Data Protection Commissioner publishes Annual Report for 2018

The Data Protection Commissioner (DPC) has published her final Annual Report covering the period of 1 January 2018 to 24 May 2018.

From 25 May 2018, the office of the Data Protection Commissioner ceased, and the new Data Protection Commission was created under the Data Protection Act 2018. The Report includes some interesting case-studies, such as the prosecution of a company for sending marketing emails to work email addresses. It also discusses litigation to which the DPC was a party to this year, including the case of *Nowak v DPC*, where the High Court followed the CJEU's decision in *Y.S. v. Minister voor Immigratie & Ors*, finding that a controller exercises some discretion in regard to how to respond to an access request. Although these cases pre-date the GDPR, they remain of interest in the post-GDPR world. This briefing note looks at some of the highlights of the Report.

Queries

Between 1 January to 24 May 2018, the DPC received over 9,900 emails, 10,200 telephone queries, and 1800 items of correspondence by post— an increase of around 30% on the preceding six months. The complexity and nature of the queries indicated a high level of awareness of the GDPR and an eagerness by controllers and processors to implement measures to comply their new obligations. The DPC has warned, however, that the 25 May 2018 was not the endgame, and that compliance with the GDPR and Data Protection Act 2018 will be an ongoing and evolving issue.

Complaints

The DPC received 1,249 complaints, with the largest single category continuing to concern access requests, which made up 45% of the total complaints received. The vast majority of complaints were concluded amicably between the parties, with only 12 formal decisions being issued under Section 10 of the Data Protection Acts 1988 and 2003. 41 complaints were made under the e-Privacy Regulations 2011 in respect of unsolicited electronic direct marketing communications, and the DPC prosecuted three companies in respect of 46 offences under those Regulations.

Breach Notifications

The DPC received 1,198 valid data security breach notifications. As in other years, the highest category of data breaches reported under the Voluntary Breach Code of Practice concerned unauthorised disclosures of data, and such breaches accounted for approximately 59% of total data breach notifications received.

Sectoral Investigations

The DPC's Special Investigations Unit continued its ongoing investigation into the private investigator sector and inspections were carried out at the premises of two private investigators. The DPC also completed its investigation into Privacy in the Hospitals Sector, and published a Special Investigations Report which identified 35 risks and 76 recommendations to mitigate those risks. The primary purpose of the investigation was to bring to the attention of every hospital in

the State, the matters of concern the DPC found in the sample of twenty hospitals inspected. In the post-GDPR environment, the DPC has confirmed it will be proactively targeting its enforcement activities at sectors involved in large-scale data processing activities that constitute a high risk, such as online tracking, automated decision-making and profiling; processing of high-risk data, such as health, biometric, financial or insurance data; and processing using emerging technologies.

Audits/Inspections

Twenty-three audits/inspections were carried out to check for compliance with data protection law. The Report sets out key findings in relation to these audits, including: retention of computerised data for longer than necessary for the purposes for which it was collected; failure by organisations to maintain a CCTV policy; failure to obtain adequate consent to the use of cookies on websites; seeking a data subjects' PPSN when it is inappropriate to do so; and reliance on data sharing agreements which are not in compliance with data protection law.

Litigation

The Report provides an overview of recent judgments in which the DPC was a party. It is worth noting, in particular, the High Court's decision in *Nowak v DPC and Institute of Chartered Accountants in Ireland* [2018] IEHC 118. In that case the 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 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 in relation to the right of access of a data subject 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. This decision pre-dates the GDPR. It remains to be seen whether Article 12/15 of the GDPR will be interpreted in a like manner.

Case-Studies

Appendix II of the Report contains a number of case-studies in relation to complaints received by the DPC this year.

Case Study 1 discusses the recent prosecution of a company for sending marketing emails to individuals' work email addresses. The e-Privacy Regulations 2011 permit electronic marketing communications to be sent to an individual on an opt-out basis where the email address reasonably appears to the sender be one used by a person in the context of their commercial or official activity.

The DPC has adopted a narrow interpretation of this rule, warning that the sender must be able to demonstrate that the marketing material *"is directly relevant to the role of the recipient in the context of their commercial or official activity (i.e. within their workplace)"*. The DPC found that this was not the case here, as the marketing communications related to attempts by the sender to sell advertisement space in various publications and to sell stands at exhibitions, but none of the individual complainants who received the communications had any role in relation to marketing related matters within their own workplaces. The DPC also noted that where a company/corporate recipient notifies the sender that it does not consent to receiving marketing emails, it is unlawful for the sender to subsequently send such emails. This approach appears to conflict with previous Guidelines issued by the DPC on direct marketing, which indicate that unsolicited marketing communications addressed to corporate entities (not office-holders within such an entity) fall outside the scope of data protection law insofar as they do not involve the use of *"personal data"*.

Case Study 4 considers the extent of a controller's obligation to undertake 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 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. The DPC further noted that where a controller relies on a statutory exemption to refuse or partially refuse an access request, it must prove convincingly, and by evidence, meeting the civil standard of proof that each of the exemptions on which it sought to rely did in fact apply and operated to trump the requestor's right of access.

This decision pre-dates the GDPR. 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.

What's ahead for 2019?

The DPC, as lead rapporteur, has commenced work on a paper on the contractual necessity legal basis under Article 6(1)(b) GDPR for processing personal data, in the context of the provision of online services, and we look forward to the publication of those guidelines in 2019. With the support of the Office of Ombudsman for Children, the DPC will also be running a consultation on specific data protection safeguards that should apply to children under the GDPR. The consultation will lead to the development of a code of conduct in line with section 32 of the 2018 Act and Article 40 of the GDPR. In addition the DPC has been appointed co-ordinator of the newly-formed Social Media subgroup whose role is to develop guidance and set strategic priorities relating to the processing of personal data by social media companies.

Further developments are also expected in relation to the Irish High Court's referral to the CJEU on the validity of the Standard Contractual Clauses for transferring personal data out of the EEA. The Irish Supreme Court is due to hear Facebook's appeal aimed at halting the referral to the CJEU on 21 January 2019. In the meantime, the High Court's reference to the CJEU remains valid and is pending before the CJEU.

In regard to enforcement priorities, the DPC has indicated that assessing compliance with the transparency requirements under the GDPR and privacy notices will be a priority focus area in the short term. This assessment can be done in a relatively hands-off manner, particularly where it involves an assessment of compliance with the requirements under Article 12, 13 and 14 of GDPR and the related WP29 Guidelines on Transparency, endorsed by the EDPB. Not unlike breach notifications and data access requests, the privacy notice, the public statement of what organisations are doing with personal data, could well become a trigger for deeper regulatory investigations. The DPC has also emphasised that it is imperative, in line with the principle of accountability in GDPR, that organisations can stand over and justify their data processing arrangements and be able to demonstrate compliance.

The Report indicates that the DPC will launch a consultation process around a GDPR-term regulatory strategy before the end of the first quarter of 2019, with the aim of providing transparency to organisations and the public in regard to resource deployment choices and to the DPC's role and how that role will be implemented.

Our team

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

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

Mark Rasdale
Partner
+353 1 649 2300
mrasdale@algoodbody.com

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

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