DILLON EUSTACE

'Massively expanded' enforcement toolkit and 'potentially colossal' fines on the way for data administrators

When the General Data Protection Regulation (EU 2016/679) comes into force on 25 May next the Office of the Data Protection Commissioner will be able to impose for the first time large administrative fines for data protection breaches. Muireann Reedy explains why it will pay to be compliant with the GDPR.

In May 2017, the Irish Government published the General Scheme of Data Protection Bill. When finalised and enacted it will give effect to various discretionary measures set out in the GDPR, as well as transposing the Police and Criminal Justice Authorities Directive (EU 2016/680). As a result of the GDPR, the Data Protection Commission, which will replace the Data Protection Commissioner, will have the power to levy administrative fines for the first time. The DPC will be the supervisory authority in Ireland responsible for, among other things, monitoring and enforcing compliance with the GDPR.

"For less serious breaches, the fine can be up to the higher of €10 million or, in respect of an undertaking, 2 per cent of its total worldwide annual turnover for the preceding financial year. But these figures can be doubled for more serious breaches."

The GDPR sets out two tiers of administrative fines, depending on which underlying provision of the GDPR has been breached. For less serious breaches, the fine can be up to the higher of €10 million or, in respect of an undertaking, 2 per cent of its total worldwide annual turnover for the preceding financial year. But these figures can be doubled for more serious breaches.

It remains to be seen if subsidiaries will be considered separately to the parent company when determining the scope of the term 'undertaking'. If they are included within this definition, entities could be looking at potentially colossal fines.

Breaches falling within the lower fine bracket include: using a data processor without obtaining sufficient guarantees that it will implement appropriate technical and organisational measures,

Muireann Reedy

failing to co-operate with a supervising authority and failing to notify a supervisory authority of a breach within the requisite time period.

Breaches which may trigger a higher level of fine include: processing personal data in a manner which is not lawful, fair and transparent; processing data which is not relevant and limited; failing to ensure that personal data is accurate and where necessary, up to date; and failing to demonstrate to the supervisory authority that the data subject has consented to processing his/her personal data.

The GDPR requires supervisory authorities to ensure that in each case the administrative fine is 'effective, proportionate and dissuasive'.

The GDPR requires various matters to be considered by a supervisory authority before deciding whether to impose an administrative fine. These include the nature, gravity and duration of the infringement, the number of data subjects affected, the degree of co-operation with the supervisory authority, any relevant previous infringements and any other aggravating or mitigating factors, such as financial benefits gained or losses avoided as a result of the breach.

The GDPR provides for the establishment of a European Data Protection Board which among other things, will be tasked with drawing up guidelines for supervisory authorities on the setting of administrative fines and corrective powers, with the aim of ensuring consistent application of the GDPR.

Supervisory authorities also have 'corrective powers' which may be used either on a stand-alone basis or in addition to the levying of an administrative fine.

"The explanatory notes within the Bill state that the corrective powers set out in the GDPR are potentially far reaching and that the administrative fines are 'potentially massive'. They state, therefore, that 'the foregoing points towards a need for robust procedural and due process safeguards'"

These powers include issuing a reprimand to a controller or processor when they have committed a data breach, ordering the controller or processor to inform the data subject of the data breach, imposing a temporary or definitive ban on data processing and ordering the rectification or erasure of personal data.

The explanatory notes within the Bill state that the corrective powers set out in the GDPR are potentially far reaching and that the administrative fines are 'potentially massive'. They state, therefore, that 'the foregoing points towards a need for robust procedural and due process safeguards'.

In practice the Bill envisages that the imposition of an administrative fine will be preceded by an investigation by an authorised officer of the DPC, with a variety of compulsory information

gathering powers at his/her disposal, which will culminate in an Investigation Report and potentially an oral hearing. The data controller or processor will be given an opportunity to comment on the matter(s) being investigated at various stages.

"The Bill goes further than the GDPR and provides that the DPC 'shall publish…in such form and manner…as it thinks fit…' details of administrative fines and corrective powers."

Any fine imposed as a result of an investigation must be confirmed by the Circuit Court, even if the fine is not contested. If the data controller or processor appeals the fine, the appeal will be heard by the Circuit Court if the fine is less than €75,000 or the High Court if it is higher.

Importantly from a reputational perspective, the Bill goes further than the GDPR and provides that the DPC 'shall publish…in such form and manner…as it thinks fit…' details of administrative fines and corrective powers.

Depending on the content of these publications (i.e. whether they name the relevant controller or processor) and the format which they take, this could cause significant reputational damage for an entity.

It is noteworthy that under the GDPR a data subject will have a right to seek compensation in the Courts if he or she believes his or her data protection rights have been infringed. A data controller or processor may find, therefore, that in addition to any administrative fine imposed by the DPC, they could also be subject to a compensation order by the Courts.

The Data Protection Commissioner, Helen Dixon, is clearly happy with the new powers. Speaking at the Data Summit Dublin 2017 last June she said: '…as a data protection authority supervising the world's largest internet companies from Dublin, we are very pleased to see our enforcement toolkit being expanded massively by the EU.' Her office's budget has been quadrupled since 2014, its staff number has trebled (and is expected to increase to around 100 by the end of this year) and it has hired specialists in the legal, technical, investigative and communications fields.

"It is noteworthy that under the GDPR a data subject will have a right to seek compensation in the Courts if he or she believes his or her data protection rights have been infringed.

It is clear from all this that it is expecting an increased workload as a result of the GDPR and is planning on exercising its supervisory muscles. Data controllers and processors should beware!

Muireann Reedy is a Senior Associate in Dillon Eustace's Regulatory Investigations Unit.