ONTIER

PRIVACY AND DATA PROTECTION INTERNATIONAL TEAM

07th November 2017
#18

Index

REMEDIES, LIABILITY AND PENALTIES

One of the biggest changes to data protection law by the GDPR causing some concern to businesses are the changes to the remedies, liabilities and, in particular, penalties. All businesses will be affected by the changes coming into force under the GDPR as it aims to harmonise enforcement of data protection law throughout and across the EU.

Current situation

a) Remedies

Under the Directive, data subjects have the right to legal remedies if there is a breach of their data protection rights. The rights held by the data subject differ between Member States as the Directive is silent on this other than the high-level concepts of broad investigative and enforcement powers, leaving it to individual Member States to create their own procedure. Supervisory authorities do have the minimum powers of investigation, intervention (for example, to order the blocking, deletion or destruction of data) and can commence legal proceedings against Data Controllers (subject to the implementation of such power under the national law of the relevant Member State).

Furthermore, the Directive does not state the circumstances as to when a supervisory authority may take enforcement actions and therefore this differs between Member States. For example, in Spain, the supervisory authority is required by law to investigate all complaints received, but this is not the case in most other Member States.

b) Liability

A data subject can hold a Data Controller liable for breaching the way in which personal data should be processed under the Directive. Data subjects will also be able to recover compensation for such a breach from the Data Controller but not from a Data Processor.

c) Penalties

Data subjects can claim compensation against Data Controllers for a breach of data protection laws but the Directive does not specify how much a Data Controller can be fined, leaving it to each Member State to set their own rules on this. Financial penalties under national law for each Member State therefore varies and supervisory authorities generally have a wide discretion as to the circumstances in which to issue a penalty but they are comparatively low. In the UK for example, the maximum fine that has can be imposed against a Data Controller is £500,000.

What's new?

a) Remedies

The rights of data subjects have been slightly strengthened under the Regulation. Data subjects now have a specific right to lodge a complaint with the supervisory authority when their personal data is processed in a way that is not compliant with the GDPR, and the supervisory authority must inform data subjects of the progress and outcome of the complaint made. The Regulation also gives data subjects the right of judicial remedy against a supervisory authority in relation to certain acts and decisions concerning them, or any failure by them to deal with, or respond to a complaint within three months.

Decisions made by the supervisory authority can be appealed by businesses and data subjects. Proceedings against a supervisory authority or public authority must be brought in the Member State in which the supervisory authority or public body is established and proceedings against a Data Controller or Data Processor may be brought in the Member State in which they have an establishment or where the data subject resides. The GDPR

also clarifies the requirements regarding claims brought by third parties on behalf of data subjects.

Supervisory authorities will be given greater power to enforce compliance including the power to compel a Data Controller or Data Processor to provide information and the ability to impose a ban on processing personal data.

b) Liability

Under Article 82 of the GDPR, both Data Controllers and Data Processors can now be found liable under the GDPR. A Data Controller can be liable for damages caused by processing that infringes the Regulation. A Data Processor is only liable to a data subject where it breaches the obligations of the Regulation directed at Data Processors or where it acts outside of the lawful instructions of the Data Controller. In order to ensure effective compensation for the data subject, both the Data Controller and the Data Processor, who are involved in the same processing and where they are responsible for any damage caused (being both pecuniary and non-pecuniary losses) by the processing, will be held liable for the entire damage caused to the data subject (Article 82(4)). Where a Data Controller has paid the full compensation to a data subject, it may bring proceedings against any joint Data Controllers and/or Data Processors to recover their portion of the damages paid. Data Controllers and Data Processors would not be liable however, if they can prove that they were not in any way responsible for the damage caused to the data subject. It is unclear whether force majeure events will exempt Data Controllers and Data Processors from liability as there is no mention of such in the GDPR unlike the Directive.

c) Penalties

In order to strengthen the enforcement of the rules of the GDPR, penalties including administrative fines would be imposed on Data controllers and Data Processors in addition to, or instead of any appropriate measures imposed by a supervisory authority for any infringement of the Regulation. The administrative fines that can be imposed under the GDPR are now considerably higher than what was possible under the Directive. Article 83 of the GDPR states that any fine imposed by a supervisory authority shall, in each individual case, be “effective, proportionate and dissuasive” (Article 83(1)).

There are two different levels of administrative fines:

a) infringements of the basic principles of processing including infringement relating to conditions for consent, data subjects’ rights, transfer of personal data to a recipient in a third country, infringement of obligations under Member State laws, and non- compliance with an order by the supervisory authority are subject to fines up to the greater of €20 million or 4% of annual worldwide turnover for the previous financial year of the Data Controller or Data Processor; and

b) infringements of other provisions of the GDPR including the failure to obtain parental consent on personal data about a child will be subject to fines up to the greater of €10

million or 2% annual worldwide turnover for the previous financial year of the Data Controller or Data Processor.

When deciding whether to impose an administrative fine and deciding on the amount, under Article 83(2), supervisory authorities should take into account of the following:

a) the nature, gravity and duration of the infringement;

b) the intentional or negligent character of the infringement;

c) any action taken by the Data Controller or Data Processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility of the Data Controller or Data Processor;

e) any relevant previous infringements by the Data Controller or Data Processor;

f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

g) the categories of personal data affected by the infringement;

h) the manner in which the infringement became known to the supervisory authority;

i) where measures have previously been ordered against the Data Controller or Data Processor concerned with regard to the same subject-matter, compliance with those measures;

j) adherence to approved codes of conduct or approved certification mechanisms; and

k) any other aggravating or mitigating factor.

What to do to adapt?

This area is arguably the biggest and most significant change in the GDPR for the purposes of data protection. Where many businesses would have previously regarded non-compliance with EU data protection laws as a low risk issue/low priority under the Directive, it is now extremely important that compliance with GDPR is given a high priority as a result of:

(i) the potential penalties that may be imposed;

(ii) the greater enforcement power afforded to supervisory authorities; and

(iii) the grounds available for seeking judicial remedies under the Regulation. It should also be noted that the remedies, liabilities and penalties under the GDPR will apply to all organisations and not just to a particular sector or size of organisations.

Businesses must therefore review and identify any areas of its processing activities that are not currently compliant with the GDPR and take steps to mitigate such non-compliance as soon as possible. They should review their existing arrangements with any joint Data

Controllers, suppliers and customers, including assessing any contract liability limitations and exclusions and determine whether they are sufficient to protect their needs or whether they need to be renegotiated.

Businesses should also address the GDPR and establish the correct procedures in order to detect, report and investigate personal data breaches within their organisation. Ensuring such a procedure is in place should limit the risk of damage to the data subject(s) and hence reduce the risk of incurring penalties. In doing this, businesses will need to assess the types of data that falls within the notification requirement. For larger businesses, developing strict but easy to follow policies and procedures for managing data breaches from now should ensure compliance and employee knowledge of the requirements in good time before the GDPR is in force. This will make the transition to GDPR compliance far smoother and allow time to correct any issues with initial policies / procedures.

Finally, and if necessary, businesses should review any insurance arrangement it has in relation to data protection and check if the cover is sufficient to cover any potential penalties under the GDPR.

A Practical Example:

A large number of customers of an internet service provider company were complaining about receiving spam emails and calls from people who pretended to provide technical support and were able to quote their account numbers and addresses. Following an investigation by the supervisory authority, it transpires that due to technical weaknesses in the company's systems in protecting personal data, thousands of customers' details, including their bank details, were stolen with ease by hackers.

If the supervisory authorities determines that the company failed to implement the appropriate cyber security measures to protect the data thereby allowing hackers to access such information with ease, it could fine the company up to the maximum penalty of €20 million or 4% of their annual global turnover (whichever is higher) depending on the seriousness of the breach.

The company may also be liable to damages or loss suffered by their customers affected by the breach.

Practical example:

A large number of customers of an internet service provider company were complaining about receiving spam emails and calls from people who pretended to provide technical support and were able to quote their account numbers and addresses. Following an investigation by the supervisory authority, it transpires that due to technical weaknesses in the company's systems in protecting personal data, thousands of customers' details, including their bank details, were stolen with ease by hackers.

If the supervisory authorities determines that the company failed to implement the appropriate cyber security measures to protect the data thereby allowing hackers to access such information with ease, it could fine the company up to the maximum penalty of €20

million or 4% of their annual global turnover (whichever is higher) depending on the seriousness of the breach.

The company may also be liable to damages or loss suffered by their customers affected by the breach.

TEAM

Joaquin Muñoz Rodríguez (Spain)
Pablo Uslé Presmanes (Spain)

Derek Stinson (UK)
Paula Enríquez (UK)

Ana Rocha (Portugal)
Joana Cunha de Miranda (Portugal)

Luca Pardo (Italy)
Giulio Ciompi (Italy)

Read more:

about us

Share on:

Linkedin Twitter

Subscribe:

our Newsletters

Contact us:

Website | LinkedIn

Rua Vitor Cordon Nº 10A - 1249 - 202 Lisboa | Portugal
Tel. (+351) 213 223 590 / Fax (+351) 213 223 599

Rua Pedro Homem de Melo, n.º 55, 8º piso - 4150 - 599 Porto | Portugal
Tel. (+351) 223 190 888 / Fax (+351) 220 924 945

PORTUGAL / **SPAIN** / **U.K** / BOLIVIA / / BRAZIL / CHILE / CHINA / COLOMBIA

USA / **ITALY** / MEXICO / PERU / VENEZUELA
