



DATA PROTECTION OVERVIEW IN IRELAND

By *Krish Bhatia*
From *Chandigarh Univeristy*

Introduction

The Data Protection Act 2018 ('DPA 2018') gives further effect to the General Data Protection Regulation (Regulation (EU)2016/679) ('GDPR'). The Data Protection Commission ('DPC') is the public independent authority responsible for upholding the abecedarian right of individualities in the EU to have their data defended. The DPC is the Irish administrative authority which is governed by the GDPR and has functions and powers related to other important nonsupervisory fabrics including the (S.I.No. 336 of 2011 – the European Communities (Electronic Dispatches Networks and Services) (Sequestration And Electronic Dispatches) Regulations 2011) and the Data Protection Directive concerning Law Enforcement (Directive (EU)2016/680). The DPC is active in respect of its complaint running and enforcement functions.

Keywords

Data Protection Commission (DPC), Data Protection Act (DPA), General Data Protection Regulation (GDPDR)

The GDPR and Ireland

As an EU Regulation, the GDPR doesn't generally bear transposition into Irish law, as EU Regulations have a “ direct effect”. In Ireland, we've introduced new legislation known as the DPA 2018 which was inked into law on 24 May 2018.

Among its vittles', the Act Establishes a new DPC as the State's data protection authority

Gives further effect to the GDPR in areas where the Member Countries have some inflexibility (Part 3 of the Act), for illustration, the digital age of concurrence

This new Act, together with the former data protection legislation will be inclusively known as the “ Data Protection Acts 1988-2018”.

Data Protection legislation

The Data Protection Acts 1988-2018 are designed to cover people's sequestration. The legislation confers rights on individualities concerning the sequestration of their data as well as liabilities on those persons holding and recycling similar data.

Particular data

Particular data means data relating to a person who's or can be linked either from the data itself or in confluence with other information that's in or is likely to come into, the possession of the Department. It covers any information that relates to a linked or identifiable living existent. These data can be held on computers or in homemade lines.

The Department's scores

Under the GDPR and DPA 'S 1988-2018, this Department, as a Data Controller, has a legal responsibility to

- Gain and reuse particular data lawfully, fairly, and transparently;
- Keep it only for one or further specified and unequivocal legal purpose (s);
- Reuse it only in ways compatible with the purpose of which it was given originally;
- Keep data accurate, applicable, and not inordinate;



- Retain it no longer than is necessary for the specified purpose or purposes;
- Keep particular data safe and secure.

Data Protection Commission

The “ DPC” is the public administrative authority in this governance and while the Irish data protection vittles don't grant the DPC any fresh powers above those granted by the GDPR, the Irish vittles are more specific regarding the exercise of those powers, which include

- The right to pierce, enter the hunt, and check any demesne where the processing of particular data takes place and to check or remove any documents and records if it considers necessary
- The right to bear workers to produce any documents, records, statements, or other information relating to the processing of particular data
- The right to conduct checkups, issue information notices, and issue enforcement notices. Where the DPC decides to issue an information notice, enforcement notice, or to put an executive forfeiture, the regulator or processor has 28 days from the date on which it's notified of the decision to appeal to the court
- The right to conduct Section 110'statutory inquiries which can be a complaint- grounded inquiry; or inquiries of the DPC's"own volition"
- The right to bear a data regulator to expose a data breach to affected data subjects
- The right to put an executive forfeiture.

Failure to misbehave with an enforcement notice without a reasonable reason, or failure to notify the DPC or the data subject of the

way taken to misbehave with an enforcement notice within the needed 28 day period, can lead to the same forfeitures and imprisonment terms as about failure to misbehave with an information notice.

We've seen that the DPC exercises its powers of enforcement regularly. In 2019, it concluded complaints, a large chance of which related to access rights and subject access requests and was managing 70 statutory inquiries as of the date of publication of its last Annual Report.

On issuing a notice, the DPC can bear a data regulator or a data processor to give it a report on any matter specified in the notice. An existent must be nominated either by the applicable regulator or processor or by the DPC, to prepare the report. Any person who obstructs or impedes this existent in the medication of the report, or deliberately gives false or deceiving information in a material respect, is shamefaced of an offense.

Sequestration professionals will also no doubt be apprehensive of the recent EU Court of Justice judgment in Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems to which the DPC was a party and led to the finding that the so-called Sequestration Shield agreement between the U.S. and the EU doesn't offer sufficient protection of EU citizens data and was thus invalid.

Powers of disquisition under Chapter 4 of the DPA 2018

Chapter 4 of the DPA 2018 powers that may be exercised include the appointment of sanctioned officers who can exercise a broad range of investigatory powers handed under the DPA 2018 enabling them to gather applicable information and accouterments (e.g. powers of entry, hunt, and examination;



powers to remove and retain documents and records and to bear information and backing to be handed in respect of a disquisition). Authorized officers may be accompanied by members of the Irish police and may apply for a hunt left to the Irish courts where access to demesne is refused.

Authorized officers may issue information notices taking a regulator or processor to furnish specified information to the DPC and may issue enforcement notices taking a regulator/ processor to take certain way specified in the notice (Sections 132 and 133 of the DPA 2018). It's an offense to fail to misbehave with these notices. There's a right to appeal any notice to the High Court within 28 days of damage of same.

Section 134 of the DPA 2018 permits the DPC, where it identifies a critical need to cover data subjects' rights and freedoms, to make an ex-parte operation to the High Court for an order to suspend, circumscribe, or enjoin the processing of particular data, or the transfer of the same to a third country or a transnational association.

Section 135 of the DPA 2018 gives the DPC the power to bear a regulator or processor to report on a matter specified by the DPC. Before exercising this power, the DPC must consider whether any other of its powers may be more applicable in the circumstances, the position of coffers available to the regulator or processor, and the likely benefit to the regulator or processor of furnishing the report. These reports must be prepared by an expert' critic,' which is either nominated by the regulator or processor and approved by the DPC or nominated by the DPC in certain circumstances. The regulator or processor must enter into a contract with the critic, containing minimal terms specified by law, which the DPC may request to see in draft

form before its prosecution similar that it can bear emendations to the same. The regulator or processor must bear the costs of the report and help the critic where nicely needed. It's an offense for any person to obstruct or stymie the critic's duties under this section or to give false or deceiving information to the critic.

Powers of disquisition under Chapter 5 of the DPA 2018

Further to the DPC's power to commence complaint- grounded and own volition inquiries (Section 110), the DPC may exercise its power to probe Chapter 5 of Part 6 of the DPA 2018.

The DPC may direct one or further sanctioned officers to carry out and report to the DPC on the disquisition. Authorized officers can exercise colorful powers to impel the product of records or documents and bear persons to appear before him/ her to produce documents or records and answer questions that may be needed under pledge. Failure to misbehave can lead to a court order compelling compliance. Still, the legal honor may apply. Authorized officers can, for a disquisition, conduct an oral hail. Section 138 (12) of the DPA 2018 sets out colorful offenses, including gumming a sanctioned officer, or withholding, destroying, or refusing to give any information for a disquisition.

After a disquisition, the sanctioned officer will shoot its draft disquisition report to the applicable regulator or processor, who'll have 28 days to give written cessions in response. Following this, the disquisition report is submitted to the DPC. This report will specify whether or not the sanctioned officer considers a violation of data protection laws has passed or is being, and give the grounds



for this determination. Still, the sanctioned officer's report can not contain any recommendation, or express any opinion, as to the corrective power under Chapter 2 or 3 of the DPA 2018 (as applicable). It's for the DPC to make its determination in this regard. However, it may conduct an oral hail, invite further sessions from the regulator or processor, If having considered this disquisition report the DPC requires further information to make its determination.

The DPC must give the regulator or processor notice of its decision, the reasons for it, and where applicable the corrective power it decides to exercise, which may be an executive forfeiture and/ or another corrective power available under Article 58 (2) of the GDPR.

Criminal Convictions Data

The Irish data protection legislation provides for several restrictions on the processing of particular data relating to felonious persuasions and offenses. In this governance, this type of particular data may only be reused where

- it is done under the control of sanctioned authority;
- the data subject has handed their unequivocal concurrence to the processing;
- the processing is necessary and commensurate for the performance of a contract to which the data subject is a party to;
- the processing is necessary for carrying or furnishing legal advice or establishing, exercising or defending legal rights;
- the processing is necessary to help injury or other damage to the data subject or another person or loss in respect of damage to,

property or else to cover the vital interests of the data subject or another person; or

- the processing is permitted by clerical regulations or else authorized by the law of the State. At this time, no similar clerical regulations have been legislated.

It's also important to note the particular conditions of the Felonious Justice (Spent Persuasions and Certain Exposures) Act 2016, which provides that certain minor persuasions which are aged than seven times are supposed" spent" and the individual concerned cannot be needed by law or general agreement to expose the conviction or circumstances relating to it, except in certain circumstances.

Enforcement selections

In November 2020, the DPC issued its 1st body fine within the quantity of €75,000 against Tusla, the Irish kid, and the Family Agency. This call involved 3 personal knowledge breaches that occurred as a result of the organization's failure to redact personal knowledge once providing documentation to 3rd parties. The DPC found that Tusla had did not implement applicable structure measures to make sure level of security applicable to the chance bestowed by its process of private knowledge and so broken Article 32(1) of the GDPR. The DPC additionally found that Tusla had broken Article 33(1) of the GDPR by failing to inform the DPC of 1 of the breaches while not undue delay.

In December 2020, the DPC issued an AN body fine within the quantity of €450,000 against Twitter. This call involved Twitter's compliance with its obligations underneath the GDPR in respect of breach notification. The DPC found that Twitter had infringed Articles 33(1) and (5) of the GDPR by not



notifying the DPC of the breach on time and by failing to adequately document the breach.

Independent superior authorities

Under the GDPR, every EU Member State can have one or additional freelance public authorities liable for observation of the appliance of the Regulation. In Ireland, underneath the DPA 2018, the info Protection Commissioner has been replaced with a DPC.

Each superior authority will:

- Monitor and enforce the appliance of the GDPR
- Promote public awareness of the foundations and rights around processing
- Advise the govt on knowledge protection problems
- Promote awareness among controllers and processors of their obligations
- Provide data to people regarding their knowledge protection rights
- Maintain an inventory of process operations requiring knowledge protection impact assessment

Each authority can have the facility to order any controller or processor to supply data that the authority needs to assess compliance with the Regulation. The authority might do investigations of controllers and processors within the sort of knowledge audits, together with accessing the premises of a controller or processor. The authority will order a controller or processor to vary their processes, go with knowledge subject requests. The authority also can issue warnings to controllers and processors, ban processes, and begin legal proceedings against a controller or processor.