant provisions of the act go to to the ICO website <<here>>

norm.

***Reassuringly dull cyber security**