A&L Goodbody

Irish Data Protection Law – *2018 in Review*

By any measure, 2018 was a historic year for data protection law with the coming into effect of the GDPR on 25 May 2018.

Ireland plays an important role in the regulation and enforcement of data protection law and decisions of the Irish courts have had a disproportionate impact on European data protection jurisprudence. With the introduction of the one-stop-shop mechanism under the GDPR it is to be expected that this trend will continue in the years ahead.

Our review of Irish data protection law in 2018 highlights the legislative developments and Irish court decisions in the past 12 months. On the legislative front, the enactment of the Data Protection Act 2018 was a major achievement, establishing as it does the national investigatory and enforcement framework for the GDPR as well as implementing Directive (EU) 2016/680 on the processing of personal data by law enforcement. 2018 also saw a steady stream of decisions by the Irish courts on topics ranging from data subject access requests (the *Nowak* series of cases), the right to be forgotten (*Savage v DPC*) and the validity of data retention legislation (*the Dwyer case*).

Looking ahead, we are keeping a close eye on developments in civil litigation. The GDPR and Data Protection Act 2018 have introduced improved civil remedies for data subjects whose rights have been breached. Section 117 of the Data Protection Act 2018 creates a new form of "*data protection suit*" and permits data subjects to seek compensation for both material and "*non-material*" damage. These are new concepts to Irish law, whose boundaries are likely to be tested before the courts

Legislation

The Irish Data Protection Act 2018 (discussed here) was signed into law on 24 May 2018, to coincide with the coming into effect of the GDPR. The Act implements derogations permitted under the GDPR and represents a major overhaul of the regulatory and enforcement framework.

New Health Research Regulations came into effect on 8 August 2018, requiring organisations to obtain an individual's explicit consent in advance of processing personal data for health research purposes (discussed here). The Regulations, known as the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 (SI 314/2018), require a number of mandatory suitable and specific safeguards to be put in place when processing personal data for health research purposes.

New court rules were also introduced on 1 August 2018 giving members of the media permission to access court documents (discussed here). These measures, which apply in both the civil and criminal courts, will formalise the media's access to information. The rules give effect to Section 159(7) of the Data Protection Act 2018 to facilitate fair and accurate reporting of court proceedings.

The EU (Measures for a High Common Level of Security of Network and Information Systems) (NIS) Regulations 2018 (S.I. 360/2018) were signed into law last September 2018, implementing the NIS Directive. The Regulations apply to Digital Service Providers, and Operators of Essential Services (OESs) in the energy, healthcare, financial services, transport, drinking water supply and digital infrastructure sectors. The OESs to whom the Regulations apply have been designated by the Government. In-scope service providers are required to implement appropriate technical and organisational measures, and comply with mandatory breach notification obligations.

Litigation

(i) Data Access Requests

There were a number of cases concerning data subject access requests over the last year, including a series of *Nowak* cases, which followed on from

the CJEU's decision in ***Nowak v DPC (20 December 2017) (C-434/16)***. In that case, the CJEU adopted a broad interpretation of the concept of *'personal data'*. The CJEU held that the written answers submitted by a candidate at an exam, and any comments made by an examiner, constitute *"personal data"*, as it is information that relates to the candidate. The CJEU held that the use of the expression *"any information"* in the definition of the concept of *'personal data'* in the Data Protection Directive 95/46/EC (**the Directive**) reflects the aim of the EU legislature to assign a wide scope to the concept, potentially encompassing all kinds of information provided that it relates to the data subject. As the GDPR contains a similar definition of *"personal data"* to that in the Directive, namely *"any information relating to an identified or identifiable natural person"*, the CJEU's broad interpretation of the concept of personal data remains relevant post-25 May 2018.

In ***Nowak v DPC and Price Waterhouse Coopers [2018] IEHC 117 (26 February 2018)***, the High Court provided further guidance on the scope of the definition of *"personal data"*. The claimant argued that a memorandum held by PWC (his former employer) contained his personal data because it related to a complaint he made to the Chartered Accountants Regulatory Board against PWC, as well as audit work he had carried out as an employee of PWC. The Circuit Court, and subsequently the High Court, agreed with the DPC that the memorandum did not contain any personal data relating to the claimant. Mr Justice Coffey, at the High Court, stated: *"specifically, there appears to be nothing in the material that relates to the appellant [Nowak] as an identified or identifiable natural person which engages his right to privacy or which could, in any meaningful way be amenable to objection, ratification or erasure under the provisions of the [1988] Act"*.

Personal data has also been held not to exist simply by virtue of the complainant being informed verbally of certain facts relating to an individual alleged to be in an email when that email was not held on an automated system. Nor could the information come within the definition of manual data, consisting as it did of information that could not be said to be part of a relevant filing system *(Shatter v Data Protection Commissioner and Another [2017] IEHC 670)*.

In ***Nowak v DPC and Institute of Chartered Accountants in Ireland [2018] IEHC 118 (26 February 2018)***, the High Court considered whether personal data can be provided in a summary format in response to a data access request, rather than providing a copy of the actual document containing the data. The claimant sought access to his original exam script, claiming that the right of access under the Data Protection Acts 1988 and 2003 (the **1988 Act**) entitled a data subject to access their personal data in its original form. The High Court, following the decision of the CJEU in joined cases C-141/12 and C-372/12, Y.S. *v. Minister voor Immigratie, Integratie en Asiel, Minister voor Immigratie, Integratie en Asiel v M [2015] 1 WLR 609*, ruled that the obligation on a data controller was to communicate the relevant information (**the personal data**) not in its original form but rather in an *"intelligible form"* to the data subject. The decision confirms there is an element of discretion as to how to respond to an access request. It remains to be seen whether the right of access under Article 15 of the GDPR will be interpreted in a like manner.

In ***Nowak v DPC and Institute of Chartered Accountants in Ireland [2018] IESCDET 196 (26 November 2018)***, the Supreme Court refused to grant the claimant leave for a '*leapfrog appeal*' directly from the High Court to the Supreme Court against the High Court's decision of 26 February 2018, that personal data could be provided in summary format in response to a data subject access request. The Supreme Court held that the more appropriate course was for the claimant to pursue an appeal in the ordinary way, to the Court of Appeal.

In ***Nowak v DPC [2018] IEHC 443 (12 July 2018)***, the High Court upheld the Circuit Court's ruling that the DPC's decision was a reasoned, rational, lucid and entirely reasonable. The DPC had made a decision that the applicant's employer, ISPL, had not breached the 1988 Act, when responding to the applicant's access request. The DPC found that while a data subject has a statutory right to a copy of any personal data which is held about him or her by an organisation (subject to any applicable statutory exemptions), where a data subject explicitly limits their access request to certain personal data, it is legitimate and appropriate for a data controller to provide solely the personal data which has been specified rather than all of the personal data which the data controller holds in relation to the data subject. The DPC concluded that the applicant had limited the categories of documents she sought by using the word *"namely"* in her data access request to ISPL. The High Court approved that decision, further noting that the data subject could equally have said *"that is to say"* or *"specifically"* which would have the same meaning.

Case Study 4 of the DPC's Annual Report for January-May 2018 considers the extent of a controller's obligation to conduct searches for personal data in order to respond to an access request. The DPC noted that there was no Irish judicial authority on this issue, but that UK jurisprudence established that the implied obligation to search for personal data is limited to *"a reasonable and proportionate"*

search. Although the DPC was not obliged to follow UK authorities, she accepted that the obligation to search for personal data, under section 4 of the 1988 Act, was not without limits, and a controller should undertake a reasonable and proportionate search to identify the personal data it held on a requester. This required the controller to carry out a balancing exercise between upholding the data subject's right of access and the burden which it would impose on the data controller to search for the personal data. In the post-GDPR world, Article 12 of the GDPR permits a controller to refuse to act on an access request where it is *"manifestly unfounded or excessive"*. It remains to be seen how broadly this exemption to the right of access will be interpreted at EU or national level, but it appears to introduce a more stringent standard for refusing an access request.

(ii) The Right to be Forgotten

In ***Savage v DPC [2018] IEHC 122 (9 February 2018)***, the Irish High Court delivered its first judgment on the *"right to be forgotten"* in Ireland. The case concerned a complaint made to the DPC about Google's refusal to delist a URL link to a web page for a discussion forum. The DPC decided that there had been no contravention of the 1988 Act, as the relevant link was accurate, in that it represented an opinion about the claimant that was expressed by a user of the discussion forum, rather than a verified fact. The Circuit Court allowed the claimant's appeal on the basis that it was not clear from the URL title that the original poster was expressing his/her opinion, and the URL title was therefore inaccurate. The Court said that if the expression was an opinion, it should have been presented within quotation marks or parenthesis. The High Court overturned the Circuit Court's decision, finding that it had erred in not considering the underlying article to which the URL link related. If the Circuit Court had done so, it could not have come to the conclusion that the URL title was inaccurate data, factually incorrect or had the appearance of fact.

The High Court also noted that Google does not carry out an editing function, and to oblige Google to place quotation marks around a URL link would involve an editing process, which was not envisaged in the *Google Spain* decision.

(iii) Standard Contractual Clauses

In ***DPC v Facebook Ireland Ltd and Schrems [2017] IEHC 545 (3 October 2017) discussed here***), the Irish High Court asked the CJEU to rule on the validity of Standard Contractual Clauses (SCCs). Ms Justice Costello has referred 11 specific questions to the CJEU. Facebook appealed the High Court's decision to make the reference to the CJEU, and the Supreme Court is due to deliver its judgment on that appeal shortly. As the High Court refused Facebook's application for a stay on the CJEU referral, the reference is now pending before the CJEU.

(iv) Data Retention

In ***Dwyer v Commissioner of An Garda Síochána [2018] IEHC 685; [2019] IEHC 48***, the High Court ruled that certain sections of the Communications (Retention of Data) Act 2011, which requires data generated by mobile phones to be retained by telecommunications service providers for two years, and allows An Garda Síochána and certain other State agencies to make requests to access such data for criminal investigative purposes, is incompatible with EU law. The Court noted that the State has been long aware of the defects with the 2011 Act, but has yet to introduce revised legislation at the Oireachtas. The State is appealing against the High Court's decision, and a stay has been placed on the Court's decision until the first directions hearing of the proposed appeal. It will be a matter for the Court of Appeal or the Supreme Court (in the event of a leapfrog appeal) as to whether the stay should be continued until the determination of the appeal. Given the matter is being appealed, the court's ruling should not be used as a reason for service providers to destroy or cease to retain telephony data.

Our team

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Claire Morrissey
Partner
+353 1 649 2246
cmorrissey@algoodbody.com

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

Davinia Brennan
Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com