TECHNOLOGY
DATA PROTECTION AND INFORMATION MANAGEMENT

Staying on the Right Side of the Law: Responding to Law Enforcement Requests in Compliance with the GDPR

15 October 2020

In this briefing, we consider some of the issues that arise in dealing with requests by law enforcement authorities to produce records that contain personal data.

Rob Corbet
Partner, Technology
+353 1 920 1211
rob.corbet@arthurcox.com

Caoimhe Stafford
Associate, Techology
+353 1 920 1328
caoimhe.stafford@arthurcox.com

LEGAL FRAMEWORK

GDPR vs Law Enforcement Directive

At a European level, the General Data Protection Regulation ("**GDPR**") and the Law Enforcement Directive (the "**Directive**") run in parallel. While the GDPR generally applies to data controllers that process personal data for any number of purposes, the Directive only applies to the processing of personal data by "*competent authorities*" for the purposes of preventing, investigating, detecting or prosecuting criminal offences (including the safeguarding against and the prevention of threats to public security) or the execution of criminal penalties.

The Directive was transposed into Irish law by Part V of the Data Protection Act 2018 (the "**Act**"), which defines a "*competent authority*" as a public authority that is competent for the aforementioned law enforcement purposes, or any other body authorised by law to exercise public authority and public powers for those purposes.

As such, when an organisation receives a law enforcement request, it must comply with the GDPR, while the organisation that issued the request must comply with the Directive.

Domestic and International Requests

While Irish businesses are more likely to encounter domestic requests, they may also receive requests from international authorities, which are typically made pursuant to mutual legal assistance treaties.

In this regard, the Criminal Justice (Mutual Assistance) Act 2008 sets out how Ireland engages with other countries in respect of law enforcement requests on foot of various treaties and conventions, with the aim of streamlining requests between different authorities and ensuring that adequate safeguards are in place to protect individuals. In Ireland, the Minister for Justice and Equality acts as the "Central Authority" for mutual assistance, confirming the validity of requests for assistance and checking that the provisions of the Criminal Justice (Mutual Assistance) Act 2008 are satisfied.

As the process can be relatively time-consuming, organisations may receive direct requests from authorities outside of the mutual legal assistance process. There are greater risks associated with handling such requests, such that organisations will often prefer to refer the requester to the mutual legal assistance process where they have no legal obligation to produce the records that have been requested.

PRACTICAL CONSIDERATIONS

There are a number of points that should be kept in mind when an organisation receives a law enforcement request.

1. Is the request valid?

   Before doing anything else, it is

crucial that the recipient checks that the request is valid. This will involve checking the authenticity of the request (e.g. if a request issued from an official email address or if it issued on headed paper) and whether the authority has cited the legal basis for the request.

Where legislation is cited, the recipient should check that legislation to ensure that all relevant requirements are met e.g. if a court order is required, that an executed copy of that court order has been provided.

2. Are there legal grounds for disclosing the personal data?

   As with all processing activities, the recipient must be satisfied that they have legal grounds for disclosing the requested personal data under Article 6 GDPR, and that if special categories of personal data are concerned, that they can avail of an exemption under Article 9 GDPR.

   Further, where a request will state or imply allegations that a data subject has engaged or will engage in a criminal offence, it is arguable that the handling of the request will involve the processing of personal data relating to criminal convictions and offences (i.e. 'Article 10 data.'). If the request has been issued by or via an Irish authority, it would be reasonable for the recipient to consider the processing to be conducted "*under the control of official authority,*" such that handling the request should not breach Article 10 GDPR or section 55 of the Act.

3. Will the disclosure involve transferring personal data outside of the EEA?

   Article 48 GDPR provides that personal data should not be transferred outside of the EEA unless the order/judgment for the data is based on a mutual legal assistance treaty or a similar regime. Notably, in its guidance on derogations for transfers under Article 49 GDPR, the European Data Protection Board advised very directly that "*in situations where there is an international agreement, such as a mutual legal assistance treaty (MLAT), EU companies should generally refuse direct requests and refer the requesting third country authority to existing MLAT or agreement.*"

   Chapter V GDPR should not pose major difficulties for organisations that agree to only handle domestic requests and requests that have been made pursuant to the Criminal Justice (Mutual Assistance) Act 2008.

4. Is disclosure necessary and proportionate for the requester's purposes?

   Section 41 of the Act is of central importance to Irish organisations who receive a law enforcement request. To rely on section 41 of the Act, the recipient must be satisfied that disclosure of the requested personal data – which would involve processing for a purpose other than the purpose for which that data was collected – is necessary and proportionate for the purposes of: (i) preventing a threat to national security, defence or public security; (ii) preventing, detecting, investigating or prosecuting criminal offences; or (iii) the purposes set out in section 47 of the Act (which deals with legal advice and legal proceedings).

   In this regard, the recipient should consider if the disclosure would align with the reasonable expectations of data subjects (based on indications made in the recipient's privacy policy or otherwise), whether the data that is requested seems excessive or disproportionate, and whether the data that is requested seems objectively necessary for the requester's stated purposes.

DEVELOPMENTS ON THE HORIZON

e-Evidence Package

For years, mutual legal assistance regimes have struggled to provide authorities with quick and effective access to important data. As more than half of all criminal investigations today include a cross-border request for evidence, the European Commission tabled two legislative proposals in April 2018, collectively referred to as the "e-Evidence Package."

The package consists of a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, and a Directive prescribing harmonised rules on the appointment of 'legal representatives' for the purposes of gathering evidence in criminal proceedings. While both the Regulation and the Directive remain in draft form, if enacted, the Regulation will enable a judicial authority in a Member State to directly obtain electronic evidence stored or held by a "*service provider*" (principally, providers of electronic communications services, information society services etc.) in another Member State. The Directive intends to complement the Regulation by prescribing rules for the appointment of legal representatives by service providers, who will have substantial obligations and responsibilities for receiving and responding to European Production and Preservation Orders.

Although Ireland did not opt in to the European Investigation Order Directive, which provide an efficient means for authorities to obtain criminal evidence in other Member States, it is understood that Ireland will exercise its discretion under Protocol 21 to the Treaty on the Functioning of the EU to adopt the Regulation.

DPC Inquiry

In the more immediate future, the Data Protection Commission confirmed in its 2019 Annual Report that it had commenced an own volition inquiry into An Garda Síochána's governance and oversight in respect of disclosure requests, and within organisations that process such requests.

It is hoped that the Data Protection Commission's findings will prove instructive for organisations that receive requests from law enforcement authorities.

KEY TAKEAWAY

In the absence of any definitive guidance, organisations would be well-advised to have policies and procedures in place to address how they handle law enforcement requests, having particular regard to the relevant provisions of the GDPR, the types of data that they hold, and the representations that they have made to data subjects.

The authors would like to thank Lorraine Sheridan for her contribution to this article.