103 Penalties

The Information Commissioner's Office (ICO) could levy penalties with an upper limit of €20 million or 4% or annual global turnover – whichever is higher. So, for many businesses, non-compliance could mean insolvency or even closure.

Article 83 provides that a Member State's supervisory authority (in the case of the UK, the ICO) is empowered to impose administrative fines on data controllers and data processors that shall "in each individual case be effective, proportionate and dissuasive".

The decision to impose a fine and the level of the fine shall be based on consideration of the circumstances of the case, including "the nature, gravity and duration of infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered" the "intention or negligent character of the infringement" and "any action taken by the controller or processor to mitigate the damage suffered by the data subjects".

The topic that dominates much of the discussion about GDPR is the level of fines that can be imposed for a breach of the regulations. This is hardly surprising when the magnitude of the fines is considered. This certainly makes compelling reason for a business to comply with the regulation.

Article 83 makes provision for infringements to be subject to a two-tiered system of administrative fines depending upon the nature of the breach.

Tier 1

Fines of up to €10,000,000 or in the case of an undertaking up to 2% of total annual global turnover whichever is higher may be imposed for breaches which include:

- Obtaining consent for processing children's data (Article 8);
- Implementing technical and organisational measures which ensure data protection by design and by default (Article 25);

Tier 2

Maintaining written records (Article 30).

Fines of up to €20,000,000 or 4% of global turnover whichever is higher may be imposed for breaches of provisions which include:

- The basic principles of processing (Articles 5, 6, 7 and 9);
- The provision of data subject's rights (Articles 12-22).

Article 84 also provides for Member States to impose penalties for breaches not covered by the two-tier fines, however, the Commission must be notified by 25 May 2018 about these penalties.

The following table itemises the penalty tier applicable to a breach of each respective Article in the Regulation.

The Fining Structure

GDPR has been designed to ensure organisations take the appropriate measures to protect personal data against the risks of loss. Whilst the fines outlined above represent the maximum financial penalties, for organisations that fail to meet the requirements the GDPR the supervising authority is can take a range of actions including:

- Issue warnings;
- Issue reprimands;
- Order compliance with Data Subjects requests;
- Communicate the Personal Data breach directly to the Data Subject.

In addition to the above the supervising authority have the power to impose administrative fines that will in each case be effective, proportionate, and dissuasive.

The following table itemises what articles of the GDPR relate to a tier 1 or tier 2 fine.

Article	Description	Tier 1	Tier 2
5	Principles relating to processing of personal data		☐
6	Lawfulness of processing		☐
7	Conditions for consent		☐
8	Conditions applicable to child's consent in relation to information society services	☐	
9	Processing of special categories of personal data		☐
11	Processing which does not require identification	☐	
12	Transparent information, communication and modalities for the exercise of the rights of the data subject		☐
13	Information to be provided where personal data are collected from the data subject		☐
14	Information to be provided where personal data have not been obtained from the data subject		☐
15	Right of access by the data subject		☐
16	Right to rectification		☐
17	Right to erasure ('right to be forgotten')		☐
18	Right to restriction of processing		☐
19	Notification obligation regarding rectification or erasure of personal data or restriction of processing		☐
20	Right to data portability		☐
21	Right to object		☐
22	Automated individual decision-making, including profiling		☐
25	Data protection by design and by default	☐	
26	Joint controllers	☐	
27	Representatives of controllers or processors not established in the Union	☐	
28	Processor	☐	
29	Processing under the authority of the controller or processor	☐	
30	Records of processing activities	☐	
31	Cooperation with the supervisory authority	☐	
32	Security of processing	☐	
33	Notification of a personal data breach to the supervisory authority	☐	

Article	Description	Tier 1	Tier 2
34	Communication of a personal data breach to the data subject	☐	
35	Data protection impact assessment	☐	
36	Prior consultation	☐	
37	Designation of the data protection officer	☐	
38	Position of the data protection officer	☐	
39	Tasks of the data protection officer	☐	
41(4)	Monitoring of approved codes of conduct	☐	
42	Certification	☐	
43	Certification	☐	
44	General principle for transfers		☐
45	Transfers on the basis of an adequacy decision		☐
46	Transfers subject to appropriate safeguards		☐
47	Binding corporate rules		☐
48	Transfers or disclosures not authorised by Union law		☐
49	Derogations for specific situations		☐
58(1, 2)	Powers		☐
85	Processing and freedom of expression and information		☐
86	Processing and public access to official documents		☐
87	Processing of the national identification number		☐
88	Processing in the context of employment		☐
89	Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes		☐
90	Obligations of secrecy		☐
91	Existing data protection rules of churches and religious associations		☐

Determining Fines

The GDPR is clear that to ensure any fine is proportionate, a range of factors will be assessed by supervisory authorities when investigating organisations that breach the GDPR.

The nature, gravity, duration and the character of an infringement will be of key importance. Actions taken by the Controller or Processor to mitigate any damage suffered by data subjects, along with the degree of responsibility for the technical and organisational measures implemented by them to prevent the breach occurring will be taken into consideration.

The Regulation also allows the Supervising Authority to consider factors such as infringement history including previous correction notices, level of co-operation, the categories of personal data affected, the way the breach became known and how it was reported, the level of adherence to approved codes of conduct or certification mechanisms and any other aggravating or mitigating factors.

With fines under GDPR being 79 higher than previously under Data Protection Act 1998 (DPA) it is clear where this is heading. Prior to GDPR coming into force the organisation that was breached would be fined under DPA, however with GDPR there is liability beyond Data Controllers so the ICO will follow the data trail to determine where it was originally collected. If the data has been passed between organisations the ICO could fine them as well as the organisation where the breach occurred.

Minimising Fines

An organisation able to demonstrate they have a positive approach to ensuring security, with a range of technical, management and operational controls will receive a lower fine than an organisation that takes no measures, or blatantly disregards its obligations under GDPR. The ICO has made it clear that in terms of incident reporting, organisations that proactively report breaches will be given more credit than organisations who do not report a breach that is then discovered by a 3rd party.

The True Cost of a Data Breach

The fines levied by the supervisory authority by no means represent the full financial impact of a data breach.

TalkTalk

In 2013 TalkTalk suffered a data breach and whilst they were fined £400,000 for the breach which was a record at the time, the reputational impact was far greater. TalkTalk's shares plummeted 10% within two days of news of the breach being broadcast. A year later it is understood the breach the reputational cost to the company reached £42,000,000 and having lost 90,000 customers.

Yahoo

In September 2016, Yahoo revealed that it had been the victim of a cyber-attack in 2014 that put 500m user accounts at risk. It has subsequently been announced by the company that every one of the three billion accounts were affected by the data theft, making it the largest data breach in history.

The news came at the worst possible time for Yahoo. The company was still recovering from a drop-in share price that occurred in 2015, but it was also in buyout negotiations with Verizon.

The massive loss of data and mishandling of both breaches by senior executives resulted in CEO Marissa Meyer losing her annual bonus and stock award, while Verizon purchased Yahoo's internet business for the low price of $4.48bn. An enormous $350m less than had been agreed prior to news of the breach.

That is by no means the end of the story for Yahoo. 43 consumer class-action lawsuits have been filed against the company as of May 2017.

Summary

Fine	The ICO as the UK Supervisory Authority can impose a fine of up to €20 million or 4% of global turnover for non-compliance with GDPR. The ICO demonstrated with the TalkTalk case that fines may approach the upper limits available to them. Organisations can significantly reduce the likelihood of receiving a maximum fine by implementing information security best practices and an ethos of protecting personal information.

Compensation	Individuals affected by a data breach may could make a legal claim for damages suffered.
Reputation	Damage to the reputation of your business resulting from a loss of consumer trust. Reputational damage to a large business can be measured in many millions of pounds, however, over 80% of SMEs who suffered a serious cyber security incident will cease trading within two years according to the Federation of Small Business.

Glossary

DPA	Data Protection Act 1998, the statute that previously governed the processing of personal data in the UK. The Data Protection Act 2018 gained Royal Ascent and came into force to coincide with GDPR.
GDPR	General Data Protection Regulation, the EU law that came into force in the UK on 25 May 2018.
Data controller	the person or business who determines the purposes for which personal data will be processed and the manner in which it will be processed.
Data processor	a person or organisation who processes the data on behalf of the controller
Commissioner	the Information Commissioner
ICO	Information Commissioner's Office
Undertaking:	an entity engaged in economic activity