LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

Investigative Powers of the Data Protection Commissioner

by **Abigail Butler**

Investigative Powers of the Data Protection Commissioner

18th September 2017 | by Abigail Butler

Under section 10 of the Data Protection Acts 1988 and 2003, the Data Protection Commissioner (DPC) must investigate any complaints which he receives from individuals who feel that personal information about them is not being treated in accordance with the Act, unless it is of the opinion that such complaints are "frivolous or vexatious". With regard to complaints of breaches of the Data Protection Acts, the Commissioner is obliged to seek an amicable resolution of the complaint in the first instance. Where this cannot be achieved, she may make a Decision on the complaint. The Commissioner's Decision can be appealed to the Circuit Court.

The Commissioner may also launch investigations on her own initiative, where she is of the opinion that there might be a breach of the Act, or where she considers it appropriate in order to ensure compliance with the Acts. In practice, the investigations to ensure compliance, usually, take the form of privacy audits. The data controller, normally, gets advance notice and the aim of the privacy audit is to assist in improving data protection practices. It is only in the event of serious breaches being discovered or failure of the data controller to implement recommendations that further sanctions would be considered.

The Office of the Data Protection Commissioner (ODPC) investigated 1,479 individual complaints in 2016.

In relation to data breaches, at present, outside the electronic communications industry, there is no legally binding obligation under Irish law to notify data breaches to either the Data Protection Commissioner or to any impacted individuals. The Data Protection Commissioner has, however, published a Code of Practice for Data Security Breaches (the Code), in the expectation that the Code will be followed.

Paragraph 9 of the Code of Practice states that the Data Protection Commissioner may launch a detailed investigation depending on the nature of the personal data security breach incident. Such investigations may produce a list of recommendations for the attention of the relevant data controller. Responsible data controllers cooperate willingly with the Commissioner's investigations and are happy to comply with any recommendations she may issue. However, in rare cases in which such compliance is not forthcoming, the Commissioner may use her legal powers to compel appropriate actions.

Investigative Powers under the General Data Protection Regulation (GDPR)

Under the GDPR, national data protection authorities such as the Data Protection Commissioner (DPC) in Ireland have a general obligation to monitor compliance, which will require them to be able to conduct investigations. The specific investigative tasks are to:

- Conduct investigations on the application of the GDPR, including on the basis of information received from another supervisory or other public authority.
- Investigate in connection with the handling of complaints
- Carry out periodic reviews of those who have been granted certifications such as seals or marks.

The powers which are linked to these tasks are set out in Article 58(1);

- to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any information it requires for the performance of its tasks.
- to carry out investigations in the form of data protection audits.
- to carry out a review on certifications issued pursuant to Article 42(7).
- to notify the controller or the processor of an alleged infringement of this Regulation.
- to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks.
- to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or Member State procedural law.

In relation to 2.2 above, the investigative power of the Data Protection Authority requires factual indications that data processing activities are being carried out by the entity in question. The power permits investigations on processing activities performed on personal data that falls within the scope of application of the GDPR, but also includes requests for general information on the entity's data processing organisation, meaning the technical and organisational procedures that form the basis for data processing. The scope of required information will be set by the requesting supervisory authority with respect to the object of investigation. The Commissioner will have to communicate the object, as well as the intent and purpose of the request, to the concerned entity. The provision explicitly commits controllers/processors and their EU representatives to provide information, but, as regards legal persons, also commits their organs and representatives.

In relation to 2.2(f) above, this provision gives supervisory authorities the power to carry out unannounced on site inspections. However, as investigative measures should be appropriate, necessary and proportionate, a prior announcement might have to take place in some cases and, so far, usually was indeed made prior to inspections. The provision does not require the occurrence of a certain incident to allow for on-site inspections. This grants supervisory authorities an investigative flexibility to make sure, at any time, that processing is carried out in accordance with the GDPR. However, supervisory authorities have to respect any available specific requirements of EU Member State procedural law, such as the requirement to obtain a prior judicial authorisation.

Under Article 58, the exercise of investigative powers will be governed by the respective EU Member State procedural law to which the supervisory authority concerned is subject.

In Ireland, under the General Scheme of the Data Protection Bill 2017, investigative powers have also been proposed for authorised officers of the DPC. In addition to the existing power of entry and power to take documents and records from data controllers/processors (subject to legal privilege), it is proposed that the DPC officers may call on individuals to provide "reasonable assistance" in relation to the operation of data equipment, including by providing passwords, and to attend before the DPC officers at a particular time and place, to provide relevant information &/or answer any questions. The DPC officers may also require a person to give their name and address for the purposes of the DPC applying for a search warrant. It will be an offence to obstruct or impede an officer, or to alter, destroy or refuse to provide any relevant information or give false or misleading information.

One of the material changes impacting controllers under the GDPR relates to the mandatory notification of data breaches to the relevant supervisory authority, unless the breach is unlikely to result in risk to the rights of individuals, and to affected individuals, where the breach is likely to result in a high risk. These new obligations are integral to the principles of accountability and transparency that run through the GDPR.

For more information please contact Aoife Bradley.

About the Author

Abigail Butler
Senior Associate

Abigail advises on a wide range of general and commercial litigation disputes including insurance coverage disputes, debt recovery, enforcement proceedings, injunctive proceedings, contractual disputes, and property disputes.
T: +353 1 638 5835 **E:** abutler@lkshields.ie