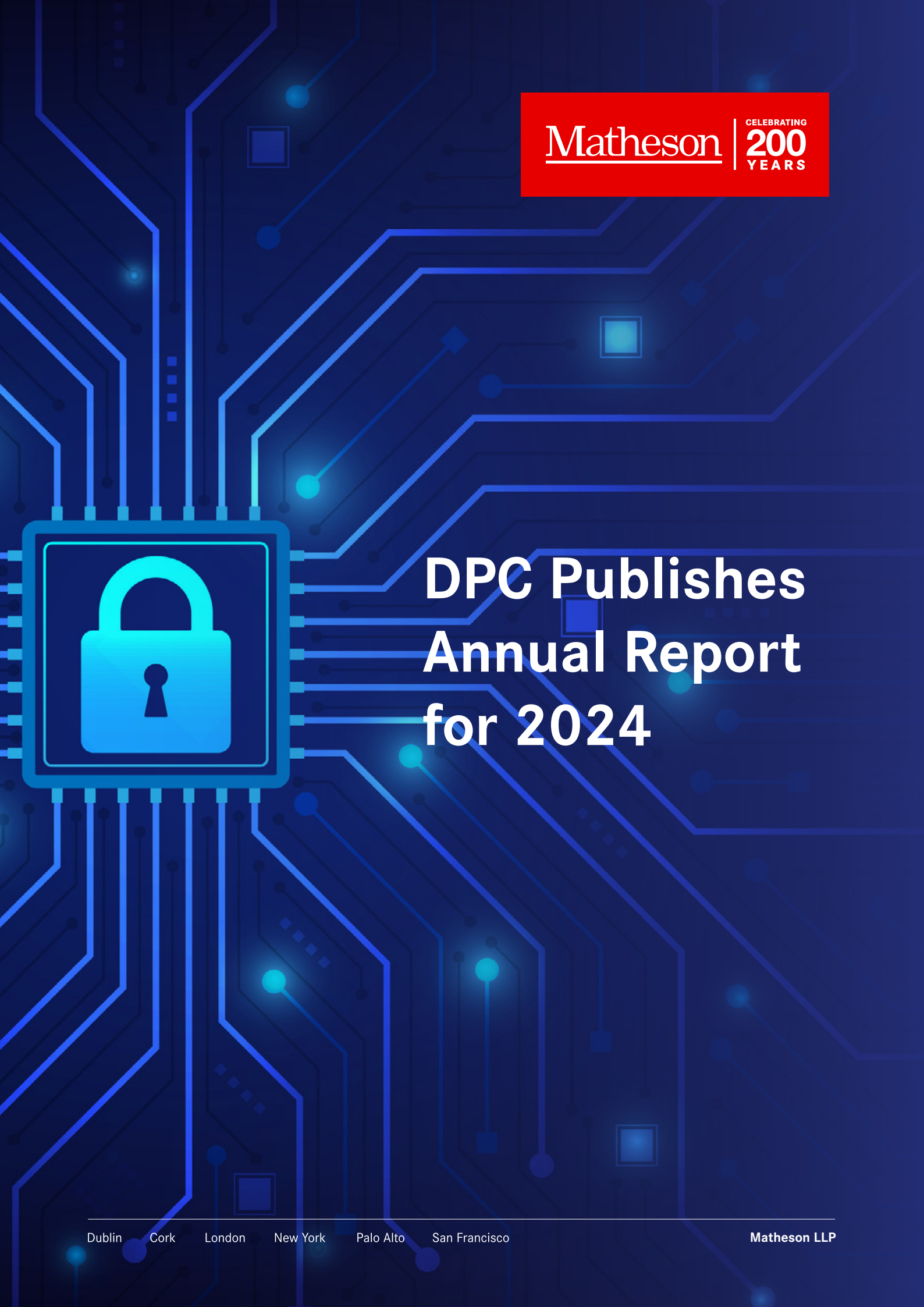
Matheson | CELEBRATING 200 YEARS



DPC Publishes Annual Report for 2024

The Irish Data Protection Commission ("**DPC**") recently published its Annual Report for 2024 ("**Report**"). As usual, the Report contains some interesting trends, statistics, and insights into the DPC's regulatory activities during 2024. The Report also highlights the significant emphasis which the new Commissioners, Dale Sunderland and Des Hogan place on the values which the DPC should exhibit as a regulator, including "*fairness, consistency and transparency*", acknowledging that these values should be inherent as they go about their work. In addition, the DPC separately published a Booklet of Case-Studies from 2024, and released its first Public Attitudes Survey. In this article, we consider some of the key highlights of the Report and some interesting case-studies.

THE REPORT

The Report highlights that although the DPC's regulation of Artificial Intelligence ("**AI**") model training attracted a lot of public interest in 2024, the DPC was active on many other fronts. For example, the DPC brought four-large scale inquiries to a conclusion, including three inquiries concerning Meta, and one inquiry concerning LinkedIn. In addition, three new inquiries were commenced into Google (AI model training), the HSE (safety of sensitive personal data) and Ryanair (use of biometric data), both in response to concerns identified by the DPC and to complaints from other parties.

The DPC also took follow-up action in respect of previous Inquiry decisions into the use of children's personal data by TikTok and Instagram. The DPC had specified corrective measures it required the companies involved to address as part of its Inquiry findings. Notwithstanding the fact that the companies are appealing these decisions, the corrective measures orders continued to have effect and the DPC monitored enforcement of these, leading to successful outcomes including children's personal data now being set as private rather than public by default.

ARTIFICIAL INTELLIGENCE

In regard to AI, the DPC intervened in a number of cases where it identified deficiencies and failures in plans to train AI models using personal data of EU/EEA citizens which could expose users to significant risks and harms, including in respect of AI model training by Twitter, Google, and Meta.

In an effort to bring greater clarity to the application of data protection requirements in AI model training and deployment, and to reach a harmonised EU position and level playing field for industry, the DPC requested a

statutory opinion from the EDPB. This involved EU/EEA regulators working together over a 14-week period. A formal opinion was adopted by the EDPB in December 2024 (previously discussed here).

With the introduction of the EU AI Act, the DPC was designated as a fundamental rights body, one of 9 such bodies in Ireland (previously discussed here). It has also been proposed by the Irish Government that the DPC will have a role as a markets surveillance authority, along with seven other regulators operating in other sectors, such as the Central Bank, ComReg, and the Competition and Consumer Protection Commission. These authorities, along with a lead regulator (yet to be appointed) will together coordinate enforcement of the AI Act.

Separately, new functions have also been given to data protection authorities under the EU Political Advertising Regulation ("**the Regulation**") adopted in March 2024. This Regulation will give the DPC an important role in ensuring that during elections personal data is only used for advertising in accordance with the Regulation.

NATIONAL AND EU COOPERATION

In order to deepen the DPC's engagement with their peer European and international data protection and privacy authorities, and in light of the new EU Digital legislation being introduced, the DPC appointed two new Deputy Commissioners last year, including:

(i) Deputy Commissioner responsible for EDPB, International affairs & the AI Act (Gráinne Hawkes) to lead DPC work in this area; and

(ii) Deputy Commissioner responsible for Inter-Regulatory Cooperation & ePrivacy Prosecutions (Jennifer Dolan) with the aim of deepening engagement with both national and EU level regulators in other regulatory spheres.

The Report notes that despite bringing additional complexity and volume to the DPC's workload, inter-regulatory cooperation has been set as a DPC priority in the interests of regulatory clarity and consistency.

The DPC's Senior Management Committee now consists of two Data Protection Commissioners (with a third Commissioner soon to be appointed), and 17 Deputy Commissioners (as detailed further in the Report).

QUERIES & COMPLAINTS

The DPC received 32,152 contacts (including queries and complaints) from the public in 2024. The Report confirms that when an individual contacts the DPC raising a concern, it will engage with the organisation whose behaviour is at issue, in particular the organisation's Data Protection Officer ("**DPO**") where applicable. In most cases this engagement will lead to resolution without further intervention by the DPC.

However, in situations where escalation is necessary the DPC emphasises the importance of it having access to written correspondence between the complainant and the organisation, which details the issues and positions of both parties.

DSARS REMAIN HIGHEST CATEGORY OF COMPLAINTS

During 2024, the DPC received 11,091 new cases (including complaints and requests for advice/guidance). 2,673 of these cases progressed to the formal complaint-handling process (including 194 electronic direct marketing complaints).

Overall, the DPC concluded 2,357 formal complaints in 2024, including 1,367 complaints received prior to 2024. In addition to 8,418 cases being resolved though amicable means. The highest category of complaints (34%) from individuals continued to concern Data Subject Access Requests ("**DSARs**"), typically due to organisations not responding within the statutory timeframe, or dissatisfaction with the response due to the application of redactions and statutory exemptions.

The Report notes that any statutory exemptions applied should be documented by the organisation, for example in the form of a table. In addition, organisations should explain the reason why the statutory exemption is being applied. The DPC warns that it is not sufficient to merely list the applicable exemptions and relevant provisions of the legislation in the DSAR response letter.

The other most common complaints concerned fair processing of personal data (17%), and the right to erasure (14%). The Report emphasises the importance of organisations communicating effectively with individuals when they make an erasure request, and explaining the reason why their personal data cannot be erased (where applicable). Individuals should also be informed of how long the organisation will continue to process the personal data in question. The more effective the communication between an individual and an organisation, the more likely it is to result in complaints being resolved prior to the DPC's involvement, or through the amicable resolution process facilitated by the DPC.

In addition, the Report notes the new location and address of the DPC, at which complainants can submit their concerns by post (if preferable), namely: 6 Pembroke Row, Dublin 2, D02 X963, Ireland. Organisations will also need to take steps to review and update any references to the DPC's old address in their Privacy Notices.

Enforcement Notices issued where no engagement occurs

Although a large volume of complaints continue to be resolved by means of amicable resolution, the DPC will utilise its powers of enforcement against an organisation when it fails to comply with its data protection obligations.

The most common example of an Enforcement Notice being issued is where an organisation does not engage at all with either the data subject or the DPC. The DPC issued eight Enforcement Notices in 2024, the majority relating to non-response to DSARs.

Electronic Direct Marketing Complaints

The Report notes that the DPC actively investigates and prosecutes offences relating to electronic direct marketing under the ePrivacy Regulations 2011. The DPC completed 146 electronic marketing investigations in 2024; issued 49 warning letters to companies on foot of unsolicited marketing communications; and prosecuted eight companies for sending unsolicited marketing communications without consent. The court directed the companies to make charitable contributions in lieu of a conviction and fine. The donations were relatively low, amounting to a total of €9,725 across all eight cases.

In line with the approach generally taken by the DPC in previous years, all of the companies prosecuted by the DPC in 2024 had received a prior warning to correct inadequate processes and procedures for electronic marketing. The DPC warned that it is critical before embarking on electronic marketing campaigns, that companies carry out robust testing and checks with their service providers to ensure that they have the valid and up-to-date consent of the individuals on their marketing lists and that their opt-out mechanisms are fully functional.

One-Stop-Shop Complaints

Since the implementation of GDPR in May 2018, the DPC has received 1,853 cross-border complaints. The DPC was designated as LSA for 1,612 of these complaints, and has now resolved 82% of these complaints.

Where the DPC was LSA, 63% of cross-border complaints were lodged by complainants with another EU/EEA supervisory authority and then transferred to the DPC via the OSS mechanism, and 37% of cross-border complaints were lodged with the DPC directly.

In 2024, the DPC concluded 145 cross-border complaints, and submitted 115 notifications of amicable resolutions via the Article 60 cooperation mechanism. Details of these cases can be found on the EDPB website.

DATA BREACHES

In 2024, the DPC received 7,781 valid data breach notifications. This represented an 11% increase (794) on the overall data breach numbers received by the DPC in 2023. Of the notifications received, 7,346 were GDPR notifications. In line with previous years, the highest category of data breaches notified to the DPC in 2024, namely 60% of notifications, concerned unauthorised disclosure of personal data, in incidents affecting single individuals or small groups.

In particular, correspondence issuing to incorrect recipients continued to feature prominently. The DPC attributes such errors to poor operational practices and human error. Staff training on this front, along with

disabling auto-complete of email addresses on outlook may assist with reducing the number of these type of breaches. Of the breach notifications received in 2024, 81% were concluded by year-end. The Report notes that the DPC continually monitors breach notifications received to identify trends and inform further investigative and enforcement actions.

The DPC also received 428 data breach notifications under the ePrivacy Regulations 2011 (up 193% on 2023). The Report attributes the increased number of breaches notified to the DPC under the ePrivacy Regulations 2011 as being the result of the entry into force of the EU (Electronic Communications Code) Regulations 2022, and the expanded definition of the term "electronic communications service". This definition brings "*over the top*" service providers, such as messaging services, within the remit of the ePrivacy Regulations 2011. Regulation 4 of the ePrivacy Regulations 2011 requires such services to report data breaches to the DPC within 24 hours.

The most frequent cause of ePrivacy breaches reported to the DPC arose as a result of:

- communications directed to the wrong recipients (email addresses / phone numbers / postal addresses / eircodes recorded incorrectly or not updated by individuals); and
- and social engineering / phishing schemes (third parties gaining access to customer accounts, including access to personal details).

The Report highlights that in 2024, the DPC handled 20 complaints from individuals relating to alleged personal data breaches, which were not resolved through an amicable resolution process.

DECISIONS AND FINES

As of 31 December 2024, the DPC had 89 statutory inquiries on-hand, including 53 cross-border inquiries and 36 domestic inquiries. In 2024, the DPC delivered 11 statutory inquiry decisions, six of which resulted in administrative fines, amounting to a total of €652 million. Four of these administrative fines concerned cross-border statutory inquiries, and two concerned domestic statutory inquiries.

Cross-Border Inquiry Fines

LinkedIn was subject to the largest fine, in the amount of €310m fine (previously discussed here). The other three fines of €11m, €240 and €91m were imposed on Meta in respect of the token breaches, and plaintext password breach (previously discussed here).

Domestic Inquiry Fines

In addition, Sligo County Council and Maynooth University were respectively subject to €29,500 and €40,000 fines. The Sligo County Council fine was imposed following an inquiry into the Council's use of CCTV cameras and automated number plate recognition cameras for the purposes of prosecuting crime and other purposes. The DPC found that the council had no valid legal basis for the processing, and had failed to erect appropriate signage in respect of the CCTV cameras. In addition, a fine was imposed on Maynooth University following a data breach notification by the university concerning unauthorised access to six email accounts of university employees. The unauthorised access led to fraud and financial loss by one affected person. The DPC imposed a fine on the basis that Maynooth University had failed to ensure appropriate security measures, and had also failed to notify the DPC of the personal data breach within the statutory timeframe.

Reprimands

The DPC also imposed reprimands on three organisations in 2024, including: Airbnb, Groupon, and Apple. In two other cases, the DPC's Inquiry resulted in no GDPR infringements being found (including in respect of Apple and Mediahuis Ireland Group Ltd). The reprimands imposed on Airbnb and Groupon concerned excessive and unlawful processing of personal data for identity verification documentation purposes, when data subjects made erasure or access requests.

The Apple Inquiry concerned a complaint that Apple had not properly complied with an erasure request in respect of a user's Apple ID. The DPC examined the legal basis on which Apple relied on to retain the hashed value of the data subject's email address. The DPC found that Apple was entitled to validly rely on the "legitimate interests" legal basis for the purpose of retaining a hashed value of the user's email address following the erasure request, and had complied with its obligations under Article 17 GDPR. However, the DPC imposed a reprimand on Apple, on the grounds that it had infringed its transparency obligations under Articles 13(1)(c) and (d) GDPR. This was due to Apple failing to inform the user of its intention to retain the hashed value of their email address, and of the lawful basis, and legitimate interests for doing so.

Fines - 2025

It is noteworthy that only three fines have been issued by the DPC to date in 2025.

These fines will be covered in next year's Annual Report. These fines include:

(i) a €550,000 fine imposed on Department of Social Protection, in respect of its processing of biometric facial templates, and associated use of facial matching technologies as part of the registration process for the Public Services Card;

(ii) a €125,00 fine following the conclusion of the DPC's Inquiry into City of Dublin Education and Training Board ("**CDETB**") for failure to implement appropriate security measures and report a personal data breach to the DPC and affected data subjects without undue delay; and

(iii) a €530m fine on TikTok following the DPC's Inquiry into its transfers of EEA user data to China. Notably, the DPC found that TikTok had failed to comply with the data transfer rules in Chapter V GDPR, and had also failed to comply with its GDPR transparency obligations. In particular, the DPC found that TikTok failed to provide sufficient information to users in its privacy notice regarding its data transfers, including the names of the non-EEA countries it was transferring data to, and the nature of the privacy operations constituting the transfer (namely remote access to personal data stored in Singapore and the US by personnel based in China).

ENGAGEMENT AND SUPERVISION

The DPC had 757 supervision engagements during 2024, the majority of which were with multinational technology companies (421) and the private sector and financial services institutions (121). The Report highlights how proactive engagement and intervention by the DPC with organisations can help organisations to identify potential data protection issues when developing new products or services. In particular, such engagement can serve to "*mitigate data protection risks and harms to individuals as well as ensuring that personal data is used in ways that are responsible, lawful and people-centred, without giving carte blanche or advance approval of plans to any organisation*".

If during engagement with the supervision function it appears that the organisation may be infringing or likely to infringe data protection law, the DPC can take relevant enforcement action in such circumstances. The Report notes that this approach supports the DPC's efforts to place resources where they can achieve the most good, and produce better results for all stakeholders.

Legislative Consultation

A key statutory function of the DPC is prior consultation on legislative measures that relate to data processing. Both the GDPR and Data Protection Act 2018 require Government Departments to consult the DPC on any legislative or regulatory measures that will involve data processing. The DPC provided guidance and observations on 56 proposed legislative measures in 2024.

Technology companies sharing personal data with law enforcement agencies

The Report notes that in 2023, the DPC contacted a number of technology companies regarding their practices in relation to how they share personal data with law enforcement and what practices and policies they have in place when doing so. This examination involved the DPC looking at matters such as the process by which controllers:

(i) authenticate requests for user data from law enforcement agencies,

(ii) determine the validity of emergency requests for user data so as to respect the principle of data minimisation when responding to requests for user data.

(iii) staff process such requests from law enforcement agencies.

Where the DPC deemed controllers' policies to not be sufficiently developed, they made recommendations on further action that could be taken in this regard. Whilst the Report confirms that this project has now been concluded, it notes that a number of organisations reverted to the DPC (as requested) during 2024 with details on how they addressed the DPC's recommendations.

Enhanced Cooperation with other EDPB Supervisory Authorities

The DPC continued its engagement with its fellow EU/EEA DPAs in day-to-day operations under the One-Stop-Shop ("**OSS**"), in the performance of its role as LSA. This included responding to routine requests for information, follow up communications and actions on OSS complaints, and providing updates on OSS inquiries and supervision cases.

In 2024, the DPC submitted seven draft decisions, and 11 final decisions to the GDPR Article 60 cooperation process. Of the seven draft decisions, four involved large-scale inquiries which received no objections from other Concerned Supervisory Authorities ("**CSAs**").

In addition, the DPC submitted, through the Article 60 cooperation mechanism, 115 notifications of amicable resolutions achieved in cross-border complaints. As a CSA, the DPC reviewed 112 Article 60 draft decisions / revised draft decisions and 31 informal consultations sent to it by peer EU /EEA DPAs during the year.

DATA PROTECTION OFFICERS (DPOs)

The Report notes that the role played by DPOs "*is critical for the successful application of data protection law... and in order to carry out their tasks in an effective manner, DPOs must be fully supported by their employer and allowed to act independently within the organisation*".

The DPC participated in the EDPB's 2023 Coordinated Enforcement Framework ("**CEF**") on DPOs, which aimed to generate deeper insights into the role at an EU level. The DPC found three substantive issues:

The Resources of the DPO - 33% of respondents felt they did not have sufficient resources to fulfil the role of a DPO.

- Conflicts of Interests - 36% of respondents indicated that they had additional tasks to those relating to data protection with a substantial number pointing to tasks which did not complement the role of DPO.
- Experience - 80% of DPOs replied they have at least 3+ years of experience working on the application and the interpretation of data protection requirements.
- Further details on this report can be found on the EDPB website here.

CASE-STUDIES

The DPC published a booklet of 31 case-studies from 2024 alongside the Report, which illustrate the regulatory approach taken by the DPC in relation to a range of data protection compliance issues, such as regarding DSARs, data breach incidents, the right to erasure, and unauthorised processing of employee data. We have set out a number of interesting case-studies below.

DSARs

In regard to DSARs, the case-studies highlight the importance of organisations providing data protection training, including refresher training, to all employees in customer-facing roles, to ensure that an individual's right of access is respected and upheld in all instances.

The case-studies also remind us that the GDPR does not apply to the personal data of deceased persons, and accordingly the right of access to such data falls outside the remit of the DPC. In addition, the case-studies highlight

that when a complaint is made to the DPC for failure to respond to a DSAR, the DPC will request documentary evidence of the efforts an organisation has undertaken to locate the individual's personal data. Accordingly, organisations must ensure that appropriate organisational measures are in place to be able demonstrate to the DPC that adequate searches have taken place to locate any records containing personal data that may be processed.

The case-studies further show that, in circumstances where an invoice references an individual, that invoice may be deemed to contain their personal data, and hence falls within the scope of a DSAR.

Erasure

In regard to the right to erasure, the case-studies confirm that once an individual attains 18 years, they have full control over their own data protection rights, including the ability to request erasure of historical data dating back to when the individual was a minor.

Parents or guardians may request the erasure of data on their behalf, only if they choose to provide their parent with a signed letter of authority. The DPC emphasises that it is for the organisation, acting as controller, to verify and ensure that any erasure request, and letter of authority, is valid under the circumstances, to ensure that no unlawful disclosure or erasure of personal data takes place.

Data Breaches

In regard to data breaches, the Report discusses a case-study which involves an increasingly common data breach scenario, namely an ex-employee forwarding emails and attachments containing personal data from their work account to their private email account.

The case-study shows the importance of organisations having a data protection policy in place setting out employees' responsibilities when processing personal data in the course of their duties, and ensuring that employees are familiar with, and receive training in respect of, this policy.

Organisations should also have strict rules in place prohibiting employees from sending work-related correspondence to their personal email or to any other unauthorised third party under any circumstances.

Unlawful Processing of Employee Data

In regard to unlawful processing of employee data, the case-studies warn employers of the risks of accessing personal correspondence sent by employees using company equipment.

The DPC highlights a complaint received from two individuals who were terminated following an employer's review of their personal email exchanges. The emails concerned a business plan that would make them a competitor to their then employer. The employer discovered the email exchange following a review of a personal email account that one individual had left open on a shared access company computer.

The DPC asked the organisation to provide its lawful basis for processing the individuals' personal data from the personal email account. The organisation claimed that the individuals had consented to the processing of any/all of their personal data, when they were provided with a copy of the company's privacy notice that informed them it would process personal data stored on any company IT equipment, and that their consent was also evident from their signed contracts of employment.

The DPC found that the individuals' data protection rights were infringed by the organisation under Articles 5(1)(a),(b),(f) GDPR, which relate to the principles of lawfulness, fairness and transparency; purpose limitation; and integrity and confidentiality. Furthermore, the initial accessing and viewing of the individual's personal email account was conducted in breach of their data protection rights, contrary to Article 32(1) and 32(2) of the GDPR.

The case-study serves as a reminder that consent should generally not be relied upon as a legal basis in an employment context due to the imbalance of power in such relationships, and the likelihood that it has not been freely and validly given. In addition, reliance on signing a contract of employment to indicate consent for processing personal data, does not meet the consent criteria under the GDPR.

Direct Marketing

Finally, the case-studies also provide some helpful guidance on what constitutes "direct marketing" communications. Although the ePrivacy Regulations 2011 set out the rules regulating electronic direct marketing, they do not contain any definition of what constitutes "direct marketing" per se, and the issue has caused some confusion over the years. FAQs on the DPC's website simply indicate that "*Direct marketing involves a person being targeted by an organisation (marketer) attempting to promote a product or service, or attempting to get the person to request additional information about a product or service*".

The case-studies helpfully highlight a complaint to the DPC concerning a communication from an airline to an individual following a recent trip with that airline. The individual viewed an email requesting feedback on their recent trip as a "*direct marketing*" email, and contacted the DPC advising that they could not find an unsubscribe option in this communication.

The DPC found that "*correspondence sent solely for informational or feedback purposes does not constitute*

direct marketing". However, if such communications included direct marketing content, it could be classified as direct marketing, thus necessitating the inclusion of an unsubscribe option. In this particular case-study, the DPC noted that the message from the airline did not include any direct marketing content, and the airline was simply seeking feedback in order to improve the service offered.

CONTACT US

If you would like to discuss the Report, or any other related data protection and data privacy matter concerning your business, please do not hesitate to contact Davinia Brennan or any member of our Technology and Innovation Group.

Anne Marie Bohan
Partner, Head of Technology and Innovation
T +353 1 232 2212
E anne-marie.bohan@matheson.com

Davinia Brennan
Partner
T +353 1 232 2700
E davinia.brennan@matheson.com

Sarah Jayne Hanna
Partner
T +353 1 232 2865
E sarahjayne.hanna@matheson.com

Carlo Salizzo
Partner
T +353 1 232 2011
E carlo.salizzo@matheson.com