July 2017

GDPR: Administrative Sanctions

Introduction

With less than a year to the introduction of the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**") and given its far reaching effect on those who process personal data, it is important to consider the potential consequences for data controllers and data processors. The GDPR envisages both administrative sanctions by the relevant supervisory authority and judicial remedies which can be brought side by side. Where a data subject alleges that there has been a breach of the GDPR which has caused the data subject damage, that is either material or non-material, he or she can lodge a complaint with the relevant supervisory authority within a member state. There is also a right to seek compensation from the data controller or data processor for the damage suffered. For a fuller discussion on judicial remedies see our next article.

Supervisory Authority

The GDPR provides for the establishment of a supervisory authority in each individual member state which has responsibility for, amongst other things, monitoring and enforcing the application of the GDPR. Each supervisory authority has investigative and corrective powers which it can apply if a data controller or data processor infringes the GDPR. Along with investigating a complaint by a data subject, a supervisory authority can also initiate an investigation of its own accord to establish whether a data controller or data processor is abiding by the GDPR. If, following investigation, it is found that a data controller or data processor is in breach of a requirement of the GDPR, the supervisory authority has the power to use its corrective powers to impose a sanction.

For further information on any of the issues discussed in this article please contact:

Peter Bredin
Partner Litigation
DD: + 353 (0)1 674 1013
peter.bredin@dilloneustace.ie

John O'Riordan
Partner Litigation
DD: + 353 (0)1 673 1792
john.oriordan@dilloneustace.ie

Alan Quigley
Litigation Solicitor
DD: + 353 (0)1 673 1899
alan.quigley@dilloneustace.ie

Ireland's Data Protection Bill

In Ireland, the Government published the General Scheme of Data Protection Bill (the "**Bill**") in May 2017 which, although not yet enacted and is subject to change, is the legislation proposed to transpose the GDPR into Irish law.

Investigative Powers

Article 58 of the GDPR sets out in broad terms the investigative powers of the supervisory authority. These powers include requiring a data controller or data processor to provide whatever information the supervisory authority deems necessary to carry out its supervisory functions under the GDPR. In practice, the manner in which the supervisory authority implements its investigative powers is left to each member state.

The Bill elaborates on the investigative powers set out in Article 58 of the GDPR and provides that, in conducting an investigation, regard may be had to any information, records or documents provided, any statement or admission made by any person, or any submissions made. If it is believed that an oral hearing will assist an investigation, such a hearing may be conducted by the Data Protection Commission (the "**Commission**") which, under the Bill, is to be the relevant supervisory authority in Ireland.

An 'information notice' may be served on a data controller / data processor which requires the furnishing of certain information as specified in the notice and failure to comply with an information notice may lead to criminal prosecution.

Once an investigation has been carried out, a report is prepared setting out the findings of the investigation. The Commission considers the findings and makes a determination as to whether there has been a breach of the GDPR. Should it be determined that there has been a breach of the GDPR, the Commission may proceed to use its corrective powers as set out in Article 58(2) of the GDPR.

Corrective Powers

The supervisory authority can impose any or all of the sanctions provided for in the GDPR (considered below). The potential level of administrative fine that may be imposed is of particular note. The GDPR goes into detail on the conditions for implementing an administrative fine and provides that any fine imposed is to be effective, proportionate and dissuasive. It remains to be seen how this will be interpreted.

Fines

There are a number of factors that are to be taken into account by supervisory authorities when deciding the level of fine to be imposed. It is important for data controllers and data processors to review the factors and establish what steps can be taken to limit the level of any possible fine. The implementation of appropriate technical and organisational measures such as ensuring that the processing of personal data is done using encryption and pseudonymisation[1], where possible, and adherence to a code of conduct are examples of

[1] Article 5 of the GDPR defines pseudonymisation as '*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such*

steps that can be taken to potentially reduce the level of fine.

In terms of the quantum of a fine, it will depend on which Article of the GDPR has been breached as the GDPR provides for two grades of fines that may be imposed. Article 83(4) provides for a maximum fine of up to €10,000,000 or up to 2% of the total worldwide annual turnover in the preceding year where the breaching party is an undertaking. The reference to worldwide revenue is of note and it remains to be seen whether subsidiaries will be considered separate to the parent company for the purposes of determining the scope of the meaning of an undertaking. Breaches to which a fine under Article 83(4) may be imposed include:

- processing data where a data subject is identified but their identification is not required;
- failing to implement appropriate technical and organisational measures;
- using a data processor without obtaining sufficient guarantees that it will implement appropriate technical and organisational measures;
- a processor engaging another processor without specific or general written authorisation of the controller;
- a processor processing data outside of the instructions provided by the controller;
- the controller failing to maintain a record of processing activities under its responsibility;
- failing to cooperate with a supervising authority;
- failing to notify a supervisory authority of a breach within the requisite time period;
- failing to notify a data subject, without undue delay, of a breach which is likely to result in a high risk to the data subject's rights; and
- failing to designate a data protection officer where one is required.

Subsection 5 of Article 83 of the GDPR provides for a higher maximum fine and so a breach of an Article to which this applies would be considered a more serious breach of the GDPR. The maximum fine under subsection 5 is €20,000,000 or, where the breaching party is an undertaking, up to 4% of the total worldwide annual turnover in the preceding year. As regards the breaches to which subsection 5 would apply, these would include, amongst others:

- processing personal data in a manner which is not lawful, fair and transparent;
- collecting personal data for a purpose which is not specified, explicit and legitimate purpose;
- processing data which is not relevant and limited;
- failing to take every reasonable step to ensure personal data is accurate and, where necessary, up to date;
- failing to demonstrate to the supervisory authority that the data subject has consented to processing his/her personal data;
- processing the special categories of personal data referred to in Article 9, unless such processing is in accordance with Article 9;
- failing to adhere to a request by a data subject for information held relating to his/her personal data;

---

additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.

- failing to adhere to a request from a data subject to rectify inaccurate personal data; and
- failing to adhere to a request from a data subject to erase his/her personal data.

Other Sanctions

It is important to be aware that there are other sanctions which can be imposed in conjunction with an administrative fine. The Commission has the power to order a data controller or data processor to communicate a personal data breach to the data subject. Such an order could have repercussions given the right a data subject has under the GDPR to compensation for material and non-material damage suffered as a result of an infringement of their rights.

A further issue for a controller or processor is that each supervisory authority shall draw up an annual report which will include infringements notified to it and the types of measures taken under its corrective powers. In Ireland, the proposed legislation has expanded on this and it sets out that the Commission has the power to publish particulars of any exercise of its corrective powers including the imposition of an administrative fine. This could be of serious consequence for some data controllers and data processors who may suffer reputational damage as a result of such publication.

Conclusion

The GDPR has the potential to have huge cost implications for business. The first step should always be prevention of any potential breach of the GDPR occurring in the first instance. Businesses need to be aware of the potential actions that may arise and the potential sanctions which may be imposed. From an administrative sanction point of view, attention should be paid to the factors that are to be considered by a supervisory authority when imposing an administrative fine. Policies and procedures should be put in place, not simply in an effort to prevent a breach occurring, but also to limit the potential exposure should a breach occur.

DILLON EUSTACE

Dublin
33 Sir John Rogerson's Quay, Dublin 2, Ireland. Tel: +353 1 667 0022 Fax: +353 1 667 0042.

Cayman Islands
Landmark Square, West Bay Road, PO Box 775, Grand Cayman KY1-9006, Cayman Islands. Tel: +1 345 949 0022 Fax: +1 345 945 0042.

New York
245 Park Avenue, 39th Floor, New York, NY 10167, U.S.A. Tel: +1 212 792 4166 Fax: +1 212 792 4167.

Tokyo
12th Floor, Yurakucho Itocia Building, 2-7-1 Yurakucho, Chiyoda-ku, Tokyo 100-0006, Japan. Tel: +813 6860 4885 Fax: +813 6860 4501.