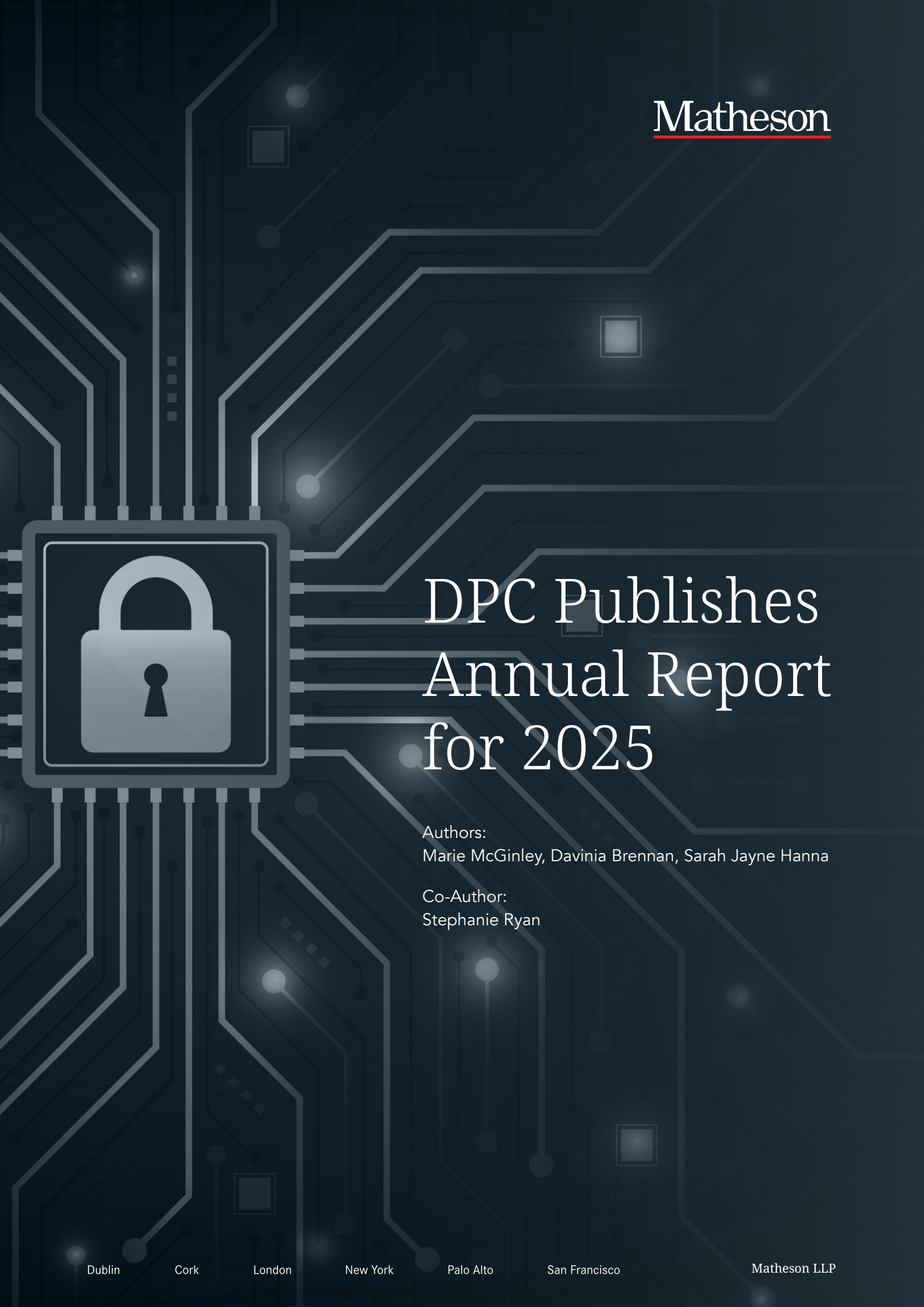
Matheson



DPC Publishes Annual Report for 2025

Authors:
Marie McGinley, Davinia Brennan, Sarah Jayne Hanna

Co-Author:
Stephanie Ryan

The Irish Data Protection Commission ("**DPC**") recently published its Annual Report for 2025 ("**Report**"), describing the year as its most active to date. The Report provides a comprehensive account of the DPC's activities during 2025, a year marked by an unprecedented 45% increase in complaints received. A key trend with many of these complaints was the use of artificial intelligence ("**AI**") tools in data subject complaint correspondence. Due to increased operational demands and its evolving regulatory remit, the DPC continued to expand its workforce in 2025, reaching a headcount of 295. The DPC intends to continue to grow in 2026. In addition, Niamh Sweeney was appointed as a third Data Protection Commissioner, alongside Des Hogan and Dale Sunderland.

The DPC also separately published a Booklet of Case-Studies from 2025, and released its first Sharenting Survey which independently surveyed parents to gain insights into their social media use and information-sharing practices in relation to their children.

In this article, we consider some of the key highlights of the Report and some interesting case-studies.

The Report – Balancing innovation and regulation

The Report notes that a central topic debated throughout 2025 concerned the balance between technological innovation and ensuring rigorous protection for personal data. In this respect, the Report notes the European Commission's legislative proposal to simplify the GDPR, amongst other regimes (previously discussed here).

The Report showcases the DPC's activity on multiple fronts, including its continued focus on regulating emerging technologies (including generative AI model training), advancing cross-border enforcement through the one-stop-shop ("**OSS**") mechanism, strengthening the protection of children's personal data, and regulating international data transfers.

Unprecedented volume of new cases in 2025

The DPC received 16,160 new cases (including queries and complaints) in 2025, representing a 45% increase on the 11,091 cases received in 2024. This has had a direct impact on the DPC's response times and case-handling time-frames. Of the new cases received in 2025, 3,385 progressed to the complaint-handling process, representing a 27% increase in comparison to 2024. In addition, the DPC responded to more than 6,500 telephone calls from individuals and organisations during the year, of which 85% were from individuals.

The DPC also conducted a total of 13 site visits with organisations (such as a solicitor's office, sole trader business premises, and a GP surgery) who failed to engage with the DPC's complaint process or who had failed to respond to a data subject's rights request. The Report notes that these visits are undertaken to determine whether the organisation remains operational, in order to highlight to smaller businesses what their responsibilities are under the GDPR, or to ensure receipt of documents prior to use of enforcement powers.

Use of AI in Complaints

During 2025, the DPC observed an increase in individuals using AI tools to assist them exercise their data protection rights. The Report warns that individuals should exercise caution when using such tools to generate complaints on their behalf, as this can often lead to inaccurate or invalid requests being submitted. This can then, in turn, hinder the exercising of rights, as well as the handling of any subsequent complaint.

Complaint-Handling

Article 57(1)(f) of the GDPR mandates that the DPC handle complaints "to the extent appropriate" depending on *"the subject matter of the complaint"*. Overall, the DPC concluded 2,569 formal complaints in 2025, including 1,691 complaints received prior to 2025. Of the cross-border complaints received through the Article 60 procedure, 208 were concluded, including 163 notifications of complaints amicably resolved and six decisions.

The Report confirms that when an individual brings a concern to the DPC's attention, the DPC generally engages directly with the relevant organisation, in particular with its Data Protection Officer ("**DPO**") where one has been appointed, with a view to resolving the matter. In most cases, this engagement will lead to resolution without requiring further intervention by the DPC. However, 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 the positions of both parties, as this documentation helps streamline the DPC's assessment of the matter raised by an individual.

Complaint Dismissals

During 2025, the DPC formally rejected or dismissed 53 complaints (19 non-cross-border and 34 cross-border in nature). The Report notes that the DPC dismisses cases where, upon examination of the matter, it determines that the organisation has not contravened any provision of the GDPR or the Data Protection Act 2018 ("**2018 Act**"). In this regard, in 2025, the DPC dismissed complaints concerning 'Right to be Forgotten' requests (such as requests for the delisting of articles from search engines) where public interest outweighed removal. Other complaints that were dismissed involved cases where processing of personal data for freedom of expression and journalistic purposes overrode a complainant's right to erasure. A large number of these types of cases relate to the reporting by a newspaper of proceedings related to criminal convictions passed down by the courts.

DSARs remain highest category of complaints

The highest category of complaints (42%) from individuals last year continued to concern data subject access requests ("**DSARs**"). The DPC notes that the majority of the DSAR complaints indicated an underlying non-data protection issue at their core, such as a deterioration in employer-employee relations, disputes involving financial matters or poor customer service.

While the Report notes improvements in practices across most organisations, the DPC stressed that organisations *"must do more to enhance transparency and provide individuals with fuller, more meaningful information when responding to DSARs"*. The Report notes that organisations frequently fail to adequately explain to individuals the rationale for relying on exemptions to the right of access, and applying redactions to, or withholding, certain documents. The DPC reiterates the need for organisations to prepare a schedule listing any documents being withheld or redacted, clearly setting out the reasons for doing so, and identifying the specific legislative provisions relied upon to restrict access. The Report notes that this documentation provides benefits to individual complainants, organisations, and the DPC, as it will help expedite the DPC's examination of any complaint.

The other most common complaints concerned the right to erasure (17%) and fair processing of personal data (16%). The Report notes that erasure request complaints often occurred due to a delay in response from the organisation or a lack of clear explanation as to why personal data cannot be deleted. Accordingly, the DPC recommends that organisations ensure they offer clear explanations in plain language, detailing why the data cannot be erased and how long it will be kept. The clearer the communication between an individual and an organisation, the higher the likelihood that complaints will be resolved without the need for the DPC to intervene, or through the amicable resolution process that the DPC facilitates.

Increase in Electronic Direct Marketing Complaints

In 2025, the DPC received 245 new complaints relating to electronic direct marketing, representing an increase of 24% in comparison to 2024. The vast majority of complaints related to unsolicited emails and SMS text messages. The DPC completed 275 electronic marketing investigations in 2025 (an 88% increase on 2024) and issued 50 warning letters to companies on foot of unsolicited marketing communications.

The Report stresses the need for companies to ensure their opt-out mechanisms work properly prior to commencing electronic marketing campaigns and are tested regularly to ensure they are fully functional.

Increase in Cross-Border Complaints

The DPC concluded 208 cross-border complaints (a 43% increase from 2024), with 163 amicable resolutions achieved through the Article 60 GDPR cooperation mechanism. Details of these cases can be found on the European Data Protection Board ("**EDPB**") website.

Since the implementation of the GDPR in May 2018, the DPC has received 2,189 cross-border complaints. The DPC was designated as lead supervisory authority ("**LSA**") for 1,927 (88%) of these complaints and has now resolved 79% of these complaints.

Where the DPC was LSA, 67% 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 33% of cross-border complaints were lodged with the DPC directly.

Decrease in GDPR Data Breach Notifications

The DPC received 6,521 valid data breach notifications in 2025 (5,692 were GDPR notifications). This reflects a 16% decrease on 2024. Of the breach notifications received in 2025, 85% were concluded by year-end, and 55% were either of low risk or no risk to data subject. The Report notes a number of potential reasons for the decrease in breach notifications, including an organisation improving their compliance with the GDPR or potentially as a result of an organisation deeming that certain breaches have not reached the threshold to report it to the DPC.

The Report reminds organisations of their obligation under Article 33(5) GDPR to record all personal data breaches, regardless of whether the breach has been reported to the DPC or data subjects. In this regard, the DPC states that it has commenced an initiative to examine organisations' compliance with this obligation. This initiative will provide further insight into the nature of breaches which have occurred, both those reported and not reported to the DPC.

The highest category of data breaches notified to the DPC in 2025, namely 50% of notifications, concerned correspondence sent to the incorrect recipient. The DPC attributes such errors to poor operational practices and human error. The DPC reiterates that organisations should implement clear procedures for verifying recipient details before sending correspondence containing personal data.

Increase in ePrivacy Breach Notifications

The DPC also received 731 data breach notifications under the ePrivacy Regulations (S.I. 336/2011), representing an increase of 71% on the 428 reported for 2024 and accounting for just over 11% of total valid cases notified for the year. Of these 731 notifications, 151 were deemed not to be reportable following assessment. Fewer than 1.5% of the breaches reported under the ePrivacy Regulations involved more than 100 individuals. The top types of ePrivacy breaches reported to the DPC in 2025 were:

- communications directed to the wrong recipients due to Eircodes / postal addresses being incorrectly recorded or not being updated by data subjects (35%);
- incorrect recording of details due to human error, which resulted in a breach due to communications being sent to the wrong email address or phone number (22%); and
- social engineering / phishing scams (third parties gaining access to customer accounts, including access to personal data) (34%).

The DPC considers the implementation of multi-factor authentication to be a baseline security standard when it comes to providing access to online accounts. Following the increase in unauthorised disclosure incidents arising from phishing scams in 2025 (which made up one-third of breach notifications received under the ePrivacy Regulations), the DPC intends to engage further with the telecommunications sector in 2026 in relation to the security measures they have in place.

DPC Decisions and Fines

As of 31 December 2025, the DPC had 87 statutory inquiries on-hand, including 53 cross-border inquiries and 34 domestic inquiries. In 2025, the DPC delivered 10 statutory inquiry final decisions, four of which resulted in administrative fines, amounting to a total of €530.8 million. One of these administrative fines concerned a cross-border statutory inquiry, whilst three concerned domestic statutory inquiries. The remaining statutory inquiry decisions resulted in either reprimands being imposed (discussed further below) or no infringement being found.

Large-Scale Cross-Border Inquiry Fine

TikTok was subject to the largest fine in 2025, namely a €530 million fine for breach of the transparency and data transfer rules. The DPC also ordered a suspension of TikTok's data transfers, and imposed a corrective order. This was the largest fine imposed by any EU data protection authority last year. Interestingly, in this case the suspension and corrective orders were potentially even more punitive than the fine. This is evident from the fact that TikTok sought and obtained a stay on these Orders pending its appeal against the DPC's decision. TikTok claimed that complying with these orders would cause it to incur billions of euro, and would cause significant disruption to its business and workforce.

In June 2026, the High Court upheld the DPC's infringement findings and its entitlement to impose administrative fines on TikTok, but left over the amount of the fines for further judgment, and proposed that the DPC reconsider the corrective measures that it imposed.

Domestic Inquiry Fines

The University of Limerick and the City of Dublin Education and Training Board ("**CDETB**") were respectively subject to fines of €98,000 and €125,000 following personal data breach notifications to the DPC. The fines were primarily imposed for failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, and failure to notify the DPC and data subjects within the statutory time-limit.

The Department of Social Protection ("**DSP**") was also subject to a fine of €550,000 in respect of its processing of biometric facial templates in connection with the issuance of Public Services Cards. The DPC found that the DSP had not identified a valid lawful basis for processing biometric data, and had unlawfully retained facial templates in breach of the storage limitation principle. In addition, the DSP failed to comply with its transparency obligations to data subjects, and failed to carry out an adequate Data Protection Impact Assessment ("**DPIA**").

Reprimands

The DPC imposed reprimands on four organisations in 2025, including Cubic Telecom, Yahoo EMEA Limited, Patreon Ireland Limited, and Microsoft Ireland Operations Limited. The reprimands imposed on Microsoft and Yahoo concerned insufficient transparency within their user-facing policy documents in relation to the erasure of user accounts.

DPC Fines in 2026

It is noteworthy that two fines have been issued by the DPC to date in 2026. These fines will be covered in next year's Annual Report. These fines include:

- **a €277,500 fine imposed on Permanent TSB** ("**PTSB**"), following an inquiry into a series of personal data breaches. Malicious actors posed as customers at PTSB's Open24 Contact Centre and exploited failures to adhere to security protocols, changed account details and obtained customer information, thereby exposing account holders to fraud and financial loss. The DPC found infringements of the security obligations under Articles 5(1)(f) and 32(1) GDPR and DPC breach notification obligation under Article 33(1) GDPR; and
- **a €300,000 fine imposed on the Health Service Executive** ("**HSE**"), following an inquiry into a ransomware attack at Midlands Regional Hospital Tullamore. The attack affected the personal data of approximately 84,000 individuals. The DPC found that the HSE had infringed the security obligations under Articles 5(1)(f) and 32(1) GDPR; failed to ensure agreements with third party processors included sufficient safeguards under Article 28 GDPR; failed to have a complete record of processing activities at the time of the breach; and failed to provide sufficient information to affected data subjects under Article 34 GDPR. In addition to the fine, the DPC ordered the HSE to implement specified policies and procedures to ensure appropriate security of personal data processing.

New Statutory Inquiries Commenced

In 2025, the DPC commenced three new statutory inquiries into the Children's Health Ireland ("**CHI**") at Tallaght University Hospital (concerning the physical safety and security of children's health records), TikTok Technology Limited (on the storage of EEA users' personal data on servers located in China) and X Internet Unlimited Company (regarding the use of EEA user data posted on the X social media platform for Grok AI model training). The CHI inquiry followed protected disclosures received by the DPC, while the TikTok and X inquiries were commenced on the DPC's own volition.

Enforcement and Supervision

The DPC had 1,222 supervision engagements during 2025, the majority of which were with multinational technology companies (498) and the private sector / financial services institutions (127). Of its engagements with multinational technology companies, 57% involved the DPC proactively contacting and engaging with the data controller. The Report highlights how this

proactive engagement allows the DPC to identify concerns early and to recommend mitigating or remedial actions prior to the commencement of data processing, thereby preventing potential infringements.

In 2025, the DPC dedicated additional resources to sectoral outreach and engagement, developing new relationships and reaching out to stakeholders in innovative ways. The Report notes that in 2026, the DPC aims to continue in this manner, and to improve data protection compliance by providing practical support and guidance to organisations.

DPC Engagement with Technology Companies

In 2025, the DPC engaged with a number of major technology companies in respect of their use of personal data for AI-related purposes. The Report notes that after extensive engagement, LinkedIn and Meta both implemented significant improvements to their transparency notices, data minimisation practices, and user safeguards in connection with their respective generative AI model training plans.

In relation to new AI product launches, the DPC reviewed OpenAI's ChatGPT Agent, a new agentic AI tool capable of performing multistep tasks on an individual's behalf. Following this pre-launch engagement, the DPC secured improvements to user transparency and onboarding notices prior to its EU launch in July 2025. Similarly, prior to the launch of its customer support chatbot in the EU, Etsy engaged with the DPC which led to Etsy updating its privacy policy following DPC recommendations concerning transparency around its customer support chatbot.

Compliance Sweep of Irish Retail Sector

In 2025, the DPC advanced its supervisory activities in respect of the retail sector. In this regard, it engaged directly with supermarket and convenience store controllers, building on an initial compliance sweep of the Irish retail sector in 2024. The DPC identified several notable developments in this sector, including the emergence of AI technologies for image processing in both store environments and supply chain operations, and increased use of technological solutions to reduce economic losses (such as body-worn cameras by security staff and the deployment of live CCTV monitoring displays at self-serve checkouts).

The DPC also identified a number of compliance deficiencies across the sector, including Records of Processing Activities based on UK templates that did not adequately reflect Irish processing operations, and privacy policies that failed to meet the transparency requirements of Article 13 GDPR.

The Report notes that the retail sector demonstrated significant engagement with data protection compliance, as evidenced by completing 835 DSARs under Article 15 GDPR in the 12 months preceding engagement, and conducting 215 DPIAs under Article 35 GDPR in the preceding three years.

While no concerns were raised regarding CCTV monitoring displays at self-service checkouts or the use of body-worn cameras, the DPC noted that other technologies under consideration would be subject to further review and confirmed its intention to strengthen targeted engagement and guidance in this area during 2026.

Continued Cooperation with other EDPB Supervisory Authorities

The DPC continued its engagement with its fellow EU / EEA data protection supervisory authorities. As part of this engagement, the DPC received 1,015 voluntary and formal mutual assistance requests from other European regulators.

In 2025, the DPC submitted, through the Article 60 cooperation process, 88 draft decisions, 7 final decisions, and 163 notifications of amicable resolution achieved in cross-border complaints. The DPC, as concerned supervisory authority, reviewed 158 Article 60 draft decisions or revised draft decisions from other LSAs, which represented a 40% increase in comparison to 2024. The DPC also engaged in 27 informal consultations submitted to it by peer data protection authorities in the past year.

Legislative Consultation

A key statutory function of the DPC is prior consultation on legislative measures that relate to data processing. Under both the GDPR and the 2018 Act, government departments are required to consult the DPC on any legislative or regulatory measures that will involve data processing. The DPC provided guidance and observations on 77 proposed legislative and regulatory measures.

Consumer Protection Code

The Report draws attention to the updated Consumer Protection Code, which was launched in 2025 and comes into effect in March 2026. Following feedback provided by the DPC, the Code was updated to reflect the concerns raised by the DPC regarding the retention of personal data for six years when an individual engages with a firm, but does not proceed to become a customer (eg., when a customer seeks an insurance quote). The updated Code now requires firms to retain such data for 12 months, rather than six years.

Case Studies

The DPC published a booklet of 39 case-studies from 2025 alongside the Report. These case-studies illustrate the regulatory approach taken by the DPC in regard to a range of data protection compliance issues, such as DSARs, data breaches, the right to erasure, the right to rectification, and use of CCTV. We discuss some key takeaways from these case-studies below.

DSARs

The DSAR case-studies highlight the importance of organisations being able to demonstrate they have carried out a balancing exercise before relying upon any statutory exemptions to the right of access, as any restrictions must be both necessary and proportionate. Evidence of this balancing test must be made available to the DPC, if requested. The DPC also emphasises that when organisations have concerns about the impact on third parties of disclosing mixed personal data, they should endeavour to comply with the DSAR insofar as possible, such as by providing documents in redacted format, rather than withholding records in their entirety.

The DPC further highlights that the mere fact that a large volume of records containing personal data exists, and that its review requires a large dedication of resources, is not a valid reason for refusing a DSAR under Article 12(5) GDPR. Organisations must implement appropriate organisational measures to ensure that they are in a position to respond to any data subject rights request within the statutory timeframe.

The case-studies also draw attention to the need for organisations to verify an individual's identity prior to providing them with a copy of their personal data, where reasonable doubt exists regarding same. Verification processes can often depend on the type of data which the organisation processes and the sensitivity of the data being requested.

Erasure Requests

The case-studies emphasise that the right to erasure is not absolute. Organisations may lawfully refuse an erasure request where it is required to retain the data for regulatory, professional, or liability-related reasons. Nevertheless, the DPC reiterates that organisations must still respond within the statutory timeframe. Organisations that rely on automated systems or online forms for erasure requests must conduct regular testing to ensure the technology is operational.

Although section 43 of the 2018 Act (known as the 'journalistic exemption') provides a broad exemption from compliance with a data subject's rights request to a news organisation, the DPC confirms that organisations must be able to clearly demonstrate their justification for relying on it.

Rectification Requests

In relation to the right of rectification, the case-studies emphasise that such a right is not absolute and only applies to factually inaccurate or incomplete personal data. Clinical notes and medical diagnoses are generally not subject to rectification as they reflect professional judgement at a point in time.

Nevertheless, where personal data is demonstrably inaccurate, controllers must rectify it without undue delay. Appropriate technical and organisational measures must be in place to handle rectification requests, including from non-customers.

Data Breaches

Regarding data breaches, a key takeaway from the case-studies is that security measures / features should be configured appropriately to the nature of the business (ie., having regard to the risk profile of the personal data). Organisations, including smaller enterprises, should have processes in place

to ensure personal data collected is accurate and that email systems used for transmitting personal data are secure and encrypted. The DPC notes that staff training deficiencies and insufficient monitoring of access to sensitive systems remain common causes of high-risk breaches.

Further to the Report's focus on AI, the case-studies highlight that free AI tools present an ongoing risk in the context of personal data. Organisations must create clear usage policies and ensure all staff understand their data protection obligations, particularly around uploading personal data to external tools.

CCTV

Complaints involving the use of CCTV footage featured heavily in the case-studies, which reiterated the need for organisations to have an appropriate lawful basis for using CCTV, and a reasonable retention period for CCTV footage. This lawful basis and retention period should be documented in a comprehensive CCTV policy.

The DPC notes that when operating CCTV in the workplace, controllers must ensure processing is necessary, proportionate, and transparent to data subjects, and balance employees' right to privacy with the organisation's safety and security objectives. Cameras and monitors must be positioned appropriately, with visible signage in place. In addition, a clear CCTV policy must be readily available to employees, setting out the purposes of the system, access arrangements, and retention periods.

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 any member of our Technology and Innovation Group.

Marie McGinley
Partner
t +353 86 170 6507
e marie.mcginley@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

Matheson

DUBLIN
70 Sir John Rogerson's Quay,
Dublin 2
Ireland

T: +353 1 232 2000
E: dublin@matheson.com

CORK
Penrose One,
Penrose Dock,
Cork, T23KW81
Ireland

T: +353 21 465 8200
E: cork@matheson.com

LONDON
7th Floor, Octagon Point,
5 Cheapside,
London EC2V 6AA,
UK

T: +44 20 7614 5670
E: london@matheson.com

NEW YORK
250 Park Avenue
New York,
NY 10177
United States

T: +1 646 354 6582
E: newyork@matheson.com

PALO ALTO
228 Hamilton Avenue,
3rd Floor,
Palo Alto, CA 94301
United States

T: +1 650 617 3351
E: paloalto@matheson.com

SAN FRANCISCO
95 Third Street
San Francisco
CA 94103
United States

T: +1 415 423 0540
E: sf@matheson.com