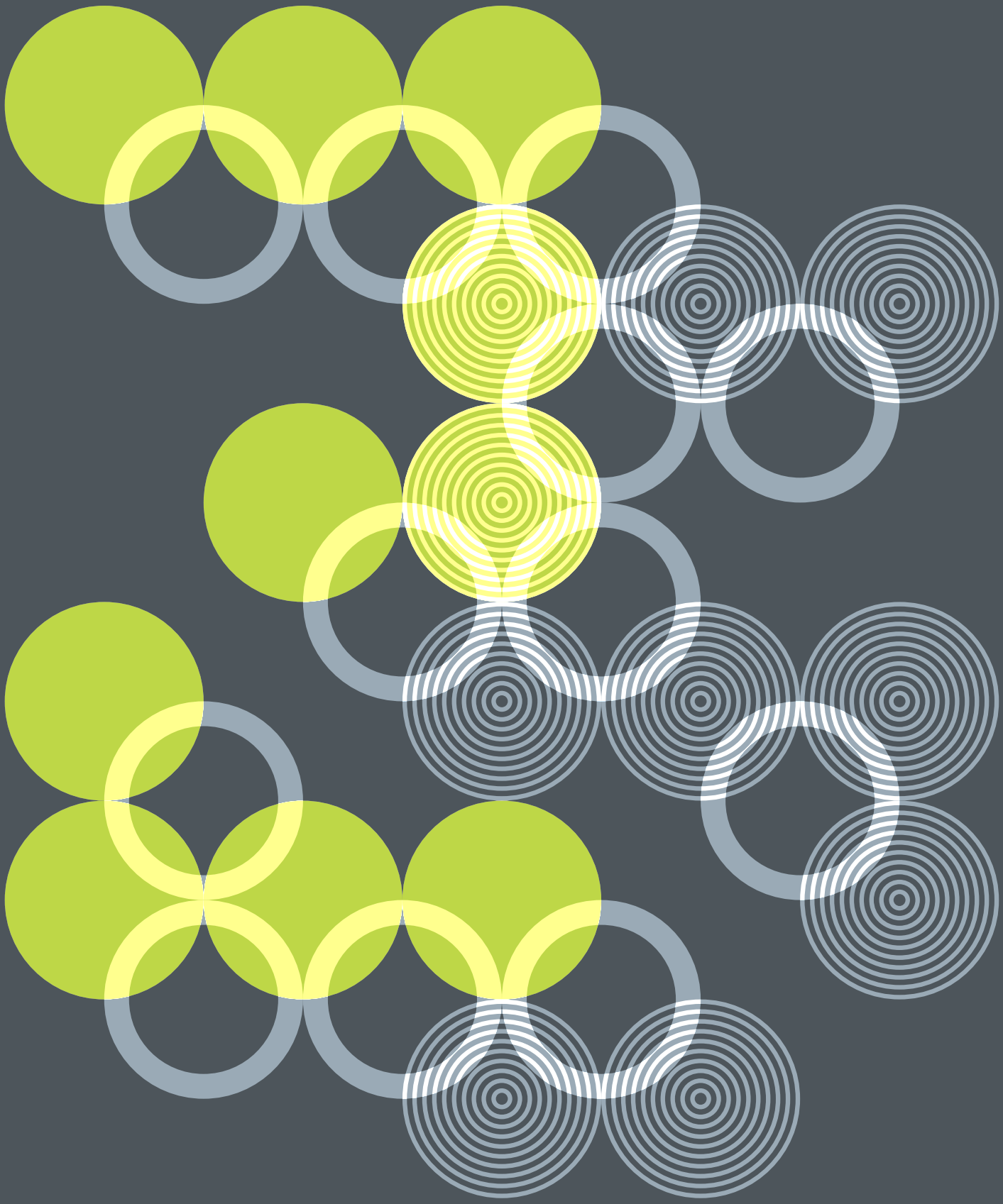


An Coimisiún um Chosaint Sonraí
Data Protection Commission

Annual Report 2025

Glossary

CSA Concerned Supervisory Authority

DPA Data Protection Authority

DPC Data Protection Commission

DPO Data Protection Officer

EDPB European Data Protection Board

GDPR General Data Protection Regulation

IMI Internal Market Information System

LED Law Enforcement Directive

LSA Lead Supervisory Authority

OSS One Stop Shop

SMC Senior Management Committee

AI Artificial Intelligence

Contents

Foreword

2025 saw an unprecedented 45% increase in complaints received by the Data Protection Commission (DPC), many of which involved the use of Artificial Intelligence (AI) by persons making complaints, adding to the volume and complexity of the documentation presented. At the same time, the scale and complexity of the use of personal data by rapidly advancing AI technologies increased significantly, with heightened risks and harms for individuals. The DPC also experienced a rise in litigation cases during the year taken by companies on foot of cross-border inquiries being initiated and concluded into their data processing activities.

Against this backdrop, a hotly debated topic throughout 2025 was the balance between technological innovation and ensuring rigorous protections for our personal data. A pervasive question was whether digital regulation was stifling innovation. The European Commission proposed a series of legislative simplification measures across various regimes including the General Data Protection Regulation (GDPR) while maintaining a consensus view that changes should not be to the detriment to European values including the fundamental right to protection of our personal data as set out in both the EU Charter of Fundamental Rights and the GDPR. In the performance of its functions, the DPC sought to uphold the view that innovation and regulation can and must co-exist in a mutually conducive balance, ensuring the right to data protection while facilitating responsible innovation.

During the year the DPC continued to discharge its mandate under the GDPR. Following the harmonised Europe-wide December 2024 European Data Protection Board opinion on Artificial Intelligence, during 2025 the DPC continued to regulate under the GDPR the training of generative AI models by the large technology firms based in Ireland. This work included close cooperation with the DPC's peer European authorities, in particular in its role as the EU Lead Supervisory Authority for the companies concerned.

In April, the DPC concluded its Inquiry into transfers of European User Data by TikTok Technology Limited to China following consensus from its peer EU regulators under the 'One Stop Shop' regulatory mechanism of the GDPR where the DPC acts as Lead Supervisory Authority.

In May, the Taoiseach and the Minister for Justice opened the new DPC offices on Pembroke Row, in Dublin. With the assistance of the OPW, the new building allowed the DPC to finally house its Dublin-based staff in one centralised modern building. In the same month, the DPC concluded its Inquiry into the use of facial matching technology in the Public Services Card.

During the year the DPC worked with its peer authorities in Europe and agreed the Helsinki Statement in July on how European data protection authorities planned to assist individuals and organisations to remain data protection-compliant through simpler guidance and increased engagement.

The DPC increased its cooperation with other digital regulators through the Digital Regulators Group, increased initiatives on advancing the safety of children and the protection of their personal data online and engaged with its European and international colleagues on multiple issues of common concern including on child safety and assurance initiatives.

In November, the DPC launched its public awareness Sharenting Campaign which was one of the most watched videos in Ireland in the past five years. The viral #PauseBeforeYouPost 'Sharenting' video was viewed world-wide and drew attention to the need to take care when sharing children's personal data on-line. The DPC deepened its engagement with bodies working on adult safeguarding, produced additional toolkits for schools and established a dedicated group comprising 20 national governing sporting bodies and local partnerships. It also deepened its work with the Irish retail sector.

In October, Niamh Sweeney was appointed as a Commissioner for Data Protection, thus completing the move from a one to three-person Commission.

The work of the DPC during 2025 could not have been achieved without the untiring commitment of the DPC's staff which increased to 295 by year end. As Commissioners we wish to acknowledge our staff who drive the DPC's mission. We also wish to acknowledge our stakeholders including the thousands of data protection officers who with us strive to ensure that the data protection rights of all persons are protected whether by government, private or voluntary organisations.

Dr. Des Hogan
Chairperson,
Commissioner for Data Protection

Timeline of 2025

Q1

Data Protection Commission (DPC) signs joint declaration on AI alongside data protection authorities from Australia, Korea, France, and the United Kingdom.

European Data Protection Board (EDPB) statement on age assurance, co-drafted by the DPC, is published.

Q2

DPC announces Inquiry into X Internet Unlimited Company (XIUC) on the processing of personal data of EU/European Economic Area (EEA) users for the purposes of generative AI model training.

DPC fines TikTok Technology Limited **€530 million** and orders corrective measures following Inquiry into transfers of EEA user data to China.

From left to right: Commissioner Dale Sunderland, Minister for Justice Jim O'Callaghan, Taoiseach Micheál Martin and Commissioner Des Hogan opening the new DPC premises on Pembroke Row in Dublin, May 2025.

Taoiseach Micheál Martin and Minister for Justice Jim O'Callaghan **open new DPC office** on Pembroke Row, Dublin.

DPC concludes investigation and issues Final Decision into facial matching technology regarding the Department of Social Protection's Public Services Card.

Final Decision published following an Inquiry into a personal data breach at the City of Dublin Education and Training Board.

Q3

DPC announces Inquiry into transfers of personal data to China following TikTok Technology Limited's discovery of an issue in February 2025 that resulted in some EEA user personal data being stored on servers located in China.

Launch of Adult Safeguarding Toolkit to protect vulnerable adults.

DPC announces Inquiry into Children's Health Ireland at Tallaght University Hospital.

DPC is shortlisted for award under the enforcement category at the 2025 Global Privacy Assembly in Seoul, Republic of Korea.

Q4

DPC, as part of the Digital Regulators' Group, launches the Short Guide to Digital Regulation.

DPC and Coimisiún na Meán sign Cooperation Agreement and issue a joint statement on Advancing the safety of children and the protection of their personal data online.

From left to right: Commissioner Dale Sunderland, Commissioner Des Hogan and Commissioner Niamh Sweeney.

Niamh Sweeney appointed as a third Commissioner for Data Protection.

DPC launches #**Pausebeforeyoupost** ad campaign about 'Sharenting' which generates over **150 million** views globally.

Deirdre O'Donovan is appointed as the DPC's Director of Legal.

DPC hosts the **Kick Start Compliance conference** in Croke Park, focusing on data protection in sport.

DPC issues Final Decision following an Inquiry into University of Limerick.

Executive Summary

Key Numbers: January 1 – December 31, 2025

New cases[1] received

16,160

representing a **45% increase** from 2024 (11,091).

Cases concluded

11,734

representing a **12% increase** from 2024 (10,510).

Cases concluded through complaint-handling

2,569

representing a **9% increase** from 2024 (2,357).

Electronic direct marketing investigations concluded

275

representing a **88% increase** from 2024 (146).

Cross-Border complaints concluded

208

representing a **43% increase** from 2024 (145).

Breach notifications received

6,521

Half of all notifications arose as a result of correspondence being sent to the wrong recipient.

Calls received

6,654

1 Cases are defined as contacts that require further engagement beyond the initial query. Cases in this instance can therefore include complaints from individuals, but also encompasses requests for advice and guidance which do not include a complaint element. This figure does not include contacts from the media, speaking invitations, breach notifications or consultation requests.

Large-Scale Inquiries concluded

4

Final Decisions

10

Provisional Decisions

92

Administrative fines imposed

€530,773,000

The largest fine was a **€530 million** penalty against TikTok Technology Limited regarding the transfer of the personal data of EU/EEA users to China. Since May 2018, the DPC has issued **€4.04 billion** in fines.

163

Notifications of amicable resolutions

were achieved through the GDPR Article 60 cooperation mechanism, representing a **41% increase** from 2024 (115).

New Inquiries

In 2025 the DPC announced the commencement of new inquiries into:

- the physical safety and security of children's health records at **Children's Health Ireland** at Tallaght University Hospital;
- transfers of EU/EEA personal data by **TikTok Technology Limited** to China; and
- use of EU/EEA user data for AI model training by **XIUC**.

Received

1,015

Article 61 GDPR Mutual Assistance Requests from other European regulators.

Participated in over

140

European Data Protection Board (EDPB) meetings.

DPC was represented on

13

EDPB subgroups.

The DPC provided input and observations on over

77

pieces of proposed national legislation.

Binding Corporate Rules

The DPC was the lead reviewing supervisory authority (SA) in relation to **13 Binding Corporate Rules** (BCR) applications from **eight different companies**, and acted as co-reviewer for other SAs on nine BCR applications from **six different companies**.

Pause Before You Post Campaign

The DPC launched a national public awareness campaign called **Pause Before You Post** which highlighted the risks associated with **'sharenting'** – i.e. the habitual sharing of children's personal information, photos, and videos online by parents.

Since its publication, the campaign has reached a wide audience.

Pause Before You Post

The campaign generated over

150 million

views globally.

45 million

views across the DPC's social channels.

New Guidance

Several new pieces of guidance were also published by the DPC in 2025, including:

An Adult Safeguarding Toolkit to support organisations dealing with the personal data of vulnerable adults.

A Short Guide to Digital Regulation which was created in collaboration with the other members of the Digital Regulators' Group – Coimisiún na Meán, ComReg and the Competition and Consumer Protection Commission – to clarify common queries in the digital regulation space in Ireland.

An online resource for schools which supports them in taking a proportionate and compliant approach to personal data processing.

A series of infographics focusing on data protection in sport.

Sharenting – Top Tips – an online resource offering practical tips to limit the risks posed when parents share or post data about their children's lives online.

The DPC's handling of Subject Access Requests – guidance for data controllers as to how to appropriately respond to a Subject Access Request made under Article 15 of the GDPR.

Staff of the DPC presented at over

100

speaking events in 2025, both nationally and internationally.

Mission, Vision and Values of the DPC

Mission

The DPC's mission is to uphold the consistent application of data protection law through engagement, supervision and enforcement, and driving compliance with data protection legislation. The DPC safeguards the data protection rights of individuals and provides clarity for the organisations it regulates by:

- educating stakeholders on their rights and responsibilities;
- taking a fair and balanced approach to complaint handling;
- communicating extensively and transparently with stakeholders;
- participating actively at European Data Protection Board level to achieve consistency;
- cultivating technological foresight, in anticipation of future regulatory developments;
- sanctioning proportionately and judiciously; and
- retaining and developing the expert capacities of its staff to ensure operational effectiveness.

Vision and Values

The DPC is committed to being an independent, fair and consistent regulator of EU data protection law; regulating with clear purpose, trusted by the public, respected by our peers and effective in our regulation. The DPC applies a risk-based regulatory approach to its work, so that its resources are prioritised on the basis of delivering the greatest benefit to the maximum number of people. The DPC is a rewarding and challenging place to work, with a focus on retaining, attracting and allocating the most appropriate people to deliver on its mandate, recognising the value and capacities of its staff as its most critical asset.

In the conduct of its duties, the DPC is committed to act always in a way that is:

- **Fair**
- **Expert**
- **Consistent**
- **Transparent**
- **Accountable**
- **Forward Looking**
- **Engaged**
- **Independent**
- **Results-driven**

The DPC's internal values focus on promoting a work culture of trust and respect, where staff feel valued, informed, and confident that decisions are fair and transparent, with strengths encouraged and areas for development supported. The goal is to ensure empathy and understanding among colleagues with opportunities for learning, growth, and advancement accessible to all, fostering equality, diversity and inclusion. Building a workplace that prioritises fairness, friendliness, and collaboration, where innovation is welcomed and supported all form part of the DPC's internal culture.

Regulatory Strategy

The DPC's Regulatory Strategy for 2022-2027 sets out how the DPC delivers on its mandate to uphold the fundamental right to data protection. The Strategy, and the work that flows from it, has been based around five interconnected pillars of equal priority.

1. Regulate consistently and effectively
2. Safeguard individuals and promote data protection awareness
3. Prioritise the protection of children and other vulnerable groups
4. Bring clarity to stakeholders
5. Support organisations and drive compliance

The Strategy is arranged according to fundamental goals, underpinned by the DPC's mission, vision and values, which collectively contribute to the delivery of its strategic priorities.

Roles and Responsibilities

1.

1. Roles and Responsibilities

Functions of the DPC

The right to the protection of personal data is set out in EU law in the EU Treaties and in the EU Charter of Fundamental Rights. The DPC is the national independent authority in Ireland responsible for upholding this fundamental right. The DPC is tasked with monitoring the application of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). The DPC also has functions relating to other regulatory frameworks, including the Irish ePrivacy Regulations (2011) and the EU Directive known as the Law Enforcement Directive (LED). The statutory functions of the DPC are as established under the Data Protection Act 2018, which gives further effect to the GDPR and to the LED.

The core functions of the DPC, under the GDPR and the Data Protection Act 2018 include:

- driving improved compliance with data protection legislation by controllers and processors;
- handling complaints from individuals in relation to potential infringements of their data protection rights;
- conducting inquiries and investigations into potential infringements of data protection legislation;
- promoting awareness among organisations and the public of the risks, rules, safeguards and rights incumbent in the processing of personal data;
- co-operating with data protection authorities in other EU Member States on mutual issues, involving cross-border processing of personal data; and
- acting as EU Lead Supervisory Authority for data controllers with their main establishment in Ireland.

The **ePrivacy Regulations** concern the processing of personal data in the context of electronic communications such as electronic direct marketing.

The **Law Enforcement Directive (LED)** applies to the processing of personal data by bodies with law-enforcement functions in the context of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties.

In addition to its functions under the GPDR, the DPC continues to perform its regulatory functions under the **Data Protection Acts 1988 and 2003**, in respect of any complaints that relate to the period before 25 May 2018 (when the GDPR came into force), as well as in relation to certain limited other categories of processing, irrespective of whether that processing occurred before or after 25 May 2018.

Funding and Administration—Vote 43 (Previously Vote 44)

The DPC is funded by the Exchequer and does not derive monetary gain from fines imposed. On confirmation by the Courts, administrative fines imposed by the DPC are remitted to the central exchequer. The Chairperson of the Commission is the Accounting Officer for the Commission's Vote, Vote 43.

The DPC's 2025 funding was **€29.12 million**, of which €19.357 million was allocated for pay related expenditure, and €9.763 million was allocated to non-pay expenditure.

The funding for 2025 represented an increase of approximately **€1 million** on the 2024 allocation.

2.

DPC Senior Team

The DPC Senior Management Team from left to right: David Murphy, Cathal Ryan, Diarmuid Goulding, Jennifer Dolan, MB Donnelly, Deirdre O'Donovan, Niall Cavanagh, Dale Sunderland, Dr. Des Hogan, Ian Chambers, Gráinne Duffy, Labhras Sammin, Sandra Skehan and Cian O'Brien. Not in photograph: Andrew Carroll, Graham Doyle, Elizabeth Finn, Gráinne Hawkes, Sarah Lea, Ultan O'Carroll, and Niamh Sweeney.

2. DPC Senior Team

The DPC's Senior Management Committee (SMC) comprises the Commissioners for Data Protection, Directors and Principal Officers.

The Commissioners and members of the SMC oversee the proper management and governance of the organisation, in line with the principles set out in the Corporate Governance Standard for the Civil Service (2015).

The SMC has a formal schedule of matters for consideration and decision, as appropriate, to ensure effective oversight and control of the organisation.

During 2025, the SMC comprised:

Dr Des Hogan
Chairperson, Commissioner for Data Protection;

Dale Sunderland
Commissioner for Data Protection;

Niamh Sweeney
Commissioner for Data Protection (from Q3 2025);

Cian O'Brien
Director and Deputy Commissioner with responsibility for Large-Scale Inquiries including Investigations & Cross-Border Complaints;

Deirdre O'Donovan
Director and Deputy Commissioner, with responsibility for Legal (from Q3 2025);

Andrew Carroll
Deputy Commissioner, Head of Large-Scale Inquiries & Investigations Team 2;

Niall Cavanagh
Deputy Commissioner, Head of Large-Scale Inquiries & Investigations Team 1;

Ian Chambers
Deputy Commissioner, Head of Frontline, Breaches, Complaints and Information;

Jennifer Dolan
Deputy Commissioner, Head of Inter Regulatory Affairs & ePrivacy Prosecutions;

MB Donnelly
Deputy Commissioner, Head of Strategy, Finance, Governance and Risk;

Graham Doyle
Deputy Commissioner, Head of Corporate Affairs, Media & Communications;

Gráinne Duffy
Deputy Commissioner, Head of People and Learning;

Elizabeth Finn
Deputy Commissioner, Head of Cross-Border Complaints & Inquiries;

Diarmuid Goulding
Deputy Commissioner, Head of Large-Scale Inquiries & Investigations Team 3;

Gráinne Hawkes
Deputy Commissioner, Head of EDPB/ International Affairs & AI Act;

Sarah Lea
Deputy Commissioner, Head of Legal Affairs (from Q2 2025);

David Murphy
Deputy Commissioner, Head of Consultation & Supervision Team 1;

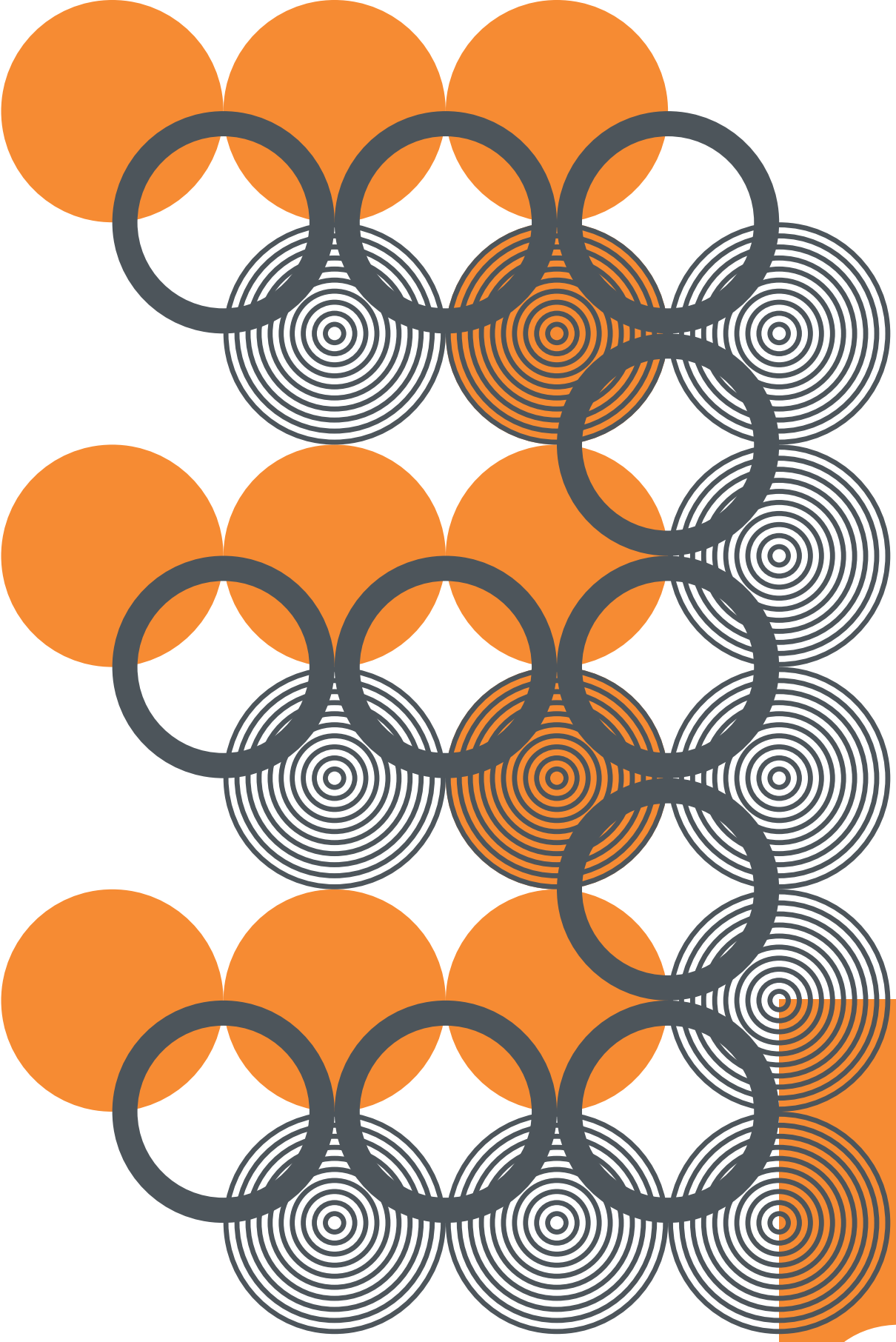
Ultan O'Carroll
Deputy Commissioner, Head of Regulatory Technology Affairs;

Fleur O'Shea
Deputy Commissioner, Head of Legal Affairs (until Q2 2025);

Cathal Ryan
Deputy Commissioner, Head of Consultation & Supervision Team 2;

Labhras Sammin
Deputy Commissioner, Head of Enterprise & ICT Operations; and

Sandra Skehan
Deputy Commissioner, Head of National Complaint Handling & Inquiries including Access Requests, LED, Breach & Processing.

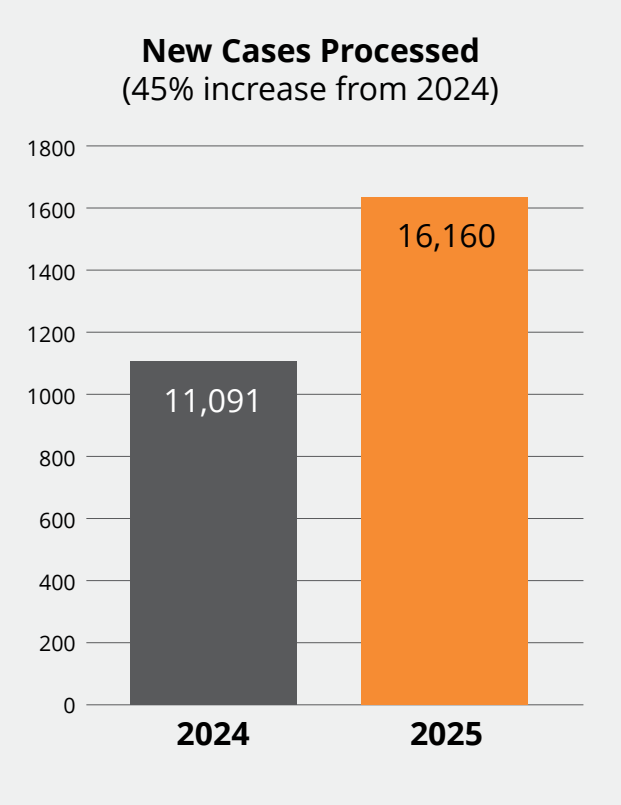


Cases and Complaints

3.

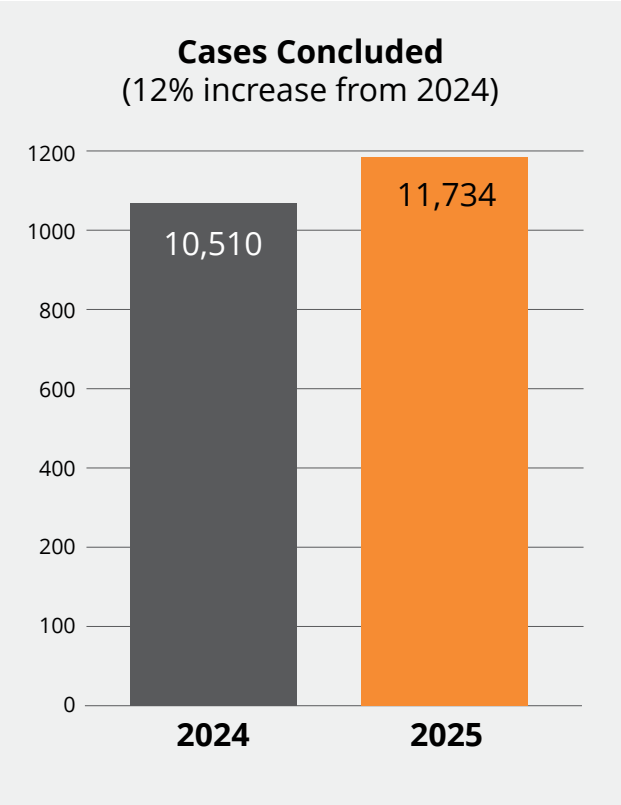
3. Cases and Complaints

In 2025, the DPC experienced its busiest year to date, with the DPC receiving **16,160** new cases[2]. This represents a **45% increase** on the number of cases received in 2024 (11,091). October 2025 was the busiest month ever recorded with **1,879** cases logged.



In total, the DPC responded to **more than 6,500** calls from individuals and organisations, of which **85%** were from individuals.

A total of **11,734** cases were concluded in 2025, representing a **12%** increase on the number of concluded cases in 2024. **9,435** of concluded cases were received in 2025.



The most common issues raised through email and webforms concerned non-responses to Subject Access Requests, concerns relating to the processing of personal data, and issues relating to social media accounts, many of which fell outside the scope of the GDPR. Telephone contacts reflected similar trends. Callers most frequently sought advice on concerns regarding the processing of their personal data or guidance on making a Subject Access Request.

2 Cases are defined as contacts that require further engagement beyond the initial query. Cases in this instance can therefore include complaints from individuals, but also encompasses requests for advice and guidance which do not include a complaint element. This figure does not include contacts from the media, speaking invitations, breach notifications or consultation requests.

Top Queries to the DPC in 2025

1. **Individuals seeking guidance on non-response to Subject Access Requests.**
2. **Processing of personal data.**
3. **Social media accounts.**
4. **How to make a Subject Access Request.**
5. **Domestic CCTV.**
6. **Organisations seeking specific guidance regarding GDPR legislation.**
7. **Breaches/breach notification.**

When individuals contact the DPC raising a concern, the DPC generally engages directly with the organisation involved, specifically the organisation's Data Protection Officer (DPO) where one has been appointed.

This engagement typically leads to resolution without requiring further intervention by the DPC. In situations where escalation is necessary, it is invaluable for the DPC to have access to written correspondence between the individual and the organisation, detailing the issue and the positions of both parties. This documentation helps streamline the assessment of a matter raised by an individual.

Exercising of rights under the GDPR and the use of Artificial Intelligence (AI) tools.

During 2025, the DPC observed an increase in individuals using AI tools to assist them exercise their data protection rights. While AI tools can assist individuals in drafting clear and well-structured correspondence, the DPC recommends caution with regards to any inputting of personal data when using these tools.

Individuals should also exercise caution when using AI 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.

Complaints

Of the **16,160 new cases**[3] received in 2025, **3,385** progressed to the complaint-handling process. This represents a **27%** increase on the number of cases progressing to the complaint-handling process during 2024.

Overall, the DPC concluded **2,569** complaints in 2025. This included **1,691** complaints received prior to 2025 and represents a **9% increase** on the 2,357 complaints concluded in 2024.

Complaints received under the GDPR: Top 3 Issues in 2025 (75% of overall cases)	**% of total**
Subject Access Request	42%
Right to erasure	17%
Fair processing	16%

Subject Access Rights

Article 15 of the GDPR provides that an individual may obtain from an organisation sufficient, transparent, and easily accessible information about the processing of their personal data so that they can be aware of and verify the lawfulness of the processing and the accuracy of the processed data. The right of access is one of the fundamental rights conferred on individuals by the GDPR. By the end of 2025, the DPC had received **1,280** complaints solely related to the right to access, accounting for **42%** of all complaints received through the year.

As in previous years, alleged noncompliance with Subject Access Requests remains the primary source of complaints to the DPC. A review of these complaints indicates that the majority of the complaints received have underlying issues at their core, such as, a deterioration in an employer–employee relationship, disputes involving financial matters, or situations that effectively began as poor customer service rather than a particular data protection concern.

The DPC continues to observe that organisations must do more to enhance transparency and provide individuals with fuller, more meaningful information when responding to Subject Access Requests. Although the DPC has noted improvements in practices across most organisations, challenges remain.

Subject Access Request Tips

Where organisations rely on exemptions when responding to a Subject Access Request, they frequently fail to clearly explain to the individual the rationale for applying those restrictions.

Organisations are not adequately documenting how and why they reach particular determinations when assessing a Subject Access Request. Organisations should prepare a schedule listing any documents being withheld or redacted, clearly setting out the reasons for doing so and identifying the specific provisions of the 2018 Act or the relevant GDPR articles relied upon to restrict access. This information should then be communicated to the individual in a clear, concise, and transparent manner as part of the response to their Subject Access Request.

3 Cases are defined as contacts that require further engagement beyond the initial query. Cases in this instance can therefore include complaints from individuals, but also encompasses requests for advice and guidance which do not include a complaint element. This figure does not include contacts from the media, speaking invitations, breach notifications or consultation requests.

Once a complaint has been submitted to the DPC, an organisation's ability to clearly demonstrate the analysis underpinning its decision-making process will help expedite the DPC's examination of the matter. This provides benefits to organisations, individuals, and the DPC alike. Where responses are comprehensive and exemptions have been appropriately and reasonably applied, such cases may be suitable for progression through the DPC's fasttrack complaint assessment and early-resolution unit.

Right to Rectification

Article 16 of the GDPR provides for the rectification of personal data where the personal data that is being processed is inaccurate, or, taking into account the purposes of processing, the data is incomplete in some way.

Organisations are obliged to rectify inaccurate personal data when it becomes apparent, whether through their own processes or following a request from an individual. If personal data is identified as inaccurate as a matter of fact, or incomplete, the organisation must take steps to amend this by correcting or completing the personal data. If an organisation is unable to correct it directly, it may, where appropriate, meet its obligations by adding a supplementary statement to clarify and rectify the inaccuracy.

The right to rectification applies, in particular, to matters of fact, which are often misinterpreted. A 'matter of fact' refers to information that can be objectively proven true or false. The right is usually not applicable to requests where the subject matter relates to an opinion or subjective assessments (unless the factual basis of the opinion is incorrect).

Right to Rectification Examples

The opinion of medical professionals is often the subject matter of rectification requests submitted as complaints to the DPC which is not rectifiable. The DPC often receives complaints where the individual complaint relates to historical medical opinions or diagnoses contained within a patient's records. While a diagnosis may subsequently be revised or updated as new information becomes available, this does not render the original diagnosis factually inaccurate or subject to rectification. A diagnosis should be understood as a point-in-time assessment, reflecting the professional judgement of the healthcare provider based on the information available at that specific moment.

Even where underlying clinical information evolves, leading to a different opinion or diagnosis at a later stage, the original record remains an accurate account of what was assessed and recorded at that time. Accordingly, it is factually correct to retain both the existence of the original opinion or diagnosis and its content as part of the medical record. In such circumstances, the data cannot be considered inaccurate, as it faithfully represents a contemporaneous professional assessment. Therefore, the right to rectification is unlikely to apply where the information in question constitutes an accurate historical record.

Another reason a medical opinion or diagnosis is likely not open to rectification is that it provides important context for any subsequent medical treatment decisions made by a healthcare provider. A prior opinion or diagnosis may explain why certain medications were prescribed or certain treatment plans adopted. Maintaining these records is not only required as a matter of law, it serves the public interest by ensuring the individual and the treating professional have a

reliable record of what has taken place. If a medical record is not open to rectification, it may still be possible for a supplementary statement to be attached to the medical record outlining where the individual believes the data is inaccurate or incomplete.

In one case dealt with by the DPC the use of the words 'multiple carers' in a report was requested to be rectified, on the basis that the complainant believed it suggested that they placed a child in the care of multiple people, which was disputed. The individual was of the opinion that it would not be in the interest of the child or their family to have such wording documented in a report. The DPC determined that the use of the term 'multiple carers' was accurate as to a matter of fact as it reflected the organisation's involvement with the child at a point in time, specifically that the child was being cared for by medical professionals. The complainant's belief that an individual reading the report may make a certain assumption about them, owing to the use of the words 'multiple carers', amounted to a disagreement between the complainant and the organisation, and therefore did not meet the Article 16 requirements.

Further examples related to cases the DPC has examined are available in the Case Studies Booklet relating to a rectification request relating to a report which had been ordered by the Irish Circuit Court and a rectification request that was submitted to a taxation authority.

Erasure Requests

Individuals have the right to ask an organisation to delete their personal data. This is known as the 'right to erasure'. This is not an absolute right and applies only in certain situations, such as when an organisation no longer needs the data, consent has been withdrawn, or where the data was used unlawfully.

Erasure requests are among the most common issues raised with the DPC, accounting for **17%** of all complaints. Often complaints occur due to a delay in response from the organisation or a lack of clear explanation as to why the data cannot be deleted.

Erasure Request Tips

Organisations should ensure they offer clear explanations in plain language, detailing why data cannot be erased and how long it will be kept. Clear communication between individuals and organisations often resolves issues early, mitigating the need for the DPC to intervene.

Complaint Handling

The DPC processes complaints under four main legal frameworks:

- General Data Protection Regulation (GDPR), which has been given further effect by the Data Protection Act 2018 (2018 Act);
- Law Enforcement Directive (LED), which has been transposed into Irish law by Parts 5 and 6 of the 2018 Act;
- Data Protection Acts, 1988 and 2003; and
- S.I. 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.

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'. Under section 109(1) of the 2018 Act, '*the Commission shall examine the complaint, to the extent appropriate, and shall, in accordance with this section, take such action in respect of it as the Commission, having regard to the nature and circumstances, considers appropriate*'. Accordingly, once a concern has been assessed as a complaint—namely that the matter relates to the processing of the individual's personal data; that there may have been a potential infringement of the individual's data protection rights and it has been established that the DPC is the appropriate authority to examine the complaint—the complaint progresses to a complaint handling unit and an examination is conducted in accordance with the legislative requirements.

In 2025, the DPC received an unprecedented volume of cases, with an increase of **45% in total cases** received when compared against 2024. This has had a direct impact on the DPC's response times and case-handling timeframes. The DPC continued to implement measures to streamline its case-handling processes. When engaging with both individuals and organisations, the DPC will be specific about the information/ supporting documents it requires to examine queries and complaints to avoid it having to issue repeated requests for information or documentation from parties which can hinder the complaint handling process and leads to frustration between the parties.

Site Visits

In cases where data controllers have not responded to a rights request or fail to engage with the DPC in the examination of a complaint, the DPC routinely carries out site visits to premises. This is undertaken to determine whether the organisation or business remains operational, in order to highlight to smaller businesses what their responsibilities are under the GDPR, or to ensure receipt of documents prior to considering use of enforcement powers.

In 2025, a total of **13 site visits** were conducted with organisations who had failed to engage with the DPC's complaint process or who had failed to respond to a rights request. The premises visited included restaurants, a GP's surgery, a solicitor's office, and the business premises (CRO registered addresses) of a number of sole traders. In some cases, the visits confirmed that a business was no longer operational. In other cases, it resulted in co-operation from the business owner when their responsibilities under GDPR were explained to them. Site visits included cases where the DPC confirmed a record of the personal data sought was not processed at all or any longer.

Complaint Outcomes

The outcome of a complaint depends on whether the processing in question is of a cross-border nature.

In many cases, both during the initial review and throughout the examination process, complaints can be resolved through the provision of information and guidance by the DPC, including clarification of relevant aspects of data protection law. A significant number of complaints are also amicably resolved following DPC intervention, for example where organisations are reminded of their obligations or directed to published DPC or EDPB guidance to ensure individuals' data protection rights are upheld. This can often be the optimal outcome for an individual, where the subject matter raised does not pose a risk to the individual, or where a misunderstanding or miscommunication between the parties has led to the matter being referred to the DPC in the first instance.

With regard to cases which are determined not to be related to cross-border processing which have not been amicably resolved, section 109(5) of the 2018 Act applies. This section sets out the grounds under which the DPC may conclude a complaint outside of an inquiry process. These grounds include: rejecting or dismissing a complaint where no infringement is found; the issuing of advice to a complainant regarding the subject matter of the complaint; the issuing of enforcement notices compelling a controller to comply with a right that has been exercised; the issuing of a reprimand; or any other action that the DPC deems appropriate taking into consideration factors related to the complaint and any mitigating actions the controller has taken during the examination of the complaint.

Where the DPC identifies a minor infringement of data protection legislation that presents a minimal risk to the individual, the DPC may issue advice or instructions to the controller regarding their current practices, procedures or the manner in which they have engaged with the complaint, with the aim of promoting improved compliance.

Complaint Dismissals

During 2025, the DPC formally rejected or dismissed **53** cases: 19 non-cross-border and 34 cross-border in nature. It is sometimes the case that individuals contact the DPC raising issues that are not related to their data protection rights, or equally where they believe that data protection legislation will resolve an entirely unrelated issue.

The DPC triages such cases, providing information as to the extent and limitations of GDPR rights, and rejects or dismisses cases as required in order to ensure that the resources of the office are applied to cases where greater risk to individuals is apparent and to which the GDPR applies.

The DPC dismisses cases where, upon undertaking an examination of the subject matter of the complaint, determines that the organisation to which the complaint relates has not contravened any articles under the GDPR or the 2018 Acts. In this regard, in 2025 the DPC dismissed cases related to complaints against both public and private companies, including:

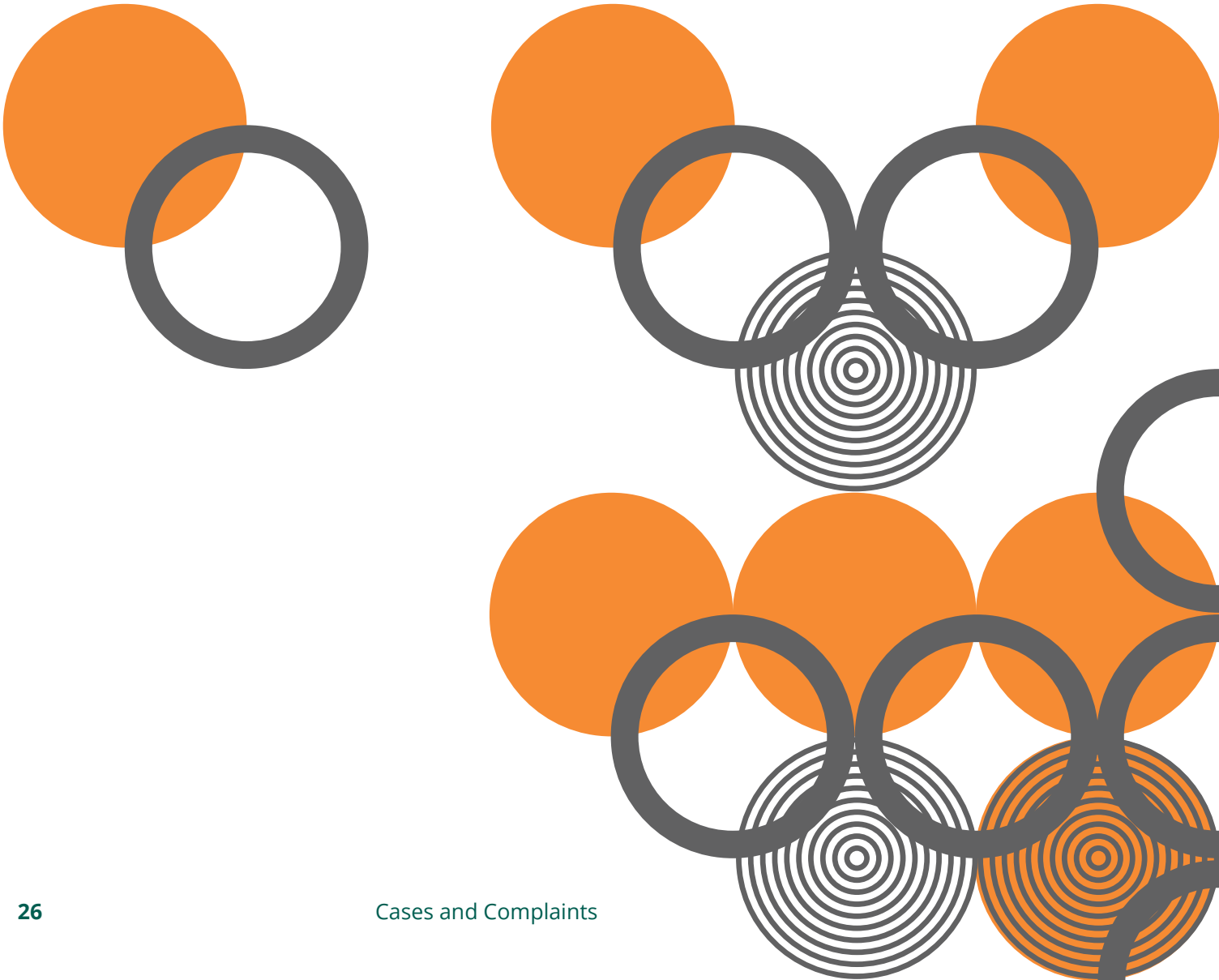
- cases related to the 'Right to be Forgotten', where individuals sought to have specific articles delisted from search engines. In many cases the DPC found it to be in the public interest for those articles to remain available, outweighing the right of the individual to have same removed;

- cases related to employment disputes and investigations resulting from same, where the details of the investigations were shared with individuals to whom the complaints related to; and

- cases where the processing of personal data for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes, was determined to override a complainant's right to erasure of specified articles relating to them. A large number of these type of cases relate to the reporting by a newspaper of proceedings related to criminal convictions passed down by the courts.

Reprimands

Reprimands are a reactive corrective measure that can be and are used by the DPC. A reprimand is a formal, written corrective power issued by the DPC to a controller (or processor) in circumstances where the DPC considers that the data processing has infringed the 2018 Act and/or the GDPR. A reprimand serves as an official, formal statement of disapproval indicating that an organisation has not complied with its regulatory obligations. Reprimands serve as a public record of non-compliance and form part of the assessment for potential future, more severe enforcement action.



Case Study: DPC issues a reprimand to the Irish Prison Service

The DPC received a complaint from an individual against their employer, the Irish Prison Service, in relation to its use of video surveillance systems in the workplace. Whilst the individual acknowledged that their image was captured on the CCTV cameras due to the high-risk environment of their workplace, they did not believe that it was appropriate to use the system's cameras for other purposes, such as monitoring employee attendance. The Irish Prison Service stated that it relied on the individual's employment contract as the basis for this processing, which would generally be consistent with Article 6(1)(b) of the GDPR.

Article 5(1)(a) of the GDPR sets out the requirement for organisations to be transparent and fair in how personal data is processed. In this regard, the DPC reviewed the Irish Prison Service's CCTV Policy and noted that it stated: *'CCTV footage and audio where it is reasonably required to assist in the establishment of facts in an investigation',* e.g. a disciplinary investigation. When personal data is processed for health and safety purposes in high-risk working environments, via CCTV, this would generally be accepted as being lawful by the DPC.

However, in these circumstances, the Irish Prison Service was also required to demonstrate that its processing of personal data, specifically the monitoring of the individual's movements by CCTV cameras, was necessary and proportionate regarding the scope of its investigation in circumstances where the complainant had admitted to the issue at the centre of a disciplinary matter. The Irish Prison Service did not provide any supporting evidence in this regard. The DPC therefore determined that the Irish Prison Service failed to demonstrate: why it was necessary or proportionate to monitor the individual's movements using its CCTV cameras; how its use of the CCTV footage, in a disciplinary process, was in line with its own CCTV Policy, and; an appropriate lawful basis under Article 6 of the GDPR.

The DPC concluded that the Irish Prison Service infringed its obligations to ensure that its processing activities were carried out transparently, fairly and lawfully. The DPC issued the organisation with a reprimand under section 109(5) (da) of the Data Protection Act 2018.

KEY TAKEAWAY:

Prior to processing personal data, an organisation should first establish: the reason(s) why they need to process personal data; if these reasons could be satisfied without the use of personal data, and if the individual has been informed that their personal data will be processed in this manner. An organisation's use of personal data should be clearly defined from the outset and it must not further process that personal data for other incompatible reasons. It is an organisation's responsibility to ensure that it is in a position to demonstrate that its processing activities are being carried out lawfully, fairly and transparently, as required under Article 5(2) of the GDPR.

Case Study: Reprimand issued to a telecommunication's provider – Vodafone

The DPC received a complaint against Vodafone and Vodafone's Intelligent Solutions (hereinafter called 'the IS provider'). In the complaint, the complainant alleged that Vodafone unlawfully processed their email address.

In 2021, the complainant notified Vodafone that their personal data (i.e. email address) had been erroneously added to a third-party customer's account and requested that Vodafone restrict the processing of their email address, as they were not a customer. Vodafone did not action the complainant's rectification request made under Article 18 of the GDPR for two years.

Due to Vodafone's failure to action the complainant's rectification request for two years, the complainant felt compelled to submit an erasure request under Article 17 of the GDPR in 2023 to Vodafone. Vodafone complied with this request within the required timeline of one month in compliance with Article 17. However, it should be noted that if Vodafone had appropriately actioned the complainant's original rectification request raised back in 2021, it would not have required the complainant to submit an erasure request in 2023.

Furthermore, over the course of four months the complainant submitted five Subject Access Requests including a number of Article 15(1) questions under Article 15 of the GDPR to the IS provider. The IS provider, as the Data Processor, should have made Vodafone aware that it had received these requests from the complainant and Vodafone, as the Data Controller, should have provided the response to these Article 15 requests. However, the IS provider failed to make Vodafone aware of the requests it had received from the complainant and as a result, the complainant's multiple requests were not responded to by Vodafone or the IS provider. Vodafone recognised that its technological and organisational processes had fallen short in this case.

The DPC found that Vodafone failure to respond to the original rectification request and the five Subject Access Request's, within the timeframe as per its obligations under Article 12(3) of the GDPR and Article 12(4) of the GDPR, demonstrated a systemic failure to adhere to its obligations as a Data Controller as set out in data protection legislation.

KEY TAKEAWAY:

When an individual notifies a data controller that their personal data has inaccurately been included in a customer's account and requests rectification, the data controller is obliged to rectify the inaccurate personal data as per their obligations under Article 18 of the GDPR.

Data controllers are required to have appropriate processes in place to ensure any rectification requests are actioned and a response given in a timely manner, in accordance with Article 12(3) of the GDPR.

Due to the inaction and lack of appropriate processes within the Data Processor's systems, the complainant in this case study felt required to make five Subject Access Requests under Article 15 of the GDPR to ascertain who had access to their personal data over the two-year period where the Data Controller unlawfully processed their personal data.

Both Data Controller and Data Processor in this case failed to respond to any of the complainant's access request's and when questioned by the DPC, failed to acknowledge the seriousness of the failure of its organisational measures, which led to the DPC issuing a reprimand on concluding its examination into this complaint.

Complaint-Based Cross-Border Reprimand Case Studies can be found on pages 49-55 of this report. Other complaint Case Studies are being published separately to this report.

EDPB Key Concepts Project

During 2025, the DPC, alongside all other European data protection authorities, has been engaged in a project to align statistical and workload reporting throughout the EEA. This project, launched by the European Data Protection Board, aims to collect data on all data protection authorities' activities across members in a uniform way. Further information on the EDPB Key Concepts Project can be found on page 104 of this report.

Electronic Direct Marketing Complaints

The DPC investigates offences relating to electronic direct marketing under S.I. 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ('the ePrivacy Regulations'). The ePrivacy Regulations implement Directive 2002/58/EC ('the ePrivacy Directive') into Irish law.

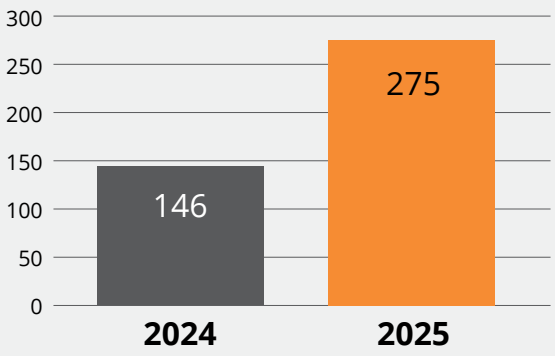
In 2025, the DPC received **245 new complaints** about electronic direct marketing, representing an **increase of 24%** on the 2024 figure. Of these 245 complaints, **73%** related to unsolicited emails, and **11%** to unsolicited SMS text messages.

275 electronic direct marketing investigations were concluded in 2025. This represents an **88% increase** on the figure reported for 2024.

This concluded figure of 275 comprises:

- **9** complaints from 2023;
- **72** complaints from 2024; and
- **194** complaints from 2025.

Electronic Direct Marketing Complaints Concluded
(88% increase from 2024)



The most frequently reported electronic direct marketing issues involved:

- Marketing communications being sent to individuals without a functional opt-out mechanism. This included instances where:
  - the opt-out request was ignored by the organisation;
  - the opt-out mechanism was not working correctly; or
  - a mechanism was not provided at all.
- Marketing communications being sent without the individual's explicit consent (and where no exemptions under the regulations were applicable).

In 2025, the DPC issued **50 warning letters** to companies on foot of unsolicited marketing communications.

Organisations must ensure that when consent is sought for marketing purposes, that this consent be clearly distinguishable and not 'bundled' in with other requests for consent. Organisations must also ensure that their opt-out procedures work properly and are tested regularly to ensure their functionality.

One-Stop-Shop Complaints

The One-Stop-Shop (OSS) mechanism was established under the GDPR to streamline how organisations operating across multiple EU Member States interact with data protection authorities (referred to as 'supervisory authorities' under the GDPR). The OSS enables such organisations to be overseen by a single Lead Supervisory Authority (LSA), based on the location of their 'main or single establishment', rather than being subject to separate regulation by the data protection authorities of each member state.

An organisation's main or single establishment is typically its place of central administration and/or the location where key decisions about data processing are made within the EU/EEA. Under the OSS, the supervisory authority that receives a complaint acts as a Concerned Supervisory Authority (CSA). The CSA serves as the intermediary between the LSA and the individual. This means that an individual in any EU/EEA country may submit a complaint either directly to the LSA or to their local/national authority, which will then forward it to the LSA. Through this mechanism, the DPC fulfils its role as a regulator for EU citizens.

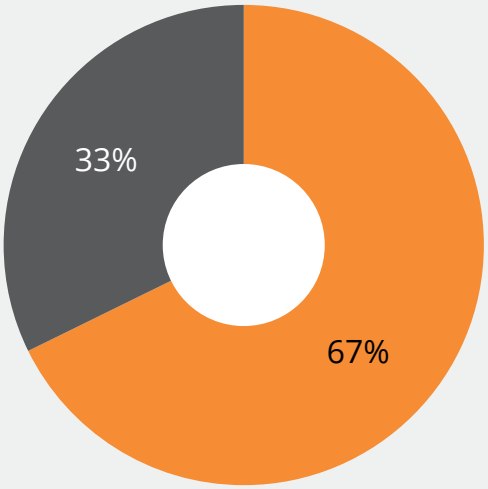
Since the implementation of the GDPR, the DPC has received a total of **2,189** cross-border complaints. The DPC has been established as the Lead Supervisory Authority for **1,927** (**88%**) of these complaints.

1,519 (**79%**) of the valid cross-border complaints, for which the DPC is the LSA, have now been concluded.

Since May 2018, **67%** of cross-border complaints, where the DPC is the LSA, were lodged by complainants with another EU/EEA supervisory authority and then transferred to the DPC via the OSS mechanism. **33%** of cross-border complaints were lodged with the DPC directly.

In 2025, the DPC received **315** valid cross-border complaints, relating to companies for whom the DPC is the LSA. By year end, the DPC had concluded **208** cross-border complaints representing a **43%** increase on the 2024 figure. A total of 34 cross-border cases were rejected or dismissed in 2025.

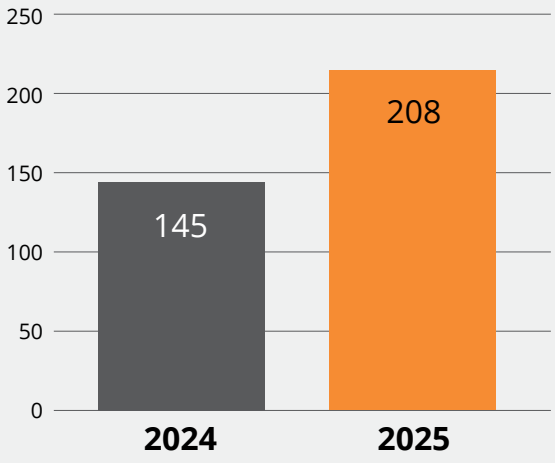
Cross-Border Complaints where DPC is LSA



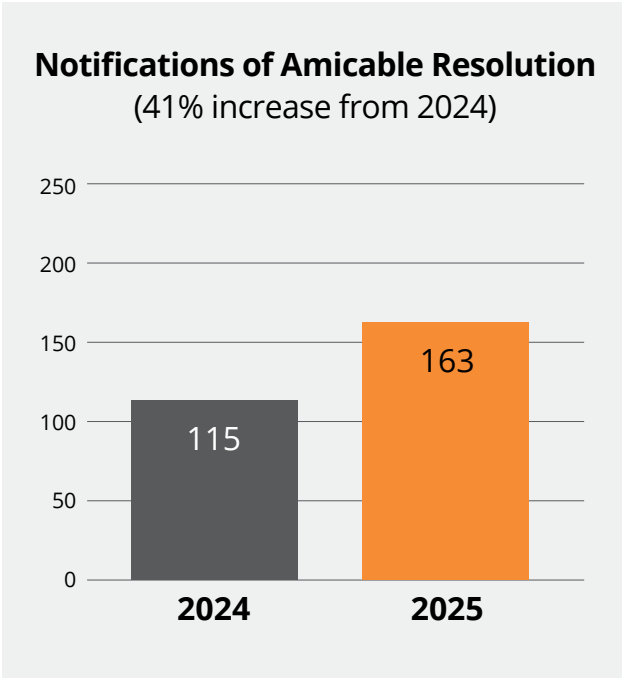
Lodged with other EU/EEA Supervisory Authority

Lodged Directly with DPC

Concluded Cross-Border Complaints
(43% increase from 2024)



Of the concluded complaints, the DPC submitted **163** notifications through the GDPR Article 60 cooperation mechanism in cases where an amicable resolution had been achieved. This represents a **41% increase** on the 2024 reported figure. Details of these cases can be found published on the EDPB website.



Further information on Complaint-Based Cross-Border Decisions can be found on pages 49-55 of this report. Cross-Border Case Studies are being published separately.

From left to right: Commissioners Dale Sunderland, Des Hogan and Niamh Sweeney attending the European Data Protection Board December Plenary in Brussels.

Law Enforcement Directive Complaints

The Law Enforcement Directive (LED), as transposed into Irish law in the 2018 Act, applies where the processing of personal data is carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties. In order for an organisation to engage with these sections, the organisation must be a 'competent authority' as set out in Section 69 of the 2018 Act.

The main two competent authorities that the DPC engages with via complaints are An Garda Síochána (AGS) and the Irish Prison Service. Statutory Bodies such as the Office of the Revenue Commissioners, county councils and the Department of Social Protection also fall to be considered competent authorities in relation to a limited number of their functions.

During 2025, the DPC increased its engagement with competent authorities. Working alongside the DPC's supervision units, this engagement has focused on ensuring that these authorities provide clear and concise information to individuals, particularly when responding to access requests. The DPC has emphasised the need for competent authorities to use plain language when explaining why records containing

personal data may not be released. In essence, organisations should more clearly set out the rationale for withholding some or all of the requested information as part of their response to the individual.

Through this work, the DPC aims to improve the efficiency of its own complaint-handling processes when asked by members of the public to review or validate a competent authority's decision to limit or restrict disclosure.

In 2025, the DPC **received 32 LED complaints** and **concluded 11 LED complaints** (including complaints received prior to 2024). **Over 65%** of complaints examined by the DPC under the LED related to Subject Access Requests. Further information on the LED is available at the DPC website: Law Enforcement Directive | Data Protection Commission

Law Enforcement Directive

Direct Intervention

The DPC often handles cases which are particularly sensitive and where immediate intervention is key to safeguarding the data protection rights of a large number of people. This tends to arise in circumstances where a serious data protection matter has been brought to the attention of the DPC, but there is no valid complaint (as defined under Section 107 of the 2018 Act) to progress, as the individual who brought the matter to the attention of the DPC is not directly affected by the issue being raised.

When such a matter is brought to the attention of the DPC, the DPC can directly intervene and engage with the data controller regarding those issues. This direct and immediate intervention can be key to ensuring the safeguarding of the data protection rights of large numbers of people.

Processing of personal data of adults at risk of harm or in vulnerable situations.

Individuals at risk of harm or in vulnerable situations might not always be in a position to raise data protection queries or complaints themselves, nor might they be in a position to exercise any of their own data protection rights.

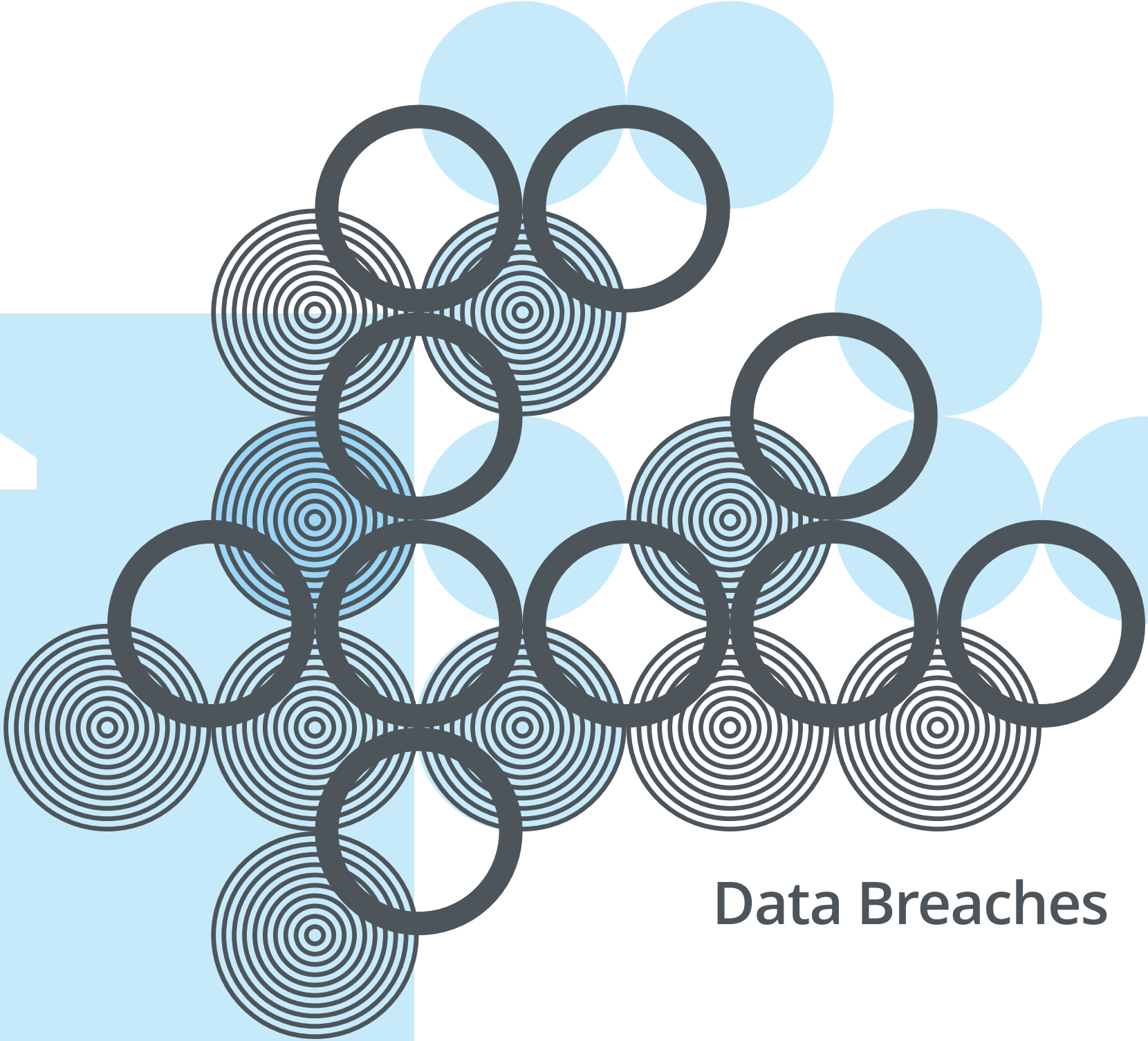
Should a family member or friend wish to assist that individual with their data protection concerns, they must have the legal authority to do so. If they do not have the legal authority to do so, such as a letter of authority from that person, or power of attorney, then the matter often cannot be addressed by the DPC by way of standard complaint handling. However, when such a matter is referred to the DPC, it can assess the concerns raised and engage directly with the data controller as may be required.

Data Brokers and Phone Location Data

A broadcast by RTE's Primetime programme on 18 September 2025 alleged that an unnamed company was selling precise location data derived from devices held by Irish data subjects. The DPC subsequently established the identity of this company, and during the year engaged in detailed correspondence with it to ascertain details of its processing activities. As a result of this engagement, the DPC secured a voluntary suspension of processing involving location data relating to Irish users. A number of other companies linked to the Irish company, operating in other EU Member States, were identified during the course of the DPC's investigations. At year end, cooperation was ongoing with the data protection authorities of those Member States who are competent for regulating these companies. The investigation of this matter remained ongoing at year's end.

In 2025, the DPC separately wrote to data brokers based in Ireland to emphasise the GDPR obligations which apply to precise location data.

4.



Data Breaches

4. Data Breaches

Under the GDPR and the ePrivacy directive, organisations are obliged to notify personal data breaches to the DPC or relevant supervisory authority where the breach presents a risk to the affected individuals. Under the GDPR, organisations must do this within 72 hours of becoming aware of the breach.

Such GDPR notifications are usually submitted by an organisation's Data Protection Officer (DPO) who can distinguish minor from major breaches by applying a risk-based approach to their assessment of the incident. The DPC engages closely with organisations to understand and mitigate the risk data breaches poses to individuals. It is of note that in 2025, **55% of breaches** reported to the DPC were of either low risk to data subjects, or no risk to data subjects could be identified. This informed the DPC's engagement with organisations with regards to their reporting obligations. Early responses can be invaluable in addressing financial, legal and reputational risks to organisations as well as in vindicating the rights of the individuals concerned.

In 2025, the DPC received **6,521 valid data breach notifications**. This represented a **16% decrease** on the overall data breach numbers received by the DPC in 2024. There may be a number of reasons for this decrease, including an organisation improving their compliance with the GDPR or potentially as a result of an organisations deeming that certain breaches have not reached the threshold to report it to the DPC. Article 33(5) of the GDPR places an obligation on organisations to record all personal data breaches and the DPC 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.

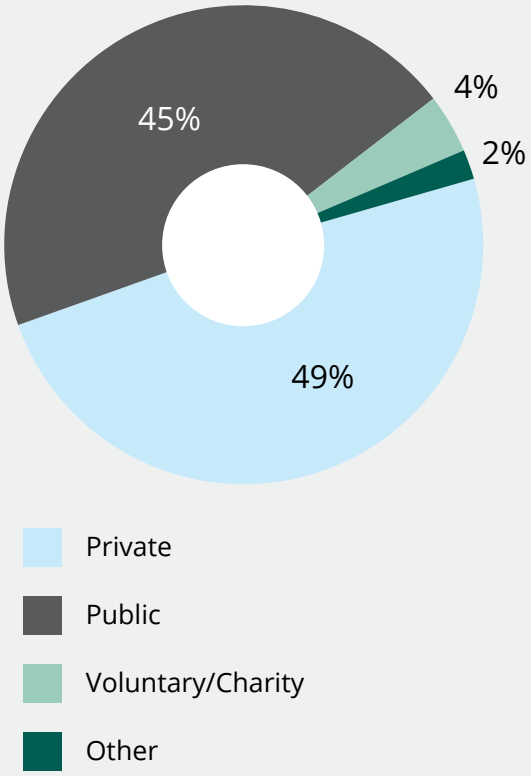
Of the 6,521 notifications received in 2025, **5,692** were GDPR notifications and of those:

49% related to the private sector;

45% to the public sector; and

4% came from the voluntary and charity sector.

Valid Data Breaches 2025

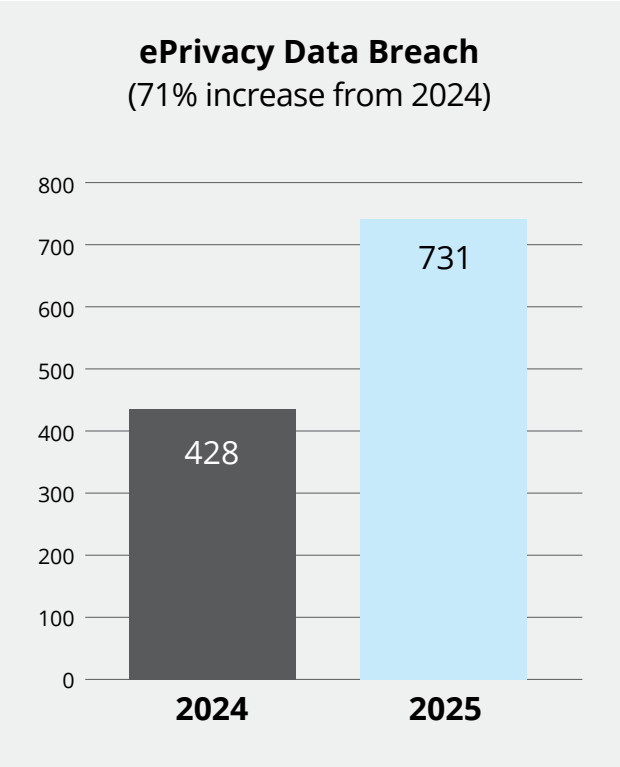


50% of notified cases arose as a result of correspondence being sent to the wrong recipient. Since the introduction of the GDPR, and in line with previous years, the highest category of data breaches notified to the DPC in 2025 related to unauthorised disclosures in incidents affecting single individuals or small groups, accounting for half of total notifications. Of the breach notifications received in 2025, the DPC had concluded its assessment in **85%** of cases by year-end.

In keeping with the trend of previous years, public sector bodies and banks accounted for the top 10 organisations with the highest number of breach notifications recorded against them. Insurance and telecom companies featured prominently in the top 20. Notably, correspondence issuing to incorrect recipients because of poor operational practices and human error – for example, inserting a wrong document into an envelope addressed to an unrelated third party – continued to feature prominently. The DPC engages with organisations to make organisations aware of their obligations and offer guidance. The DPC continually monitors breach notifications received to identify trends and inform further investigative and enforcement actions.

ePrivacy Breaches

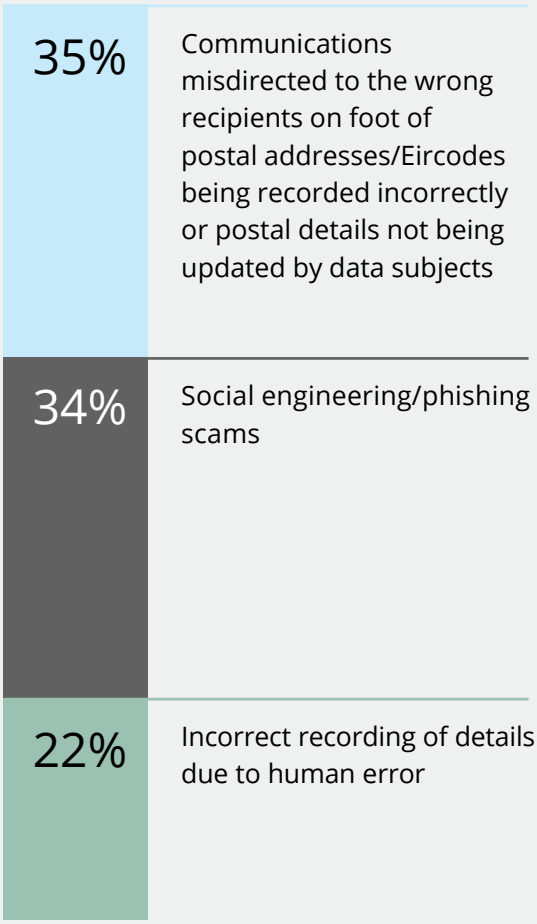
In 2025, the DPC received a total of **731 data breach notifications** under SI 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ('the ePrivacy Regulations'). The ePrivacy Regulations implement Directive 2002/58/EC ('the ePrivacy Directive') in Irish law. The figure of 731 represents an increase of **71%** on the 428 reported for 2024 and accounted 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 S.I. 336/2011 involved more than 100 individuals. The top three types of breaches reported under S.I. 336/2011 can be categorised as follows:

- communications misdirected to the wrong recipients on foot of postal addresses/ Eircode's being recorded incorrectly or postal details not being updated by data subjects **(35%)**;
- social engineering/phishing scams (third parties gaining access to customer accounts, including access to personal data) **(34%)**; and
- 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%)**.

Top Three Types of Breaches Reported Under S.I. 336/2011



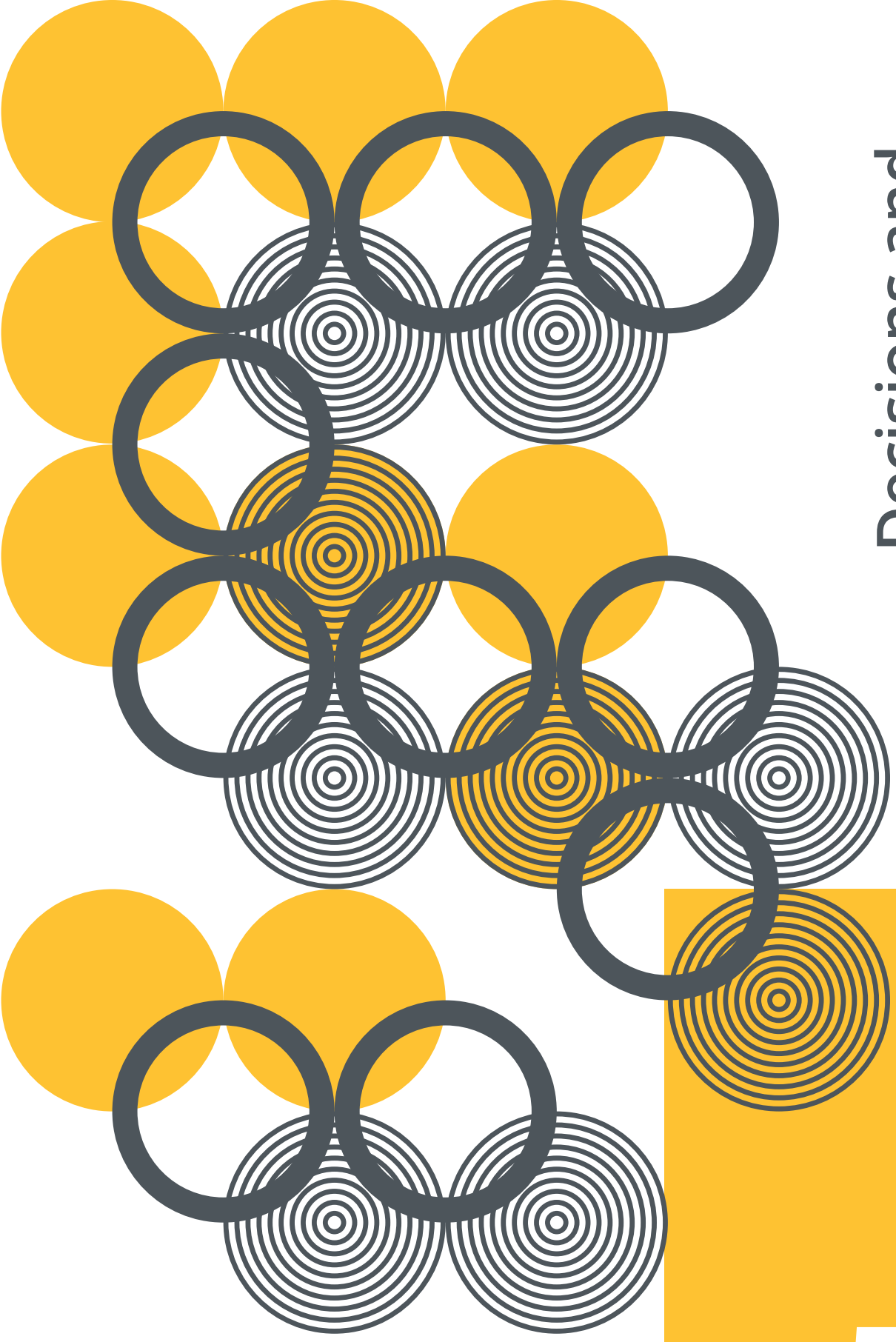
Over **one-third** of breaches notified to the DPC under S.I. 336/2011 were as a result of phishing scams. Phishing is a process whereby someone fraudulently attempts to trick users into disclosing sensitive information, such as usernames and passwords, by disguising themselves as a trusted source in an electronic communication. The DPC received a number of breach notifications in 2025 whereby malicious actors had targeted customers through SMS phishing and fraudulently obtained their passwords/one-time passcodes, in order to gain access to customers' online portal accounts.

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 this increase in unauthorised disclosure incidents on foot of phishing in 2025, the DPC intends to engage further with the telecommunications sector in 2026 in relation to the security measures that they have in place.

Law Enforcement Directive Breaches

The DPC also received **92** valid breach notifications in relation to law enforcement matters submitted under the notification requirements of the Law Enforcement Directive which was transposed into Irish law by the 2018 Act.

Data Breach Case Studies are being published separately to this report.



Decisions and Inquiries

5.

5. Decisions and Inquiries

Statutory Inquiries by the DPC

Under section 110 of the 2018 Act, the DPC may conduct two different types of statutory inquiry in order to establish whether an infringement of the GDPR or the 2018 Act has occurred:

- a complaint-based inquiry; and
- an inquiry of the DPC's 'own volition'.

As of 31 December 2025, the DPC had **87** Statutory Inquiries on-hand, including **53 Cross-Border Inquiries**. Notably, following amendments made to the Data Protection Act 2018, the DPC is empowered to impose reprimands on data controllers and data processors as part of its complaint-handling procedures—a corrective power previously reserved for statutory inquiries only.

The DPC issued **10 Final Decisions** and **92 Provisional Decisions** in 2025, with regulated entities given an opportunity to make submissions on proposed findings in all cases. **Seven of these Final Decisions and 88 of these Provisional Decisions** were in accordance with the Article 60 co-decision making process.

Overview of Final Decisions taken in 2025

Name	Date of Decision	Fine	Corrective Measures Imposed
Microsoft Ireland Operations Limited	20 February 2025	N/A	No infringement found. Complaint dismissed in accordance with Section 113(2)(a) of the Data Protection Act 2018, as amended, and in accordance with Article 57(1)(f) of the GDPR.
Patreon Ireland Ltd	3 April 2025	N/A	Reprimand issued for infringements in relation to Article 12(2) and 12(3) of the GDPR.
TikTok Technology Limited (TikTok)	30 April 2025	€530,000,000	The DPC found that TikTok infringed Articles 46(1) and 13(1)(f) of the GDPR. The DPC issued an order requiring TikTok to suspend transfers of EU/EEA user data to China and an order requiring it to bring its processing into compliance.
Yahoo EMEA Limited	6 May 2025	N/A	Reprimand issued for an infringement in relation to Article 13(2)(a) of the GDPR.

Name	Date of Decision	Fine	Corrective Measures Imposed
Department of Social Protection	9 June 2025	€550,000	The DPC found that the Department infringed Articles 5(1)(a), 6(1), 9(1), 5(1)(e), 13(1)(c), 13(2)(a), 35(7)(b) and 35(7)(c) of the GDPR. The DPC issued an order to cease processing of biometric data related to SAFE 2 registration within nine months unless a valid lawful basis can be identified. The DPC also issued a reprimand in respect of the infringements.
City of Dublin Education and Training Board (CDETB)	18 June 2025	€125,000	The DPC found that CDETB infringed Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4) of the GDPR. The DPC issued an order to bring processing into compliance with the GDPR's security requirements. The DPC also issued a reprimand in respect of the infringements.
Cubic Telecom	28 July 2025	N/A	Reprimand issued for an infringement in relation to Article 15 of the GDPR.
Meta Platforms Ireland Limited (MPIL)	5 August 2025	N/A	No infringement found. MPIL was found to have sufficiently demonstrated its compliance under Article 15(4) of the GDPR.
Microsoft Ireland Operations Limited	1 September 2025	N/A	Microsoft Ireland Operations Limited was ordered to bring its processing into compliance and was issued a reprimand in relation to Articles 12(4) and 5(1)(a) of the GDPR.
University of Limerick	11 December 2025	€98,000	The DPC found that the University of Limerick infringed Articles 5(1)(f), 32(1), 30(1), 33(1) and 34(1) of the GDPR. The DPC imposed a reprimand in respect of these infringements.

Confirmation of Administrative Fines

In 2025, the DPC imposed **over €530 million in administrative fines.** These included fines imposed on TikTok Technology Limited over the transfer of the personal data of European users to China, as well as fines against the Department of Social Protection and City of Dublin Education and Training Board.

All fines imposed by the DPC must be confirmed in court before they can be collected. Once collected, fines are remitted to the central exchequer in Ireland.

In 2025, the DPC collected and remitted a total of €125,000 from one administrative fine to the central exchequer in Ireland. The relevant fine was collected from City of Dublin Education and Training Board which was confirmed in the Dublin Circuit Court in 2025.

Since May 2018, the DPC has issued **€4.04 billion** in fines.

Domestic Decisions that Concluded in 2025

Inquiry regarding Department of Social Protection

In June 2025, the DPC adopted a Final Decision finding that the Department of Social Protection (DSP) infringed Articles 5(1)(a), 5(1)e, 6(1), 9(1), 13(1)(c), 13(2)(a) and 37(5) of the GDPR. The Decision concerned the lawfulness, fairness and transparency of the DSP's processing of biometric facial templates in the context of SAFE 2 registration for the Public Services Card (PSC). The processing examined under the Inquiry included the collection, processing and retention of facial templates generated by the DSP from individuals applying for, or renewing, a PSC.

The Inquiry followed a prior DPC investigation, which was concluded in 2019, concerning certain aspects of the DSP's processing of personal data in connection with the issuance of Public Services Cards. The Inquiry considered if the DSP had an appropriate lawful basis for processing biometric data under Articles 5(1)(a), 6(1) and 9(1) of the GDPR and if the DSP had provided individuals with sufficiently clear and transparent information regarding the processing to the extent that it was foreseeable to individuals that their biometric data would be processed by the DSP and the purposes of the processing. The Inquiry further considered if the DSP's Data Protection Impact Assessment (DPIA) complied with the requirements of the DPIA under the GDPR.

In its Decision, the DPC found that the DSP had not identified a valid lawful basis for processing biometric data and therefore infringed Articles 5(1)(a), 6(1) and 9(1) of the GDPR. The DPC also found that the DSP had infringed Article 5(1)(e) of the GDPR in unlawfully retaining facial templates. The Decision also found that the DSP infringed Articles 13(3)(c) and 13(2)(a) of the GDPR for failing to provide data subjects with sufficiently clear and transparent information about the processing of biometric data and a breach of Article 35(7)(b) and (c) of the GDPR as the DSP did not include details required by the GDPR in its DPIA for SAFE 2 registration.

In the Decision, the DPC issued a formal reprimand to the DSP and imposed fines totalling €550,000. The DPC ordered the DSP to cease biometric data processing related to SAFE 2 registration within nine months unless a valid lawful basis can be established. This Decision has been appealed by the DSP.

Inquiry concerning Department of Social Protection

Inquiry regarding City of Dublin Education and Training Board

In June 2025, the DPC adopted a Final Decision finding that the City of Dublin Education and Training Board (CDETB) infringed Articles 5(1)(f), 32(1) and 32(2), 33(1), 34(1) and 34(4) of the GDPR. CDETB is the State education and training authority for Dublin city and is also responsible for Student Universal Support Ireland (SUSI), the national awarding authority for student grants.

CDETB notified the DPC of a personal data breach regarding its web server which was retaining the personal data of student grant applicants who had uploaded information related to their grant applications through the SUSI website, as well as the discovery of malware on the web server. The breach impacted approximately 13,000 data subjects, identifiable by email address, who had submitted supplementary forms through the SUSI website during 2017 and 2018. The personal data impacted by the breach included names, surnames, birth dates, PPSNs, contact details, identification data, and special categories of data (such as data revealing racial or ethnic origin and health data).

The DPC assessed CDETB's technical and organisational measures for ensuring the security of personal data that it processed on its website in light of the risks presented. Those risks included the risk of unauthorised access or disclosure of personal data to third parties. They also included risks of accidental or unlawful destruction, alteration, or loss of availability of the personal data processed on the website.

The DPC also examined CDETB's compliance with its obligation to notify breaches to the DPC promptly, as well as CDETB's obligation to notify data subjects of the breach. In this matter, the DPC specifically requested CDETB to notify affected data subjects, but it declined to do so until 16 December 2020, which was over two years after it became aware of the breach.

The DPC's Decision found that CDETB:

- infringed Articles 5(1)(f), 32(1) and 32(2) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data on the SUSI website, and by failing to assess the appropriate level of security;
- infringed Article 33(1) of the GDPR by failing to notify the DPC of the breach without undue delay;
- infringed Article 34(1) of the GDPR by failing to notify the affected data subjects of the breach without undue delay; and
- infringed Article 34(4) of the GDPR by failing to communicate the breach to data subjects when required to do so by the DPC.

The DPC issued a number of corrective measures on foot of the infringements found in the inquiry, including: **a reprimand; an order to CDETB to bring its processing into compliance with the GDPR's security requirements; and administrative fines totalling €125,000.**

However, the DPC considered the actions taken by CDETB and its engagement with the DPC, since being presented with the DPC's proposed findings in a draft version of its Decision, to be commendable. CDETB accepted each of the findings of infringements set out in the draft Decision, acknowledged full responsibility for the breach, apologised to both the data subjects affected and the DPC, and proactively took steps, without having specifically been directed to do so by the DPC, to reduce the likelihood of similar breaches occurring in future. As a result, the DPC decided to impose a substantially lower total fine than the fining range proposed in the Draft Decision.

Inquiry into City of Dublin Education and Training Board

Inquiry regarding University of Limerick

Between 30 November 2018 and 20 January 2020, University of Limerick (UL) notified the DPC of 12 personal data breaches: in six of them, unauthorised persons gained access to the work email accounts of UL staff members by means of phishing attacks. The unauthorised users were able, in some cases, to set up forwarding rules which diverted emails containing specified keywords to a folder they had created in the user's mailbox. The compromised email accounts contained personal data including identity information, contact details, PPSNs, bank information, medical or legal documentation, staff disciplinary and HR records, and data belonging to students, staff, and external parties.

The DPC carried out this own-volition Inquiry under sections 110 and 111 of the Data Protection Act 2018. It assessed UL's compliance with: Articles 5(1)(f) and 32(1) of the GDPR (implementation of appropriate technical and organisational measures to ensure appropriate security of the personal data processed on its email service); Article 30(1) of the GDPR (maintenance of a record of processing activities); Article 33(1) of the GDPR (notification to the DPC of personal data breaches without undue delay, and in any event within 72 hours of becoming aware of them); and Article 34(1) of the GDPR (notification to concerned data subjects without undue delay of personal data breaches assessed to pose a high risk).

In its Final Decision of December 2025, the DPC found that UL did not implement appropriate technical and organisational measures to ensure the security of personal data as required by Articles 5(1)(f) and 32(1) of the GDPR. The DPC also found that UL's initial record of processing activity did not fully comply with the requirements of Article 30(1) of the GDPR, although UL implemented a compliant record of processing activity in May 2020, after the period assessed by the DPC in this Inquiry. The DPC found that three breach notifications were filed more than 72 hours after UL became aware of them and, therefore, were not reported without undue delay in accordance with Article 33(1) of the GDPR. With respect to Article 34(1) of the GDPR, the Inquiry found that UL had failed in three cases to inform persons affected by a high-risk breach without undue delay. The DPC therefore found **infringements of Articles 5(1)(f), 32(1), 30(1), 33(1), and 34(1) of the GDPR and issued UL with a reprimand and administrative fine of €98,000.**

The DPC's decisions on corrective measures took account of UL's significant steps to remediate the deficiencies in its processing of personal data identified in this Inquiry. Based on the details of those improvements provided by UL in its submissions, the DPC decided that it was not necessary or proportionate for it to issue an order for UL to bring that processing into compliance with the GDPR. The DPC's acknowledgement of those improvements does not, however, relieve UL of its obligation to continually evaluate the effectiveness of its measures and the measures that are necessary to ensure a level of security that is appropriate to the dynamic risk presented by its processing.

Inquiry Concerning the University of Limerick

Domestic Cases that Reached a Key Investigative Stage in 2025

Permanent TSB plc

The DPC commenced this Inquiry following three separate breach notifications from Permanent TSB plc (PTSB) in May 2022. The personal data breach notifications concerned circumstances where malicious actors, in possession of certain customer information, attempted to gain access to data subjects' bank accounts and amend account details by calling PTSB's Open24 call centre and posing as those customers. The scope of the Inquiry concerns the organisational and technical measures implemented by PTSB in the Open24 call centre, to ensure the security of personal data, and whether PTSB complied with its obligations to notify the DPC of data breaches without undue delay. The DPC issued a **Draft Decision to PTSB in August 2025**. PTSB made submissions on the Draft Decision and at year-end the DPC was preparing its Final Decision in the Inquiry.

Children's Health Ireland, Tallaght University Hospital

During 2025, protected disclosures regarding certain processing activities within one specific facility at Children's Health Ireland (CHI) at Tallaght University Hospital were received by the DPC. The DPC also received a data breach notification related to the unauthorised access and disclosure of a child's medical file at this facility.

Following a review of these disclosures and engagement with the DPO of the facility at CHI, the DPC carried out an unannounced site inspection. Following this inspection, the DPC subsequently **commenced an Inquiry on 14 August 2025**. At year-end the matter was ongoing.

Central Bank of Ireland

The DPC opened an ownvolition Inquiry in October 2023 after the Central Bank of Ireland reported a personal data breach earlier in the year involving the Central Credit Register database.

The DPC issued a **Statement of Issues in September 2025**, setting out a focused overview of the facts established during the Inquiry and outlining the matters to be determined during the Inquiry's decisionmaking stage. The Central Bank of Ireland submitted observations on the Statement of Issues. At year-end, the DPC was assessing those submissions.

An Post GeoDirectory DAC (Designated Activity Company)

In July 2023, the DPC commenced an own-volition Inquiry concerning the products and services offered by An Post GeoDirectory DAC. The DPC issued a **Statement of Issues** to An Post GeoDirectory DAC in **November 2025** which provided a focused overview of the facts established during the inquiry and identified a principal preliminary issue to be determined during the Inquiry's decision-making stage. An Post GeoDirectory DAC made submissions in response and at year-end the matter was ongoing.

HSE Dublin and Mid-Leinster (Tullamore)

The DPC commenced an own-volition Inquiry in October 2019 in relation to a ransomware attack that affected the processing being conducted within a laboratory system in the Midlands Regional Hospital, Tullamore. The scope of the Inquiry concerns the organisational and technical measures implemented by the HSE in relation to that system and the manner in which the HSE responded to the attack. The DPC completed its Final Inquiry Reports on those matters in March 2021 and issued its Draft **Decision to the HSE in December 2025**.

Cross-Border Cases

Where a particular inquiry or complaint concerns the examination of cross-border processing, the GDPR requires the DPC, where it acts as the Lead Supervisory Authority (LSA), to conclude its decision in accordance with the cooperation mechanism set out in Article 60 of the GDPR. The Article 60 mechanism outlines a procedure designed to facilitate the conclusion of decisions on the basis of consensus between the LSA and other European Data Protection Authorities, known as Concerned Supervisory Authorities (CSAs). In accordance with the GDPR and its duty of sincere cooperation, the DPC cooperates with its peer EU/EEA regulators throughout the inquiry process. Through the Article 60 mechanism, CSAs are enabled to share their views on the inquiry or complaint (as the case may be) with the LSA, which must take due account of their views. Where those views take the form of a relevant and reasoned objection, the LSA must take account of those objections by amending its draft decision, failing which it must refer the objections to the European Data Protection Board for determination pursuant to the Dispute Resolution process set out in Article 65 of the GDPR.

Large-Scale Cross-Border Cases that Concluded in 2025

Inquiry regarding TikTok Technology Limited's transfers of EEA users' personal data to servers located in China

In April 2025, the DPC adopted a Final Decision finding that TikTok Technology Limited (TikTok) had infringed Articles 13(1)(f) and 46(1) of the GDPR regarding its transfers of EEA user data to China. The transfers of personal data considered in the Decision consisted of TikTok's transfers of EEA user data to China by way of remote access to that personal data by personnel of the ByteDance group of companies who are based in China.

In the Decision, the DPC found that **TikTok infringed Article 46(1) of the GDPR** during the temporal scope of the Inquiry by carrying out the data transfers while failing to verify, guarantee and demonstrate that that the personal data of EEA users subject to the data transfers was afforded a level of protection essentially equivalent to that guaranteed within the European Union.

The DPC found that **TikTok infringed Article 13(1)(f) of the GDPR** from 29 July 2020 to 1 December 2022 by failing to provide data subjects with required information on the data transfers and information on how the processing concerned remote access to personal data stored in Singapore and the United States by personnel based in China.

Having considered the infringements of the GDPR as set out above, the DPC decided to order **TikTok to suspend the data transfers and to bring the processing into compliance.** The DPC also imposed **two administrative fines totalling €530 million. This Decision has been appealed by TikTok.**

During the Inquiry, TikTok informed the DPC that it did not store EEA user data on servers located in China. Rather, TikTok's position, until after the DPC submitted its Draft Decision to the GDPR cooperation mechanism, was that its transfers of EEA User Data to China consisted of remote access to that personal data by personnel of the ByteDance group of companies in China. Accordingly, the Decision considered whether those transfers by way of remote access complied with Chapter V of the GDPR. The DPC's Decision was appealed by TikTok (see the Litigation section of this report).

In April 2025, TikTok informed the DPC of an issue that it discovered that resulted in limited EEA user data being stored on servers in China. TikTok informed the DPC that this had resulted in TikTok providing **inaccurate information** to the Inquiry. While the Decision related to TikTok's transfers by way of remote access only, the Decision expressed the DPC's deep concern that TikTok had submitted inaccurate information to that inquiry.

On 4 July 2025, the DPC commenced a **separate own-volition Inquiry to consider the lawfulness of these transfers** as set out on page 47 of this report.

Fiosrúchán maidir le TikTok Technology Limited

Large-Scale Cross-Border Cases Inquiries that Reached a Key Investigative Stage in 2025

Inquiry regarding X Internet Unlimited Company

In April 2025, the DPC commenced this own-volition Inquiry relating to the processing of personal data comprised in publicly-accessible posts, posted on the X social media platform by EEA users, associated with the development of the Grok AI models.

The Inquiry is considering X Internet Unlimited Company's (XIUC) compliance with a range of provisions of the GDPR, including with regard to the lawfulness of the processing of personal data, compliance with the principle of purpose limitation, and transparency. A notice of commencement issued to XIUC in April 2025 and submissions in response to a number of rounds of queries have been received from XIUC. The information gathering phase of the Inquiry was ongoing at year-end.

Inquiry regarding TikTok Technology Limited transfers of EEA users' personal data to servers located in China

In July 2025, the DPC commenced this own-volition Inquiry relating to TikTok Technology Limited's (TikTok) transfers of EEA users' personal data to servers located in China. The Inquiry follows on from the DPC's Decision of 30 April 2025 in relation to a separate TikTok Inquiry (see above), which also considered TikTok's transfers of EEA users' personal data to China. However, during that previous Inquiry, TikTok maintained that transfers of EEA users' personal data to China took place by way of remote access only and that EEA user data was not stored on servers located within China, i.e. EEA user data was stored on servers located outside of China and was accessed remotely by TikTok staff from within China. Accordingly, the DPC's Decision of 30 April 2025 did not consider TikTok's storage of EEA users' personal data on servers located in China. In April 2025, TikTok informed the DPC of an issue that it had discovered in February 2025 where limited EEA user data had in fact been stored on servers in China, contrary to TikTok's evidence to the previous Inquiry.

The DPC expressed its deep concern that TikTok had submitted inaccurate information to the previous Inquiry. In its press release issued at the time of the conclusion of that Inquiry, the DPC stated that it was taking those developments 'very seriously' and was 'considering what further regulatory action may be warranted, in consultation with our peer EU Data Protection Authorities'. As a result of those considerations, the **DPC decided to open this new Inquiry into TikTok under section 110 of the Data Protection Act 2018.** The purpose of the Inquiry is to determine whether TikTok has complied with its relevant obligations under the GDPR in the context of the transfers now at issue, including the lawfulness of the transfers pursuant to Chapter V of the GDPR. Throughout the year, the DPC gathered relevant information and conducted an on-site inspection at TikTok's offices in November 2025.

Meta Platforms Ireland Limited

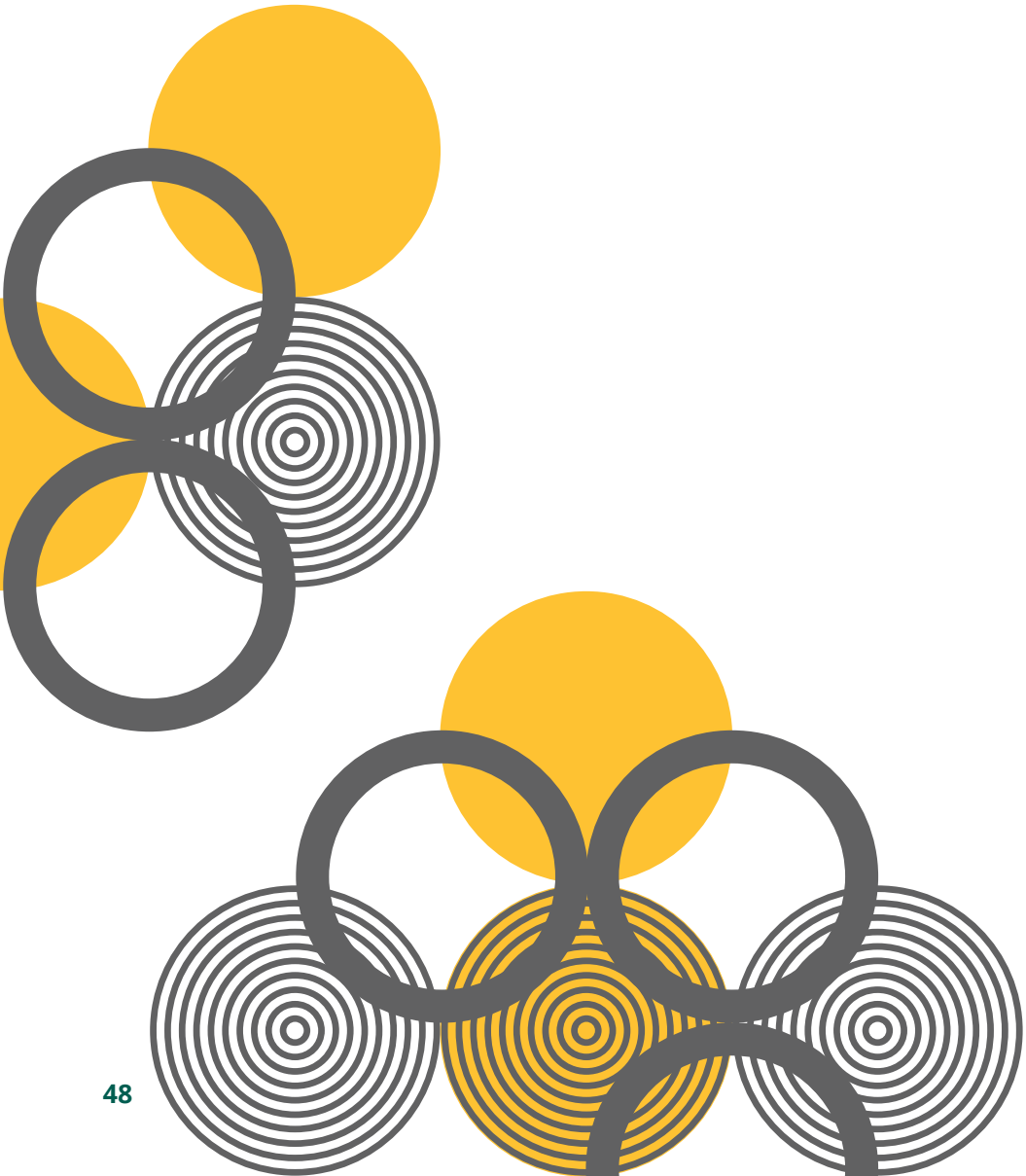
This complaint-based Inquiry concerns data subject rights under the GDPR. In 2018, the complainant made a written request to Meta, pursuant to the right of access and right to data portability. This request concerned certain information held in Meta databases, which was not otherwise accessible to users by means of automated access tools. The DPC subsequently commenced an Inquiry to assess whether Meta's refusal of the complainant's request was compliant with the GDPR.

In October 2025, the DPC issued a **Preliminary Draft Decision**, which sets out a detailed analysis of the legal and factual issues arising, and includes the DPC's provisional findings. In December 2025, Meta initiated Judicial Review proceedings challenging the Preliminary Draft Decision.

Cross-Border Cases involving Individual Complainants Concluded by DPC through EU Co-Operation Procedure in 2025

In addition to these large-scale inquiries, the DPC also concludes individual cross-border cases, including notifications of outcomes achieved in complaints amicably resolved through the EU cooperation procedure.

In 2025, the DPC concluded 208 cross-border complaint cases through the Article 60 procedure, including **163 notifications of complaints amicably resolved and six decisions**. This represents an increase of **42%** from 2024. Details of the amicably resolved notifications will be published on the EDPB Article 60 case register.



Complaint-Based Cross-Border Decisions that Concluded in 2025

Microsoft Ireland Operations Limited: Right to Be Forgotten

The DPC received a complaint directly from an EU/EEA citizen living outside of Ireland. The complaint concerned a Right to be Forgotten (RtbF) request submitted to Microsoft in relation to three URLs returned by its Bing search engine when the individual's name was entered as a search term. The URLs in question provided additional information on the individual's previous criminal conviction for sexual offences, which had resulted in a custodial sentence, their name being placed on the Sex Offenders Register and a sexual harm prevention order issuing against them. The individual argued that the continued availability of this information by Bing caused discrimination, hindered their employment prospects, and amounted to a disproportionate interference with their right to private life given that, under their national law, the sentence had now been served.

The individual made a search delisting request (in line with Article 17(3) of the GDPR) to Microsoft first. Microsoft removed one URL, finding its contents less reliable; however, following the application of a balancing test (an assessment of the individual's rights when balanced against the rights and freedoms of others as required under the GDPR), declined to delist the other two complained-of URLs. Dissatisfied with Microsoft's response, the individual submitted a complaint to the DPC.

As part of its investigation, the DPC considered the controller's balancing test in light of Articles 17 and 21 of the GDPR and the relevant EDPB guidance in particular. The DPC noted Microsoft's consideration of several factors, including the seriousness of the offences, the reliability of the source material and the public's legitimate interest in accessing information relating to offences, including those involving risks to minors. The DPC concluded that Microsoft had appropriately considered the individual's delisting request and acted consistently with its obligations under the GDPR. In **its Decision the DPC dismissed the complaint** in accordance with Section 113(2)(a) of the Data Protection Act 2018, as amended and Article 57(1)(f) of the GDPR respectively, **having found no infringement of the GDPR in this instance.**

KEY TAKEAWAYS:

The Right to be Forgotten is not an absolute right; requests may be partially declined, or declined in full, based on the individual circumstances relevant to each request. This case highlights the importance for controllers to conduct appropriate balancing tests for requests of this nature, thereby enabling them to sufficiently explain the rationale behind their decisions to partially decline or fully decline a deletion request.

Patreon Ireland Ltd: Subject Access Request and Scope of Controller Responsibility

This case contains two distinct GDPR-related issues, namely an alleged data breach on a third-party website; and Patreon Ireland Ltd.'s (Patreon) handling of both an access and erasure request.

Patreon provides a web hosting service to customers. The complainant in this case alleged a data breach (in line with Chapter 3 of the GDPR) had occurred on a third-party website which was hosted by Patreon. In addition to the alleged breach, the individual indicated that they had made an erasure request (in line with Article 17 of the GDPR) to Patreon, seeking to have 'false information' about them removed from the same third-party website. During its examination of the complaint, the DPC considered the alleged breach and concluded that Patreon was not the Data Controller for any processing carried out in respect of the third-party website, as it did not operate it, or determine the purposes and means of processing undertaken by the third-party website. Additionally, the individual was asked to provide a date or evidence of the erasure request made to Patreon. The individual was unable to locate a copy of the erasure request and, as such, the DPC was not in a position to consider either aspect of this complaint further.

The individual stated that they had made a Subject Access Request to Patreon in line with Article 15 of the GDPR. Patreon argued that the individual's access request had been unclear and was sent to the wrong email address. The DPC determined that the individual's initial email had constituted a valid access request, noting that it referenced GDPR rights, and was sent to a legitimate Patreon support address. The DPC's Subject Access Requests: A Data Controller's Guide makes it clear that data subjects 'can always validly lodge an access request by contacting the organisation through any method of communication be it by phone, post, informal chat or in person', and that a data controller, such as Patreon, 'may re-direct the data subject to the relevant department of the organisation dealing with access requests, or may re-direct the correspondence themselves by internal email or post. However, the clock for complying with the relevant time limit begins from the day the request is received by the data controller'.

Ultimately, in its Decision, the DPC found that Patreon had failed to act on the individual's Subject Access Request initially and only responded to their request several months later. The DPC held that Patreon had **infringed Article 12(2) and 12(3) of the GDPR** and issued Patreon with **a reprimand**.

KEY TAKEAWAYS:

This case highlights the importance of controllers ensuring they do not adopt an overly narrow view of what constitutes a valid access request.

This case also highlights a controller's role in ensuring that appropriate systems are put in place to identify and re-route access requests, where applicable, to the relevant team within its organisation.

Data Subject Access Requests FAQ's

Yahoo EMEA Limited: Transparency and Account Deletion

The DPC examined a complaint regarding the deletion of data associated with a Yahoo email account following a prolonged period of user inactivity. Having engaged with Yahoo directly and having been dissatisfied with Yahoo's response to the queries they had raised in relation to the deletion of their account and associated data, the individual brought their complaint to the DPC.

After discovering that emails, including sensitive special category personal information (such as medical data), had been removed, the individual sought details about the erasure and queried why they had not been notified in advance of the deleting of data associated with their email address. Yahoo explained to the individual that accounts inactive for over 12 months are automatically deleted in accordance with the organisation's then Terms of Service. Yahoo informed the DPC that this action was supported by its account activity logs, which confirmed that the individual in this case had not logged into their email account for more than a year. Additionally, Yahoo clarified that system-generated notifications would have been sent to the user's Yahoo address and registered recovery emails, if implemented, prior to the deletion taking place.

During the DPC's consideration of this complaint, Yahoo provided the exact deletion date and acknowledged that it should have given clearer information to the individual about its approach to erasure earlier in the process. The DPC considered Yahoo's compliance with its transparency obligations under the GDPR, including the clarity of user information, notification processes, and accessibility of relevant policies and concluded that Yahoo had failed to comply with its transparency obligations. While the DPC did find an **infringement in relation to Article 13(2)(a) of the GDPR**, the DPC also noted that Yahoo has subsequently updated its privacy policy to provide enhanced clarity in relation to the deletion and retention of its users' mailboxes. Consequently, in its **Decision the DPC issued a reprimand** to Yahoo.

KEY TAKEAWAY:

This case highlights the importance of clear and proactive communication being used by controllers with their service users when implementing automated deletion policies affecting users' data.

Cubic Telecom: Misinterpreted Subject Access Request and Unlawful Erasure

This case concerned a Subject Access Request submitted to Cubic Telecom following the individual's attempt to register with the service. Having complained to Cubic Telecom, the individual was dissatisfied with the way in which their request was dealt and brought their complaint to the North Rhine-Westphalia Data Protection Authority (NRW DPA). NRW DPA transferred the complaint to the DPC as the Lead Supervisory Authority (LSA) for Cubic Telecom, in respect of the processing at issue in the complaint.

During the DPC's examination of the complaint it was discovered that, due to a customer support error, the individual's access request was incorrectly interpreted as an erasure request after the individual wrote to Cubic Telecom stating: 'I'm renouncing your service…'. Cubic Telecom stated that the initial access request had been processed by an external support contractor who misunderstood and misclassified it as an erasure request. As a result, key personal data relating to the individual, including their date of birth, contact details, account identifiers and the access request email they had sent to Cubic Telecom, were deleted.

Cubic Telecom further clarified to the DPC that additional personal data relating to the individual (such as their name, address and traffic session data) was also subsequently deleted in line with Cubic Telecom's retention policy.

Following the DPC's intervention, Cubic Telecom provided the individual with all the remaining personal data it had retained. Cubic Telecom also implemented measures to ensure the error would not reoccur. These included introducing additional reviews for all access and erasure requests going forward and providing GDPR-related refresher training for support staff.

The DPC found that Cubic Telecom had **infringed Article 15 of the GDPR** by both failing to provide the individual with a copy of their personal data and by mistakenly erasing the individual's personal data. The DPC noted that Cubic Telecom had taken steps to try and reduce the likelihood of this type of human error from happening again, including the provision of refresher training to its staff. In its Decision, the DPC **issued a reprimand** to Cubic Telecom in respect of this complaint.

KEY TAKEAWAY:

This case highlights the importance providing adequate training for staff and external support contractors in key, customer-facing roles, to ensure that data subject rights requests are correctly identified and actioned in a timely manner.

Meta Platforms Ireland Limited: Subject Access Request and Article 15(4) of the GDPR

This complaint concerned an individual who was unable to access their Facebook account after Meta disabled it for what it determined to be a serious breach of its Terms of Service. The individual submitted a Subject Access Request looking for all of their saved personal data, including their Messenger contacts and phone numbers. Meta initially provided the individual with access to most of their personal data via a 'burner link.' However, Meta decided to withhold certain information, relying on Article 15(4) of the GDPR, advising that the disclosure of the withheld personal data, could potentially adversely affect the rights and freedoms of others. The individual, unhappy with Meta's decision, lodged a complaint with the DPC.

During the DPC's examination of this complaint, Meta detailed its investigation of this account, the basis for the disablement of the relevant account, and its reliance on Article 15(4) of the GDPR for withholding specific categories of data, including the reported violating content, details of reporters, and account review information.

Having considered Meta's balancing test and the supporting evidence, the DPC determined that, in this particular case, Meta had undertaken the appropriate steps in an attempt to balance the individual's right of access to their personal data against the fundamental rights of others, in accordance with the principal of proportionality. The DPC was satisfied that, in this instance, Meta had sufficiently demonstrated its reliance on Article 15(4) of the GDPR for restricting the individual's right of access. The DPC decided that Meta had complied with its obligations in responding to the individual's access request in this instance and **no infringement was found**.

KEY TAKEAWAY:

This case highlights the competing considerations which must be taken into account when applying an Article 15(4) of the GDPR balancing test. This case is a good example of a controller being able to explain and provide documentary evidence in support of its decision not to release certain categories of personal data.

Microsoft Ireland Operations Limited: Subject Access Request

This Inquiry concerned a complaint regarding Microsoft's handling of a Subject Access Request and its refusal to provide the individual with a copy of their personal data following their account suspension due to an alleged violation of Microsoft's Services Agreement. The individual's Microsoft OneDrive account was subsequently terminated after the access request was made and all of the individual's data was deleted.

Microsoft sought to rely on Article 15(4) of the GDPR in refusing to provide the individual with their personal data, stating that to do so would 'adversely affect the rights and freedoms of others'.

The scope of the Inquiry examined Microsoft's handling of the access request under Articles 12(4), 15(4) and 5(1)(a) of the GDPR. The Inquiry examined Microsoft's justification for refusing the access request, and whether it provided the individual with the necessary information contained in Article 12(4) of the GDPR, i.e. whether it gave the individual reasons for refusing access and informed them of their right to lodge a complaint with a supervisory authority and to seek a judicial review without undue delay. The Inquiry also examined whether Microsoft complied with the principles of lawfulness, fairness and transparency under Article 5(1)(a) of the GDPR in deleting the individual's personal data after the access request was made.

The Inquiry established that Microsoft's policies were unclear as regards: the procedures that apply to locked, suspended, closed and deleted accounts; when precisely account data would be deleted following account closure; and what, if any, appeal options are available to users whose accounts have been closed by Microsoft for an alleged violation of the Microsoft Services Agreement. Microsoft erased the individual's OneDrive account data, despite not clearly informing the individual that their account had been terminated.

The DPC ultimately established a lack of clarity and transparency to the individual in Microsoft's handling of the access request and in the subsequent deletion of the individual's data. The DPC was satisfied that erasure of the individual's data took place despite a lack of clarity and transparency about whether the account was closed and the data scheduled for deletion, and in circumstances where Microsoft had failed to provide all of the required information in response to a Subject Access Request. The deletion of the account data therefore did not comply with the lawfulness, fairness and transparency required under Article 5(1)(a) of the GDPR.

The DPC found in its Decision **two infringements under Articles 12(4) and 5(1)(a) of the GDPR**. Specifically, Microsoft had failed to inform the individual of the possibility to lodge a complaint with a supervisory authority and to seek a judicial remedy following their access request infringing Article 12(4) of the GDPR. Microsoft infringed Article 5(1)(a) of the GDPR in its handling of the complainant's access request and in its decision to delete their data after receipt of the access request. The **DPC issued a reprimand** in respect of the two infringements identified in accordance with its powers under Article 58(2)(b) of the GDPR.

The Decision also ordered Microsoft to **revise its policies and procedures to bring its processing into compliance**, particularly: to clarify its retention policies for accounts terminated by Microsoft due to an infringement of the Microsoft Services Agreement; to clarify in what circumstances such data is permanently deleted; and to outline how users can appeal such an account termination.

Before finalising this Decision, in accordance with the co-operation mechanism provided by Article 60 of the GDPR, the DPC received a relevant and reasoned objection from a Concerned Supervisory Authority (CSA). The DPC worked with the CSA in question to reach consensus on a revised Draft Decision which was resubmitted and accepted by all the supervisory authorities concerned.

KEY TAKEAWAY:

This case highlights the necessity to provide clarity to users in policy documentation as regards what happens to user account data when their account is suspended or terminated by the controller.

Enforcement of Corrective Powers Exercised by the DPC

Sligo County Council

In September 2025, the DPC concluded its enforcement process following a Final Decision adopted by the DPC in November 2024. That Decision concerned an Inquiry into Sligo County Council's (the Council) processing of personal data through the use of CCTV and Automated Number Plate Recognition systems, and any other technologies that may be used to monitor individuals.

The Inquiry sought to assess whether the processing of personal data by the Council was in compliance with the GDPR and the Data Protection Act 2018. The DPC found that the Council had infringed Articles 5(1)(a), 5(1)(c), 5(1)(e), 5(1)(f), 13, 24(1), 25, 30 and 32(1) of the GDPR along with sections 71(1)(a), 71(1)(c), 71(1)(e), 71(1)(f), 71(10), 72, 72(1), 72(2), 75(1), 75(3) 76(2), 78, 79, 81, 82(2), 84 and 90(1) of the 2018 Act.

The corrective measures exercised by the DPC included:

- a temporary ban on the processing of personal data through CCTV cameras and ANPR cameras at a number of locations until a valid legal basis could be identified;
- an order to Sligo County Council to bring its processing of personal data into compliance taking certain actions specified in the Decision;
- a reprimand in respect of Sligo County Council's infringement of section 79 of the Data Protection Act 2018; and
- an administrative fine of €29,500.

The DPC carried out an **on-site inspection on 16 June 2025** to ensure compliance with the Decision. The inspection included meetings with council officials at County Hall as well visits to the Council's CCTV sites and control rooms in Cranmore and Sligo Harbour. The inspection team noted various positive changes carried out by the Council including the digital mapping of CCTV cameras, erected signage and the implementation of enhanced security measures in CCTV control rooms.

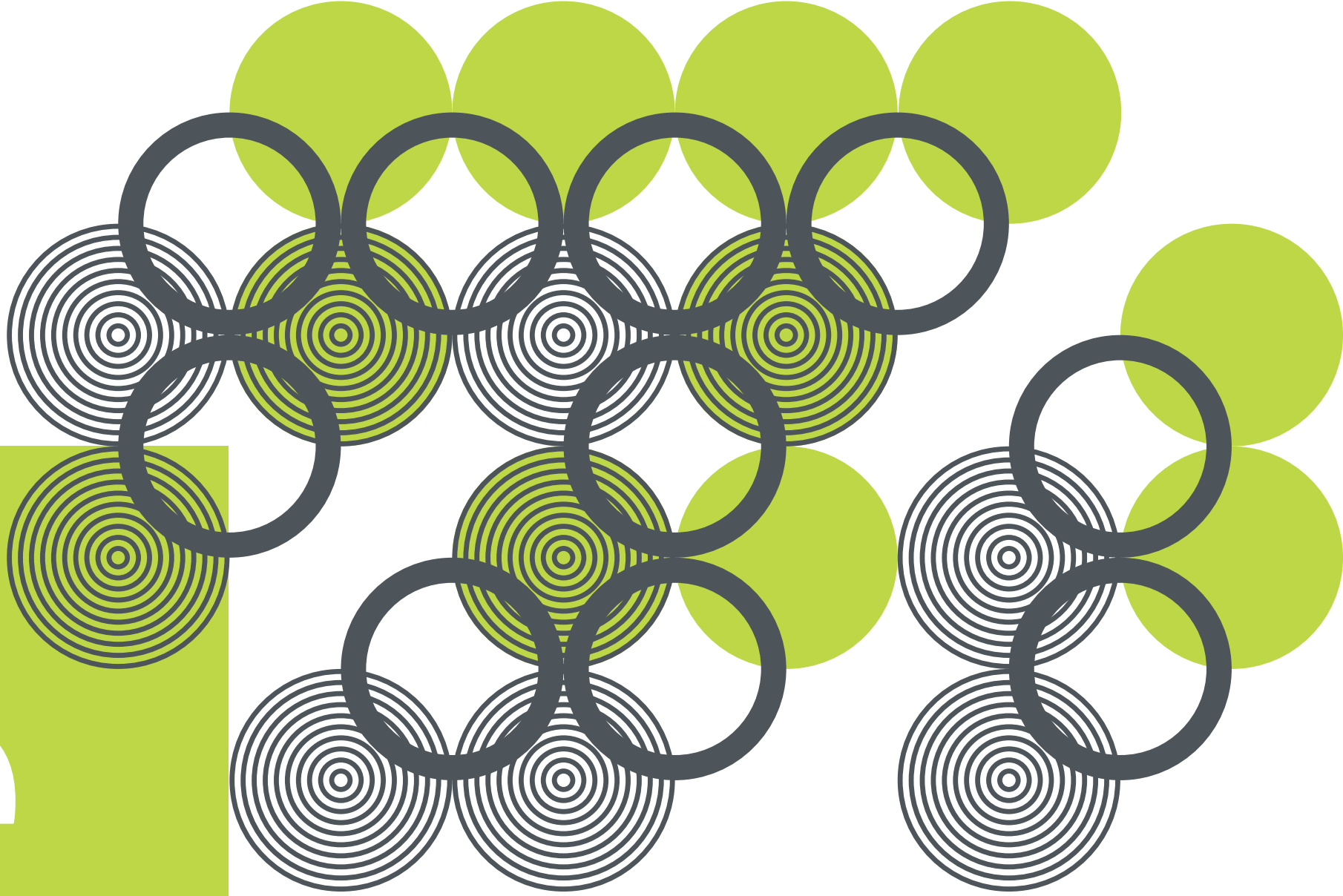
The DPC engaged further with the Council following the inspection and thereafter confirmed that the Council had brought its processing into compliance with the GDPR and Data Protection Act 2018 in respect of the issues that were the subject of the DPC's Inquiry.

Maynooth University

In April 2025, the DPC concluded its enforcement process following a Final Decision adopted by the DPC in November 2024. That Decision concerned an Inquiry regarding Maynooth University. The Inquiry related to a personal data breach notified by Maynooth University in November 2018. The breach affected the email accounts of a number of university employees.

The DPC assessed Maynooth University's technical and organisational measures for ensuring the security of personal data that it processed, and examined compliance with the controller's obligation to notify breaches promptly. The DPC found that Maynooth University had infringed Articles 5(1)(f), 32 and 33 of the GDPR. The DPC reprimanded Maynooth University, imposed administrative fines totalling €40,000 and ordered Maynooth University to bring its processing into compliance with the security requirements of the GDPR.

In January 2025, Maynooth University **submitted a report to the DPC** detailing revised technical and organisational measures for security, training for staff and students, and ensuring compliance with GDPR requirements. The measures include the use of Multi-Factor Authentication, a review of anti-malware measures and policies, security updates for software and changes to password policies. The DPC analysed Maynooth University's updated security measures and found that Maynooth University had complied with the DPC's order.



9.

Litigation

6. Litigation

Judgments Delivered and Final Orders made in 2025

No. 1

Record No.
[2023] 341 JR

Title
European Center for Digital Rights (NOYB) v Data Protection Commission

Type of action and venue
Judicial Review – High Court

Date of Judgment/Order
16 January 2025

Current Status
Proceedings concluded

Outcome:
By Order made on consent on 16 January 2025, the High Court struck out NOYB's judicial review, NOYB having agreed to withdraw the proceedings rather than pursuing them through to trial.

In the proceedings, NOYB had challenged the DPC's alleged failure to investigate a series of additional 'discrete issues' said to arise in connection with three complaints previously made by NOYB against Facebook, Instagram and WhatsApp respectively, and in respect of which the DPC had already adopted Decisions containing findings adverse to those controllers.

The proceedings were fully opposed by the DPC on all grounds.

By agreement, the Court also directed NOYB to make a contribution to the DPC's costs in a fixed amount.

No. 2

Record No.
General Court Record Nos.
T-70/23,
T-84/23,
T-111/23

Title
Data Protection Commission v European Data Protection Board

Type of action and venue
Appeal – EU General Court

Date of Judgment/Order
29 January 2025

Current Status
Proceedings concluded

Outcome:
By judgment delivered on 29 January 2025, the General Court of the European Union (CJEU) dismissed an action brought by the DPC against the European Data Protection Board (EDPB) in Joined Cases T 70/23, T 84/23 and T 111/23.

The proceedings concerned the DPC's challenge to one sub-element of a suite of Decisions adopted by the EDPB on 5 December 2022 in respect of certain complaints lodged from NOYB. In the Decisions in question, the EDPB had directed the DPC to carry out fresh investigations in respect of the processing of special categories of personal data by the controllers of the Facebook, Instagram and WhatsApp platforms in particular contexts. (The DPC had earlier found that, contrary to Article 6 of the GDPR, the controllers in question were processing 'non-special category data' for behavioural advertising purposes without a legal basis).

In the proceedings before the General Court, the DPC argued that the EDPB had exceeded its authority under Article 65(1)(a) of the GDPR, contending that binding Decisions of the EDPB cannot require the investigation of additional issues or the delivery of draft Decisions in respect of such issues.

The Court disagreed, holding that a 'relevant and reasoned objection' under Article 4(24) of the GDPR may address the scope of an investigation, thereby authorising the EDPB, when adopting a binding Decision under Article 65(1)(a) of the GDPR, to direct a Lead Supervisory Authority to extend the scope of its investigation and associated analyses and, if necessary, to conduct fresh investigations and deliver a follow-on draft Decision to the Article 60 cooperation procedure. The Court also elaborated on the operation of the cooperation and consistency mechanism under Chapter VII of the GDPR.

The DPC's complaint was therefore dismissed. Costs were also awarded against the DPC.

No.3

Record No.
[2024] 3881

Title
Mullan & Mullan v Data Protection Commission

Type of action and venue
Statutory Appeal – Circuit Court

Date of Judgment/Order
26 February 2025

Current Status
Proceedings discontinued

Outcome:
On 26 February 2025, the Circuit Court made an Order recording the fact that an appeal brought by the plaintiffs against a Decision of the DPC made on 16 August 2024 had been discontinued.

The Decision under appeal was concerned with two related complaints investigated by the DPC under the pre-GDPR regime relating to the processing of the Appellants' personal data during a receivership.

The DPC's Decision contained eight formal findings, upholding certain elements of the complaints but rejecting others. Notably, the DPC found that the controller had failed to provide information it was obliged to provide to the data subjects under section 2D of the Data Protection Acts 1988 and 2003 and had unlawfully disclosed personal data in 2015. Separately, it found that the controller had a lawful basis for obtaining and processing the Appellants' data for the purposes of the receivership.

Papers were filed by the DPC in opposition to the appeal on 15 January 2025. Before the proceedings next came before the Court on 26 February 2025, it became clear that the Appellants no longer intended to pursue their appeal. On that date, the proceedings were duly marked as having been discontinued.

No.4

Record No.
[2022] 699 JR

Title
McShane v Data Protection Commission (and HSE)

Type of action and venue
Judicial Review – High Court

Date of Judgment/Order
3 April 2025

Current Status
Proceedings concluded

Outcome:
On 3 April 2025, the High Court (O'Donnell, J.) refused an application for judicial review brought by Mr McShane, challenging a Decision of the DPC made on 23 May 2022, in respect of a complaint made by Mr McShane further to the May 2021 cyber-attack on the HSE.

In its decision, the DPC determined that the HSE was not a 'data controller' for any non-work personal data stored on a work phone issued by the HSE to its employee, Mr McShane. Accordingly, it had dismissed the complaint.

In his proceedings, Mr McShane alleged (amongst other things) that, in its examination of his complaint, the DPC had misapplied the GDPR.

In its judgment, the Court held that the DPC acted lawfully and proportionately in its handling of the complaint as presented, which focused on non-work-related personal data said to have been held on Mr McShane's work phone. The Court accepted the DPC's view that the HSE was not to be treated as a controller of that data because it did not determine the purposes and means of the data processing. The Court rejected arguments that the DPC was obliged to conduct a broader Inquiry into the HSE's processing of Mr McShane's work-related data, noting that such issues were outside the scope of the complaint. The application for judicial review was therefore dismissed.

On 3 June 2025, the Court directed Mr McShane to pay the DPC's costs (and those of the HSE) from the date leave was granted (3 November 2023).

Mr McShane subsequently appealed the High Court's Judgment and Orders to the Court of Appeal.

No. 5

Record No.
[2025] IECA 97

Title
Meta Platforms Ireland Limited v Data Protection Commission

Type of action and venue
Appeal from High Court – Court of Appeal

Date of Judgment/Order
12 May 2025

Current Status
Proceedings concluded

Outcome:
On 12 May 2025, the Court of Appeal found in favour of the DPC, in an appeal brought by the DPC against an earlier Judgment (and related Orders) of the High Court.

In its earlier application, Meta Platforms Ireland Limited had asked the Court to adjourn and/or stay Meta's appeal against a particular Decision of the DPC (in which the DPC had made findings against Meta), pending the determination of other, unrelated proceedings presently pending before the CJEU *(WhatsApp, Case T 709/21)*.

The DPC opposed that application, contending that the appeal should proceed to hearing, whether in whole or in part.

The High Court had granted the general adjournment sought by Meta. The DPC duly appealed.

In its judgment of 12 May 2025, the Court of Appeal set aside the High Court's judgment, noting that:

- the discretion to stay proceedings must be exercised sparingly and only where necessary to avoid injustice;
- Meta had not demonstrated that continuation of the Irish proceedings would cause prejudice or duplication that could not be managed by case management measures; and
- the existence of related EU proceedings did not justify a blanket stay, particularly where the issues were not identical and the DPC's statutory functions would be impeded.

On costs, the Court ruled that the DPC was entirely successful in defending the applications before it and so was entitled to recover its costs in both the High Court and the Court of Appeal.

No.6

Record No.
[2025] IECA 195

Title
Nowak v Data Protection Commissioner

Type of action and venue
Appeal from High Court – Court of Appeal

Date of Judgment/Order
19 September 2025

Current Status
Proceedings concluded subject to the Supreme Court's consideration of an application for leave to bring a further appeal to that court

Outcome:
On 19 September 2025, the Court of Appeal (Faherty, A. and Meenan, JJ.) delivered judgment dismissing Mr Nowak's appeal against a Judgment and Order of the High Court, in which the High Court had in turn upheld the Circuit Court's dismissal of Mr Nowak's appeal against a Decision of the DPC made on 21 April 2022.

The DPC's Decision of 21 April 2022 originated in a complaint made by Mr Nowak to the DPC in 2010 in which he alleged that Chartered Accountants Ireland had wrongly refused access to certain of Mr Nowak's examination scripts, in response to a data subject access request made by Mr Nowak.

While, following a ruling of the CJEU in Case *C 434/16*, Mr Nowak had long-since secured access to his examination script, Mr Nowak later alleged that the DPC had failed to address five other issues said to arise from his original complaint.

In its decision of 21 April 2022, the DPC examined the five issues in question, ruling against Mr Nowak on each one.

Appeals by Mr Nowak against that Decision were rejected by the Circuit Court (on 9 October 2023) and the High Court (on 2 July 2024).

The Court of Appeal rejected Mr Nowak's further appeal to that Court, upholding the DPC's analysis of all five of the follow-on issues raised by Mr Nowak.

By further Order dated 28 October 2025, the Court directed Mr Nowak to pay the DPC's costs of the appeal, to be adjudicated in default of agreement.

Mr Nowak subsequently applied for leave to bring a further appeal to the Supreme Court, which application was pending at year's end.

No. 7

Record No.
[2024] 533 MCA and [2025] 6 MCA

Title
Meta Platforms Ireland Limited v Data Protection Commission

Type of action and venue
Statutory Appeal – High Court

Date of Judgment/Order
31 October 2025

Current Status
Proceedings ongoing in relation to costs

Outcome:
By Consent Order made on 25 June 2025 in an (unrelated) appeal brought by LinkedIn Ireland Unlimited Company against a Decision of the DPC, the High Court directed that four identified issues should be determined prior to any hearing of LinkedIn's underlying or substantive appeal. (In essence, those issues are concerned with identifying the nature/type of appeal that may be brought by a controller against a decision of the DPC in a case where the DPC has found that the controller has infringed one or more identified provisions of the GDPR and has imposed an administrative fine in respect of such infringements.)

On 31 October 2025, the High Court (Cahill, J.) delivered an ex-tempore judgment refusing Meta's application for a trial of the same four preliminary issues in the context of two separate appeals brought by Meta Platforms Ireland Limited against Decisions of the DPC.

In the context of its application, Meta argued (amongst other things) that, for reasons of fairness and proportionality, Meta should be heard in relation to LinkedIn's preliminary issues, either at the same time as those issues were being considered in the context of LinkedIn's proceedings, or immediately thereafter.

The DPC (and the State) opposed Meta's application, contending that, in the usual way, Meta had no entitlement to be heard in another party's proceedings; accordingly, it should simply await the outcome of the trial of LinkedIn's preliminary issues. The Court also accepted that a trial of the same preliminary issues in the context of Meta's appeal would give rise to duplication and would therefore impose an undue burden on the Court and the parties. For these and other reasons, the Court refused Meta's application.

Issues in relation to the costs of the application had not yet been decided by year's end.

No. 8

Record No.
[2025] IEHC 619

Title
TikTok Technology Limited and TikTok Information Technologies UK Limited v Data Protection Commission

Type of action and venue
Statutory Appeal – High Court

Date of Judgment/Order
13 November 2025

Current Status
Interim stay granted; appeal pending

Outcome:
On 30 April 2025, the DPC adopted a final Decision in which it made certain findings adverse to TikTok in relation to data transfers to China. Amongst other things, those findings related to the processing of TikTok's EEA users' data in China in circumstances where, although stored on servers located in other countries, the data is remotely accessed from (and is processed in) China. Such access is facilitated by means of a 'remote access solution' implemented by or on behalf of TikTok and which is said to feature a suite of technical and other controls.

On foot of its findings of infringement, the DPC made an Order requiring TikTok to bring its processing of such data into compliance within a period of six months ('the Corrective Order'). It also directed TikTok to suspend its transfers of EEA user data to China in the event that compliance was not achieved within that six-month period ('the Suspension Order').

Separately, the DPC imposed administrative fines in the aggregate amount of €530 million.

TikTok appealed against the DPC's Decision. In circumstances where that appeal would not come on for hearing for some time, TikTok separately brought an application to stay the coming into effect of the Suspension Order and the Corrective Order pending the outcome of the appeal. In the context of that application, it contended (amongst other things) that compliance with the Suspension and Corrective Orders would require it to take irreversible steps, including relocating thousands of staff, incurring billions of dollars in costs and degrading service quality for its users.

The DPC opposed TikTok's application for a stay, citing, amongst other things, risks to the fundamental rights of TikTok's EEA user-base if transfers of data to China were not brought to a halt within the timeframe identified in the DPC's decision.

Following a hearing conducted over four days in early October 2025, the High Court (Mulcahy, J.) delivered judgment on 13 November 2025. The Court acceded to TikTok's application, suspending the coming into effect of the Suspension and Corrective Orders subject to certain conditions. Specifically, the Court directed that additional information be communicated by TikTok to its EEA user-base in relation to the transfer of their data to China; the Court also directed TikTok to undertake to take all reasonable steps to ensure that its underlying appeal against the DPC's Decision would be heard as soon as practicable.

TikTok were awarded their costs of the stay application. The DPC appealed against the Judgement and Order of the High Court. By determination delivered on 23 December 2025, the Supreme Court granted leave for the hearing of an appeal by that Court (as opposed to the Court of Appeal).

No. 9

Record No.
[2024] 1279

Title
Dáil Éireann & Ors v Data Protection Commission

Type of action and venue
Statutory Appeal – Circuit Court

Date of Judgment/Order
25 November 2025

Current Status
Proceedings concluded

Outcome:
Statutory appeal brought under Section 150 of the Data Protection Act 2018 against an Enforcement Notice issued by the DPC on 16 February 2024. That Notice directed the Houses of the Oireachtas to comply with a Subject Access request submitted by an identified data subject in July 2018. (The Oireachtas had declined to engage with the access request in question on the basis of its view that any processing of personal data by the Oireachtas fell outside the scope of EU law and/or the exercise by the data subject of their right of access was restricted by Sections 60 and/or section 43 of the 2018 Act.)

Subsequent to the bringing of its appeal, and reflecting certain developments under EU law, the Houses of the Oireachtas took steps to deal with the access request in issue on its merits. On the basis of the parties' shared view that this rendered the Enforcement Notice moot, the Oireachtas agreed to discontinue its appeal. An Order was duly made by the Circuit Court to that effect on 25 November 2025.

The Court made no Order as to costs.

No. 10

Record No.
[2024] 580 MCA

Title
LinkedIn Ireland Unlimited Company v Data Protection Commission

Type of action and venue
Statutory Appeal – High Court

Date of Judgment/Order
2 December 2025

Current Status
Judgment pending

Outcome:
Statutory appeal under sections 142 and 150 of the Data Protection Act 2018 against the DPC's Decision of 22 October 2024. In that Decision, the DPC found infringements by LinkedIn of Articles 5(1)(a), 6(1)(a), 6(1)(b), 6(1)(f), 13(1)(c), 14(1)(c) of the GDPR in connection with its processing of platform users' personal data for behavioural analysis and targeted advertising purposes. As one element of its analysis, the DPC concluded that LinkedIn could not validly rely on the 'consent', 'contractual necessity' or 'legitimate interests' legal bases for the processing operations under examination.

On foot of these findings of infringement, the DPC went on to make an Order requiring LinkedIn to bring its processing into compliance and to amend its privacy policy. It also imposed administrative fines in the aggregate amount of €310 million.

LinkedIn brought an appeal against all aspects of the DPC's decision on 18 November 2024.

On 25 June 2025, the High Court (Gearty, J.) directed, with the consent of the parties, that four discrete issues arising in the appeal should be determined before the appeal proper is brought on for hearing. The preliminary issues in question include the following:

- whether, in a case where a decision of the DPC imposes an administrative fine, the entirety of any appeal against that Decision can be brought under Section 142 of the 2018 Act, or whether that section is limited to dealing solely with the administrative fine element of the DPC's decision, with other points of appeal to be addressed under Section 150 of the 2018 Act;

- the standard/scope of review applicable under each of Sections 142 and 150 of the 2018 Act; and

- whether, for the purposes of any appeal, the Court may admit new evidence and arguments that had not been raised before the DPC.

A trial of these preliminary issues was conducted over three days commencing on 2 December 2025. (The Attorney General was joined to the hearing of the application given the constitutional and EU law dimensions raised).

The Court had reserved its Judgment by year-end.

No.11

Record No.
[2025] 5323

Title
City of Dublin Education and Training Board v Data Protection Commission

Type of action and venue
Application for Confirmation of Administrative Fine – Circuit Court

Date of Judgment/Order
16 December 2025

Current Status
Concluded

Outcome:
Application by the DPC under section 143(1) of the Data Protection Act 2018 for an Order confirming its Decision of 18 June 2025 to impose certain administrative fines on the Respondent following an Inquiry into a personal data breach notified on 16 November 2018.

In its Decision, the DPC found infringements of Articles 5(1)(f), 32(1), 32(2), 33(1), 34(1) and 34(4) of the GDPR, including a failure to implement appropriate security measures, a failure to notify the breach without undue delay, and a failure to communicate the breach to affected data subjects when directed.

As well as issuing a reprimand under Article 58(2)(b) of the GDPR, and an Order directing the controller to bring its processing into compliance under Article 58(2)(d) of the GDPR, the DPC imposed administrative fines on the controller totalling €125,000.

Under section 143(1), the DPC is required to apply to the Court for confirmation of its decision to impose an administrative fine. In the present case, that application was heard by the Circuit Court (unopposed) on 16 December 2025. The Court duly confirmed the fines imposed by the DPC and awarded the DPC its costs of the application.

Supervision

7.

7. Supervision

Proactive engagement with the data controllers and processors regulated by the DPC provides opportunities to advocate for the protection of individuals' data rights and to prevent potential infringements before they occur. Interacting with organisations through consultative engagement and supervisory interventions leads to better outcomes for individuals and the public as a whole. This proactive, preventative approach is a central element of the DPC's regulatory toolkit.

Alongside supporting organisational data protection compliance, proactive engagement allows the DPC to identify concerns early and recommend mitigating or remedial actions prior to the commencement of data processing. This approach also allows the DPC to take appropriate action where engagement indicates that an organisation may be infringing, or be likely to infringe, data protection law. This ensures that regulatory resources are directed where they can have the greatest impact, delivering better results for all stakeholders.

This engaged approach to supervision and consultation implements the DPC's functions under the GDPR to raise the awareness of controllers and processors of their data protection obligations, and also to monitor relevant technological, commercial, and other developments insofar as they have an impact on the protection of personal data. In a rapidly changing technological environment, it is incumbent on the DPC to keep pace with innovation. Direct engagement with stakeholders is an important part of this.

Through constructive supervisory and consultative engagement, the DPC can understand how organisations process personal data and fulfil their responsibilities as data controllers. By building open, and communicative relationships with stakeholders, the DPC can work to strengthen compliance, accountability, and a culture of data protection awareness in all sectors. In 2025, the DPC was able to dedicate additional resources to sectoral outreach and engagement, developing new relationships and reaching out to stakeholders in innovative ways. In 2026, the DPC aims to continue in this manner, and to continue to improve data protection compliance by providing support and guidance to organisations.

The DPC had 1,222 supervision engagements during 2025.

The sectoral breakdown is as follows:

Law Enforcement 80	**Health** 123	**Public Sector** 162
Charities/Voluntary Bodies 191	**Children/Family** 41	**Private Sector & Financial** 127
Multinational Technology 498	**Total** 1,222	

In addition, across all sectors the DPC engaged in **280** supervision meetings with organisations in 2025. It can be observed from the above that a significant amount of DPC engagement is with the multinational technology sector. This proactive engagement involves regular consultation, engagement and follow-up, both with the controllers involved and the DPC's peer regulators, with the aim of ensuring regulatory consistency across the European Union.

Of the 498 Multinational Technology Supervision engagements, 352 were directly related to tech companies.

152 (43%) were reactive
(i.e multinational tech companies reaching out to the DPC

200 (57%) were proactive
(i.e. the DPC actively contacting the data controller)

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 (such as a statutory Code of Practice) that will involve data processing. The scope of this obligation is broad, as it applies to all legislation affecting the processing of personal data. However, it is particularly important where legislation aims to introduce a new legal basis for the processing of personal data by public bodies or to restrict the rights of individuals under data protection law.

Where legislation aims to provide a new legal basis for processing personal data, it must meet the requirements that are set out in the GDPR. It must be shown that the data processing is necessary to achieve a clearly articulated objective in the public interest, and will not have a disproportionate impact upon affected persons. Furthermore, the legislative measure should be clear and precise in setting out how personal data will be processed, leading to a foreseeable outcome for individuals. If legislation aims to provide a legal basis for processing special categories of personal data, in addition to the general requirements, it must also provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Should a legislative measure aim to restrict the rights of data subjects, the DPC advises drafters on how to meet the requirements of Article 23 of the GDPR to ensure that any restriction is necessary and proportionate in safeguarding a clear public interest and respects the essence of the fundamental rights and freedoms in question.

In addition to consultation on primary and secondary legislation, the DPC also engages with stakeholders on Codes of Practice governing the processing of personal data, and ancillary documentation such as data protection impact assessments. This assists in ensuring that data will be processed lawfully by public bodies when new legislation becomes operative.

In 2025, the DPC provided guidance and observations on **77** proposed legislative and regulatory measures including:

- Roads 1993 Act, as amended by the 2023 Act (Road Traffic Collision Data Sharing);
- European Single Access Point Omnibus Directive, amending IORP II Directive (2016/2341);
- European Union (Internal Market in Electricity) (No. 2) Regulations 2022 Statutory Instrument No. 37 of 2022 (S.I.37/2022) - Smart Meter Access Codes;
- CRMS 2268/2025 FB25 Amendment Section 851A Taxes Consolidation Act (De Minimis Regulation);
- Automatic Enrolment Retirement Savings System Regulations 2025;
- Health (Amendment) (Home Support Providers) Bill 2025;
- Construction Safety Licensing Bill 2023;
- Road Transport (Operator's Licence Application) (Amendment) Regulations 2024;
- Apartments and Duplex Defects Remediation Bill 2025;
- Planning and Development (Strategic Environmental Assessment) Regulations 2025; and
- Proceeds of Crime (Amendment) Bill.

Public Service Transformation and Engagement

Throughout 2025, the DPC actively engaged with a range of public sector bodies and government departments across several major projects and working groups. This included engagement on the planned **publication of the 1926 Census by the National Archives**, to ensure that the data protection rights of centenarians included in the Census were adequately addressed. The DPC also participated in an advisory capacity to the Public Sector Data Strategy Working Group of the Department of Public Expenditure, Infrastructure, Public Service Reform and Digitalisation. The Strategy aims to enhance quality, accessibility, and efficiency of public services for citizens. The DPC welcomes the opportunity to contribute expertise in these projects, and to assist in ensuring data protection considerations are at the forefront.

Across these engagements, the DPC provided guidance on embedding data protection by design and default, and ensuring that safeguards are in place to protect data subjects. The DPC will continue to collaborate with public sector bodies to ensure that data protection remains at the core of projects, while promoting the development and delivery of improved public services.

Company Law Review Group and Publication of Personal Data

In May 2025, the DPC was invited by the Company Law Review Group (CLRG) to attend its Corporate Governance Meeting (CGM) to discuss the publication of residential addresses of company directors as prescribed by the Companies Act 2014. The CLRG invited the DPC for the purposes of providing advice on the data protection implications arising from this matter.

While the Companies Act 2014 creates a legal obligation for the Companies Registration Office (CRO) to process the personal data of company directors by publishing their residential address on a public register, questions have arisen as to whether this processing meets the requirements of data protection law to be necessary and proportionate to achieve a purpose in the public interest.

As part of its consideration, the DPC examined whether the safeguards, provided under section 150(11) of the Companies Act 2014, which allows a director to apply for the removal of their residential address from the register on the basis of risk, (significant threat to their personal safety) are effective in their application.

The DPC's advice to the CLRG focussed on ensuring that the legal obligation to publish personal data **should be assessed in relation to its necessity and proportionality in ensuring transparency** in relation to the directorship of companies, and that any **safeguards** should be assessed for their genuine effectiveness in addressing the risks identified arising from the publication of personal data.

In September 2025, the CLRG issued a report which adopted the views outlined by the DPC at the CGM and recommended that the legislation be amended to preclude availability of residential addresses on the CRO register.

This engagement reflects the DPC's approach to the topic of the publication of personal data by public bodies in general, where it is important that the public interest in openness and transparency is adequately balanced with the **fundamental rights of individuals**, and their legitimate concerns regarding public access to their personal data.

From left to right: Commissioner Des Hogan, Assistant Commissioner Clare Barry, Tim Hanly National Safeguarding Office, HSE, Babiana Savin CEO Sage Advocacy and Deputy Commissioner David Murphy at the launch of the DPC's Adult Safeguarding Toolkit, July 2025.

Adult Safeguarding Toolkit

In 2025, the DPC continued to **prioritise the protection of vulnerable adults** in line with its Regulatory Strategy 2022-2027. A key milestone was the publication of the Adult Safeguarding Toolkit in July 2025. Developed following extensive cross team collaboration and engagement with relevant stakeholders (including advocacy groups, service providers across the public, private and voluntary sectors, alongside other relevant regulatory bodies), the Toolkit provides practical guidance on different aspects of data protection law in the specific context of Adult Safeguarding. It provides FAQs addressing common queries received by the DPC from the health sector, and resources to support organisations working with at-risk adults.

Adult Safeguarding Toolkit

To support the launch, **the DPC hosted a stakeholder event** in its Pembroke Row offices attended by over **120 representatives** across healthcare providers, social care organisations, legal, professional, advocacy bodies and media representatives.

Following publication of the Toolkit, the DPC undertook a number of outreach events to assist organisations in applying the guidance in practice. These included presentations delivered to social workers in the Cork and Kerry region, as well as delivering workshops at the HSE's National Learning and Development Seminar in Galway.

The DPC also met with Nursing Homes Ireland and the Decision Support Service to explore areas for future collaboration in 2026 on adult safeguarding matters.

Sports Sector Engagement

Following on from 2024's work with the sports sector and in line with Goal 4 of the Regulatory Strategy 2022-2027, the DPC continued to strengthen its engagement and support for organisations across the sporting landscape. Building on positive momentum generated in 2024, the DPC established a dedicated focus group comprising 20 National Governing Bodies (NGBs) and Local Sports Partnerships (LSPs).

Throughout the year, the group met on several occasions to discuss emerging challenges, real-life issues facing sports bodies, and practical ways in which the DPC can assist.

In direct response to feedback from the focus group, the DPC hosted the ***Kick Start Compliance: Data Protection in Sport*** **all island conference** on the 28th of November in Croke Park – **the first event of its kind delivered by the DPC, and with contributions from the Information Commissioner's Office (ICO) branch in Northern Ireland.** The event brought together experts from across data protection, sport, and technology, including former professional athletes, offering sessions on practical GDPR implementations and the deployment of new technologies. The conference also addressed the complex area of children's data processing and the interplay with safeguarding.

To complement this work, the DPC published a series of concise, easy-to-use infographics tailored specifically for the sports sector. These resources were developed following feedback from the focus group who emphasised the need for simple, accessible guidance to help organisations navigate their data protection obligations. As part of its ongoing resources for those working with personal data, the DPC has made the recordings of the conference available on its website under the tab 'For Organisations'.

Recordings of the Kick Start Compliance Conference

Infographics from the Kick Start Compliance Conference

From left to right: Anna Morgan (Bird & Bird's International Privacy and Data Protection Group), Caroline Mooney (ICO), Kelly Cunningham (GAA), Jenny Dolan (DPC), Colin Gorman (TUSLA) at the Kick Start Compliance Conference, November 2025.

From left to right: Dale Sunderland (DPC), David Murphy (DPC), Ellen Hayes (Sport Ireland), Caroline Mooney (ICO), Des Hogan (DPC), Kate Colleary (Pembroke Privacy) at the Kick Start Compliance Conference, November 2025.

Charities Engagement

In line with Goal 5 of the DPC's Regulatory Strategy 2022-2027, which commits to supporting organisations of all sizes and driving compliance, **the DPC delivered several online sessions tailored for charities and voluntary organisations** throughout 2025. These sessions built upon the DPC's 2024 engagement and directly addressed the data protection challenges faced by the not-for-profit sector. Recognising the unique challenges facing the sector, the DPC embarked on an extensive engagement programme to support these vital organisations in meeting their data protection obligations. Many of the charities with which the DPC engaged provide services in the areas of health and social care, and work with vulnerable and at-risk service users in a variety of contexts. This can present additional challenges in terms of processing special category data for these organisations.

As part of this commitment, the DPC delivered seven in-person *Let's Talk Data Protection* sessions in partnership with the Charities Institute Ireland, in different regions of the country. The DPC also contributed an article to the *Charity Leader*, the Charities Institute Ireland's magazine for nonprofit leaders, on key data protection recommendations for charities.

The DPC also engaged with several major organisations in the charities sector to deliver bespoke, online presentations for their members. In May, the DPC delivered a webinar to registered bodies with the Charities Regulator entitled titled *Data Protection for Charities*, and in October delivered an online session to charities affiliated with the Carmichael Centre, entitled *Navigating AI and Data Protection*.

The online and in-person presentations covered crucial topics for charities such as data breaches, requests from law enforcement bodies such as An Garda Síochána for information on service users, use of AI, and data subject access requests from clients.

Stakeholder engagement in the sector was also enhanced in 2025 by the participation of DPC staff in an information stand at *The Wheel Summit 2025: Thriving Through Change* which took place in May in Croke Park.

Partnering with organisations such as Carmichael, The Wheel, and Charities Institute Ireland enables the DPC to greatly increase both the quality and quantity of engagement with the charity sector.

Data Protection Toolkit for Schools

Protecting children's personal data is one of the five strategic goals of the DPC's 2022-2027 Regulatory Strategy. Acknowledging the challenges that schools, particularly smaller schools, face on a day-to-day basis in ensuring compliance with their **data protection obligations towards children, the DPC published a new Data Protection Toolkit for Schools** (the Toolkit) resource in late 2024. Given the importance of the protection of children's personal data under the GDPR, this resource was focused on the processing of student/children's personal data within a school environment.

Data Protection Toolkit for Schools

Following the Toolkit's publication, the DPC began the task of promoting the resource within the education sector throughout 2025, in particular through collaboration with Education Support Centre Ireland's (ESCI) regional centres across the country. With these centres' support, the **DPC presented a series of workshops and information sessions to school leadership, at both primary and post primary levels**, addressing various topics from the Toolkit.

In addition to its collaboration with the ESCI, the DPC attended a number of education sector focused conferences and conventions to promote awareness of the Toolkit and address concerns school leadership may have in a more informal setting.

Schools' Processing of Personal Data During Pre-Enrolment

During 2025, the DPC engaged with a number of primary schools following concerns brought to the DPC's attention regarding the collection of personal data, including special category data, during the pre-enrolment stage of the admissions process. These concerns highlighted issues around the volume and type of data being requested before any school place had been offered or accepted.

Through this engagement, the DPC observed varying practices across schools in relation to the information requested at the pre-enrolment stage, including having a valid legal basis for processing special category data at this stage. Some schools also referenced the use of standardised templates within school administration platforms, which may inadvertently have led to the inclusion of fields seeking data that was not necessary or appropriate at this stage of the admissions process.

To support schools in meeting their obligations under the GDPR, and to encourage a more proportionate approach to data collection during pre-enrolment, **the DPC published a blog post—*Processing Personal Data During Pre-Enrolment: What Schools Need to Know***—on its website in 2025. The blog provides practical guidance on what information schools should and should not request at the pre-enrolment stage, outlines the relevant GDPR principles, and includes key questions schools can use to assess whether their data collection practices are necessary, lawful and transparent.

Blog: Processing Personal Data During Pre-Enrolement: What Schools Need to Know

CCTV and Schools

2025 saw a number of concerns raised regarding the processing of personal data in schools via CCTV systems, in particular, where the cameras were located within the vicinity of bathrooms. The DPC engaged with numerous schools regarding these data processing practices.

While the use of CCTV in schools is not prohibited, it is important for schools to have appropriate safeguards in place. This includes:

- conducting a **Data Protection Impact Assessment** (DPIA) prior to the deployment of such technology, to identify and mitigate any potential risks;
- having an up-to-date **CCTV Data Protection Policy** in place;
- availing of masking or privacy filter technology where required;
- having appropriate signage on display to inform people CCTV is in operation; and
- ensuring **appropriate security** of the data being processed by way of the CCTV system.

Further guidance on CCTV usage can be found in the DPC's Data Protection Toolkit for Schools and guidance note CCTV Guidance for Controllers.

Data Protection Toolkit for Schools

CCTV Guidance for Controllers

Compliance Sweep of Supermarket and Convenience Store Sector

Following the initial compliance sweep of the Irish Retail Sector in 2024 with the objective of gaining deeper insights into the sector's personal data processing activities and compliance levels, **the DPC advanced its supervisory activities in 2025 by engaging directly with supermarket and convenience store controllers**. These controllers, which have a significant footprint in data processing across Ireland, included:

- primary market leaders (holding a combined 66.8% market share[4]);
- discount retail operators;
- convenience and specialised retail networks; and
- international retail operations.

The review greatly enhanced the DPC's understanding of the sector and its associated data processing activities. It identified emerging technological developments and data processing practices influenced by economic pressures, highlighting the need for ongoing review to ensure sustained compliance and the protection of data subjects' rights.

The review identified several significant sectoral data protection developments, including:

- the recognition, for certain retail brands, that **loyalty applications and websites function as separate data controllers** from their respective physical retail outlets;
- the ongoing **deployment and assessment of technological solutions to reduce economic losses** and enhance staff safety in response to rising levels of retail crime, including the increased use of body-worn cameras by security staff and the deployment of live CCTV monitoring displays at self-service checkouts to observe transactions as customers scan their purchases; and
- the **introduction and assessment of artificial intelligence technologies for image processing** in both store environments and supply chain operations.

The sector demonstrated significant engagement with data protection compliance, as evidenced by completing **835 Subject Access Requests** under Article 15 of the GDPR in the 12 months preceding engagement and conducting **215 Data Protection Impact Assessments** under Article 35 of the GDPR in the preceding three years.

The review process identified and facilitated the resolution of several material data protection compliance deficiencies across the sector, thereby advancing controllers' adherence to their obligations under the GDPR.

For example, a Data Controller submitted a Record of Processing Activities, as part of its questionnaire response, that did not comply with Article 30(1)(c) and (d) of the GDPR, as it was based on a UK template and did not adequately reflect processing operations specific to Ireland. In another matter, a Controller's Privacy Policy did not meet the requirements of Article 13 of the GDPR as it failed to provide all of the required information to individuals. Furthermore, in some instances controllers did not initially provide their Record of Processing Activities upon request by the DPC.

The supervisory review process identified and facilitated the resolution of several material data protection compliance deficiencies across the sector, thereby advancing controllers' adherence to their obligations under the GDPR.

The complexity of processing activities related to the detection and prevention of criminal activities continues to present unique data protection challenges for data controllers in the retail sector. Through its recent supervisory initiatives, the DPC has identified the urgent need for robust safeguards that both protect data subject rights and support legitimate efforts to tackle increasing retail crime. The review did not raise any concerns regarding the use of CCTV monitoring displays at self-service-checkouts or any material concerns regarding use of body-worn cameras but other technologies under consideration will be subject to further review.

4 Grocery Market Share—Worldpanel by Numerator

The DPC's commitment to collaboration and ongoing regulatory oversight will ensure sectoral reviews stay focused on improving compliant processing practices. Recognising the importance of these developments, the DPC will further strengthen its targeted engagement and guidance in this area during 2026. By maintaining continuous dialogue, assessment, and support for data controllers, the DPC remains dedicated to reinforcing sectoral resilience and promoting high standards of data protection compliance in response to evolving risks.

SME Project

Throughout 2025, the DPC made significant progress in understanding the complex landscape of data processing in micro, small and medium enterprises.

In line with Goal 5 of the Regulatory Strategy, the DPC focused on prioritising the development of guidance for micro, small and medium enterprises. In order to establish an understanding of the data protection awareness of key actors in this area, the DPC engaged extensively with representative associations including; the Small Firms Association, ISME, IBEC, Digital Business Ireland, the Freight Transport Association of Ireland, the Convenience Stores and Newsagents Association, the Local Enterprise Office, Enterprise Ireland, and Chambers Ireland. The DPC has also co-hosted a number of webinars for the sectors to enhance understanding and awareness of data protection obligations. In November, a public consultation was published to help support understanding of the challenges faced by micro, small and medium enterprise owners in complying with GDPR and their data protection obligations.

The DPC's next steps will include a complete review of the findings of the consultation and continued engagement with the sector to assist with the development of tailored guidance and toolkits.

Transact Payment Malta Limited: Protected Disclosure

In 2023, the DPC received a protected disclosure related to a number of credit unions who, by virtue of their Programme Authorisation Agreement with Transact Payments Malta Limited (TPML), were required to forward a copy of Suspicious Transaction Reports to the money laundering reporting office of TPML which is located in Malta. The disclosure raised concerns that, by requiring credit unions to provide TPML with suspicious transaction reports, TPML was requiring credit unions to disclose personal data which, without a substantive legal or legislative basis for dual STR reporting under AML laws, was an act of excessive, disproportionate and unnecessary processing of personal data under the GDPR.

Following engagement with PAYAC Services CLG, who acted as a commercial intermediary in the relationship between TPML and the credit unions for the purpose of facilitating the relevant services, and engagement with colleagues in the Maltese Office of the Information and Data Protection Commission and the Financial Intelligence Analysis Unit in Malta, the Programme Authorisation Agreement was updated to cease the sharing of suspicious transaction reports between the credit unions and TPML.

This case highlights the importance of having robust data governance structures in place and the benefits of positive engagement with the Regulator.

Consumer Protection Code

The Consumer Protection Code, was launched in March 2025 and will come into effect in March 2026. Following feedback provided by the DPC, the Code was updated to reflect the concerns raised by the DPC concerning the **retention of personal data for six years** when an individual engages with a firm but does not proceed to become a customer i.e. when seeking an insurance quote or applying for a mortgage online. The updated consumer protection code confirms that the retention of such data for six years is not necessary or proportionate and **the updated code requires firms to retain such information for 12 months.** Such engagement as this clearly demonstrates the DPC's dedication to safeguarding the fundamental right to data protection for all.

LinkedIn: Use of First Party Data to Train AI Models

In March 2025, LinkedIn informed the DPC of its intention to train its own proprietary generative AI models using the personal data of LinkedIn members based in the EU, beginning in early November 2025. After extensive engagement with the company, the DPC identified a number of issues with the proposed processing of personal data. The DPC communicated these concerns and made a number of recommendations to LinkedIn concerning **transparency, data minimisation, special category data, and processing of data for individuals under the age of 18.**

As a result, LinkedIn adopted a number of changes to its plan, including:

- **improved transparency notices** for users helping them to understand the personal data LinkedIn will process to train its AI models and their ability to opt out if they so wish;
- **a reduction in the scope of the personal data** that LinkedIn would process to train its models, both in terms of the personal data to be used and the time period from which it proposed to draw the data;
- **improved measures to prevent** the personal data of LinkedIn users **under the age of 18** from being used to train the models; and
- **improved measures to protect users**, including through the implementation of filters to avoid the collection of potentially sensitive information shared on certain LinkedIn pages and groups, including trade union content.

The DPC has not approved or found compliant LinkedIn's use of users' personal data for generative AI model training. However, the additional measures implemented by LinkedIn have **sufficiently addressed the DPC's concerns** such that further regulatory intervention is not considered necessary at present.

The DPC will continue to monitor LinkedIn's GDPR compliance and is requiring LinkedIn to compile a report within five months of the commencement of processing which, amongst other things, will include an updated evaluation of the efficacy and appropriateness of the measures and safeguards.

Data Protection Assessment of Third-Party Developer Access to Personal Data of Meta Users – Update

In 2024, the DPC issued an Assessment to Meta containing a number of recommendations in relation to its third-party developer access to personal data. The Assessment was primarily concerned with access to personal data held by Meta which is provided to third parties as part of app development for the Meta platforms. In February 2025, Meta provided a response on the report and detailed steps it has taken to comply with the DPC's recommendations.

Based on the DPC's recommendations, Meta reviewed the existing governance and control mechanisms over third-party developer access to data, developed a new system to enable Meta to oversee implementation of its instructions on third-party risk management from end-to-end, and updated policies and procedures around compliance, enforcement, and oversight of the developer platform, app onboarding processes, and app review processes.

In addition, Meta conducted testing to ensure that the investigations and enforcement processes were operating effectively. Of particular importance, Meta confirmed that developers who fail to fully comply with the annual review processes will lose access to personal data until these processes are completed.

Another concern held by the DPC related to Meta's ability to identify a developer who sought access to personal data. The DPC recommended re-evaluating the process used to identify developers and redesigned it where necessary to provide greater certainty regarding the developer's identity, thereby giving Meta a better basis for risk-assessing developers. This recommendation has been implemented through extending existing verification and checks to all developers, in addition to the introduction of a data-handling questionnaire which includes processes to verify the identity of the developer and the business they represent – as well as a risk assessment by Meta to determine whether an increased risk to the privacy of individuals is presented due to the identity of the developer.

Additionally, Meta clarified that, in order for a third-party developer to gain access to consumer data, they must complete, at a minimum, the following compliance checks:

- the successful creation and verification of a developer account;
- agreement to the Platform Terms and Developer Policies;
- completion of Business Verification; and
- completion of a data-handling questionnaire.

Meta advised that the completion of a data-handling questionnaire is now a compulsory part of its risk assessment process before advanced access is granted to a developer. This will also be incorporated into Meta's annual Data Use Checkup for all developers that have advanced access. Developers cannot complete their annual data checkup until they complete the data-handling questionnaire. If the third-party developer does not successfully complete these steps, they will not gain advanced access and can have their access revoked.

The DPC recognises that Meta has taken steps to minimise risks to individuals through the changes made on foot of the DPC's assessment. The DPC will continue to monitor Meta's GDPR compliance and will exercise further regulatory powers if necessary.

Meta: Use of First-Party Data to Train AI Models

In 2025, the DPC continued its extensive regulatory engagement with Meta regarding the company's plans to train its Large Language Model (LLM) using public content (known as first-party data) shared by adults on Facebook and Instagram across the EU.

In February 2025, the DPC received updated data protection documentation from Meta following the company's decision to pause processing in June 2024, having agreed to the DPC's original request to do so.

Meta implemented a number of measures and improvements based on the DPC's recommendations following its review of Meta's documentation and through extensive engagement with the company, including the following:

- updated transparency notices to users, including specific notifications to all users in both 2024 and 2025;
- updated and more user-friendly objection form;
- provision of longer notice period to users and information on controls available to change all published posts from public to private to avoid being trained for the model;
- ensuring objection forms work in-app, and in all jurisdictions across Europe; and
- updated its measures to protect data subjects, such as de-identification, filtering of data sets and output filters.

Additionally, the DPC required Meta to compile a report setting out the appropriateness of the measures and safeguards it has introduced. The report is due to be submitted to the DPC once a training run with EU/EEA data has been completed. As with all its engagements, the DPC has not approved or found compliant Meta's use of users' personal data for generative AI model training. The DPC will continue to monitor Meta's GDPR compliance and will exercise further regulatory powers if necessary.

Meta: Celeb-Bait

In September 2024, Meta informed the DPC that it was planning to implement facial recognition technology to help identify the presence of public figures in advertisements as a further measure to **detect when an unauthorised image is being used as 'celeb-bait'**. Celeb-bait is advertising content which features imagery of public figures, using their reputation to leverage the trust and familiarity of the public to defraud people.

Meta stated that the feature was opt-in only, limited to public figures who are over the age of 18 and whose likenesses are deemed to be at high risk of being used in celeb-bait, and who have consented to the processing of their image. Additionally, this processing would only be applied to advertisements which have been identified through other means as likely to contain scams. During this engagement with Meta, the DPC cooperated closely with the Polish Data Protection Authority which had active complaints from individuals about their images being used in celeb-bait.

Through the engagement process, the DPC identified some areas where Meta could make the information it was providing to individuals **more transparent and made several recommendations for improvements**.

In response to the DPC's transparency recommendations, Meta updated the text on the in-app notices making it clearer to individuals what photos would be processed and how long they would be retained for. Meta also updated the relevant Help Centre articles to provide clearer information to individuals regarding the retention periods for embeddings generated as part of the processing. The DPC understands that Meta began processing in the EU in March 2025.

As part of its ongoing monitoring, the DPC required Meta to compile a report which set out an updated evaluation of the efficacy and appropriateness of the measures and safeguards it has introduced. This report was received in August 2025 and later shared with European Data Protection Board colleagues. In the report Meta indicated that they had received positive feedback from a number of public figures and their teams concerning Meta's efforts to limit the issue of celeb-bait by leveraging this technology to improve detection and enforcement.

OpenAI: ChatGPT Agent

In February 2025, the DPC was informed by OpenAI of plans to launch an optional experience for individuals called ChatGPT Agent in the EU. Chat GPT Agent can perform multi-step tasks on an individual's behalf, for example finding a particular product, comparing prices for flights or booking a table in a restaurant. ChatGPT Agent is trained to ask for user confirmation prior taking significant actions, such as to complete booking reservation, or to log in into a private account. When the individual completes the action, they can hand the control back to ChatGPT Agent.

As part of the **pre-launch engagement, the DPC reviewed OpenAI's Data Protection Impact Assessment (DPIA) and other documentation**. During this review the DPC requested a technical demonstration of the back-end of ChatGPT Agent to better understand and view the guardrails that OpenAI had advised it had in place to protect individuals. OpenAI brought the DPC through a demonstration and the security measures put in place. Through this engagement, the **DPC identified several areas where improvement was needed,** specifically in relation to user transparency, including improving the basic information about the novel agentic technology being shared with individuals and improving the in-app onboarding notices to be more specific to ChatGPT Agent.

In response to DPC recommendations **OpenAI applied a number of changes**, for example:

- a revised 'safety and privacy' section in OpenAI's Help Centre article;
- an updated ChatGPT Agent onboarding experience with a 'learn more' link that directs users to the updated 'safety and privacy' section in the Help Centre article; and
- the incorporation of additional language to the in-app onboarding notices specific for ChatGPT Agent, highlighting the importance to monitor ChatGPT Agent given that it would be given significant authority to act on an individual's behalf.

OpenAI launched ChatGPT Agent feature in the EU in July 2025. The DPC will continue to monitor OpenAI's GDPR compliance.

Etsy: Chatbot

In March 2025, the DPC engaged with Etsy on the launch of a customer support chatbot in the EU. Etsy stated that it wished to utilise the chatbot to assist its EU users by providing answers to common and frequently asked questions. Etsy utilised a third-party product for this. The chatbot was trained on Etsy Help Centre articles, and other customer service repositories, on common customer queries and configured not to engage in general conversations or to use reasoning to formulate responses outside of its knowledge base.

Through its engagement with Etsy, **the DPC identified some concerns in relation to the provision of transparency and ensuring customers were informed on data protection implications** of the chatbot. In addition, the DPC had concerns about the way Etsy had chosen to communicate the retention periods associated with use of the chatbot. After assessment of the information provided by Etsy, the DPC provided recommendations in June 2025 highlighting the need for improvements in transparency, in particular that individuals would be made aware what personal data would be processed as a result of using the Etsy chatbot.

As a result of the DPC's engagement **Etsy made improvements**, including:

- a hyperlink to the Help Centre article on the initial greeting screen once the chatbot goes live; and
- express reference to the applicable retention periods for customer support information, including chat transcripts, in the Etsy Privacy Policy.

Etsy confirmed that its Privacy Policy was updated in August 2025 and the chatbot launched in September 2025. The DPC will continue to monitor Etsy's chatbot GDPR compliance.

Inter-Regulatory Affairs

Inter-regulatory cooperation was highlighted as a priority for 2025 on foot of expectations that the EU's new digital legislative package (e.g. the Digital Markets Act the Digital Services Act, amongst other new EU legislation) would bring additional complexity and volume to the DPC's workload. This has proven to be the case and during 2025, the DPC played a prominent role in providing data protection expertise and guidance to other regulators at national and EU level. From actively engaging on issues of intersection and common interest, to establishing new cooperation mechanisms and procedures, the DPC held **over 50 meetings** with peer regulators and other complaint-handling bodies in 2025.

From left to right: Commissioners Dale Sunderland, Niamh Sweeney, Des Hogan with Niamh Hodnett (CnaM) and John Evans (CnaM) signing Cooperation Agreement on the protection of children online.

Publication of Cooperation Agreement and Joint Statement with Coimisiún na Meán

October marked a key milestone in the DPC's commitment to inter-regulatory cooperation with the publication of a Cooperation Agreement with Coimisiún na Meán (CnaM), as well as a joint statement on the protection of children online.

As active regulators in the digital space, the DPC recognises the importance of working closely with CnaM on areas of potential synergy to ensure that we share expertise and deliver a coherent and cohesive approach to regulation. The objective of this Cooperation Agreement is to provide for a structured, effective working relationship between both organisations, including through the appropriate sharing of information and cooperating on matters of common interest. The DPC is committed to putting this Cooperation Agreement into action and looks forward to continued fruitful engagement with CnaM in 2026.

The DPC and CnaM also published a joint statement on advancing the safety of children and the protection of their personal data online, in line with Pillar 3 of the DPC's Regulatory Strategy, which sets out a strategic objective to prioritise the protection of children and vulnerable people. The DPC is committed to working alongside CnaM to uphold robust standards that safeguard children's rights in the digital environment, where data protection and online safety are built in from the start. This joint statement demonstrates a shared commitment to ensuring that the rights and best interests of children are respected and upheld by the online services that both the DPC and CnaM regulate.

The DPC looks forward to continued cooperation with regard to this important topic. Both organisations will have regular, structured engagement in 2026 in the context of the Cooperation Agreement, and future cooperation in relation to children may include sharing insights on emerging risks to the safety and protection of children's personal data online and joint work on educational resources relating to the protection of children online.

DPC and CnaM Cooperation Agreement

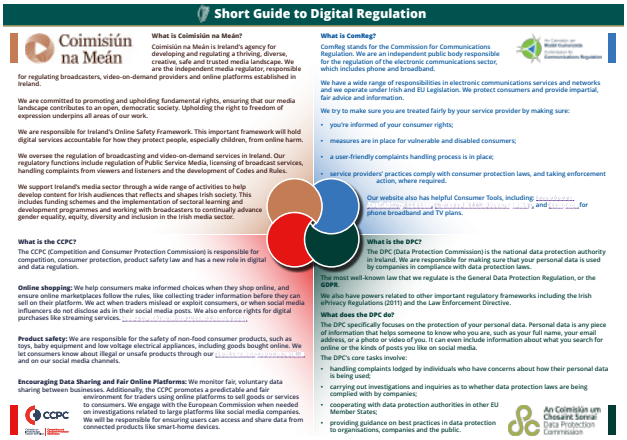
Commissioner Des Hogan participating in a panel exploring the balance between innovation and regulation at the EU Digital Summit (European Business Summits) in Brussels.

Ireland's Digital Regulators Group

The DPC continued to play an active role as a member of Ireland's Digital Regulators Group (DRG) throughout 2025. The DRG — comprising the DPC, CnaM, the Commission for Communications Regulation (ComReg), and the Competition and Consumer Protection Commission (CCPC) — is a platform for collaboration between regulators with remit over the digital space and whose work has a direct impact on Ireland's digital economy. This purpose of this group, which meets monthly, is to support a coherent and cohesive approach to digital regulation in Ireland, and to lead and develop regulatory cooperation on substantive issues of common interest arising in the digital space.

This year, DRG members collaborated to publish a Short Guide to Digital Regulation, aimed at clarifying the different roles and responsibilities of digital regulators in Ireland, and signposting to individuals the correct body to whom they should direct their queries and complaints in respect of different topics.

Short Guide to Digital Regulation


Short Guide to Digital Regulation

Coimisiún na Meán

What is Coimisiún na Meán?

Coimisiún na Meán is Ireland's agency for developing and regulating a thriving, diverse, creative, safe and trusted media landscape. We are the independent media regulator, responsible for regulating broadcasters, video-on-demand providers and online platforms established in Ireland.

We are committed to promoting and upholding fundamental rights, ensuring that our media landscape contributes to an open, democratic society. Upholding the right to freedom of expression underpins all areas of our work.

We are responsible for Ireland's Online Safety Framework. This important framework will hold digital services accountable for how they protect people, especially children, from online harm.

We oversee the regulation of broadcasting and video-on-demand services in Ireland. Our regulatory functions include regulation of Public Service Media, licensing of broadcast services, handling complaints from viewers and listeners and the development of Codes and Rules.

We support Ireland's media sector through a wide range of activities to help develop content for Irish audiences that reflects and shapes Irish society. This includes funding schemes and the implementation of sectoral learning and development programmes and working with broadcasters to continually advance gender equality, equity, diversity and inclusion in the Irish media sector.

What is the CCPC?

The CCPC (Competition and Consumer Protection Commission) is responsible for competition, consumer protection, product safety law and has a new role in digital and data regulation.

Online shopping: We help consumers make informed choices when they shop online, and ensure online marketplaces follow the rules, like collecting trader information before they can sell on their platform. We act when traders mislead or exploit consumers, or when social media influencers do not disclose ads in their social media posts. We also enforce rights for digital purchases like streaming services.

Product safety: We are responsible for the safety of non-food consumer products, such as toys, baby equipment and low voltage electrical appliances, including goods bought online. We let consumers know about illegal or unsafe products through our and on our social media channels.

Encouraging Data Sharing and Fair Online Platforms: We monitor fair, voluntary data sharing between businesses. Additionally, the CCPC promotes a predictable and fair environment for traders using online platforms to sell goods or services to consumers. We engage with the European Commission when needed on investigations related to large platforms like social media companies. We will be responsible for ensuring users can access and share data from connected products like smart-home devices.

CCPC

What is ComReg?

ComReg stands for the Commission for Communications Regulation. We are an independent public body responsible for the regulation of the electronic communications sector, which includes phone and broadband.

We have a wide range of responsibilities in electronic communications services and networks and we operate under Irish and EU Legislation. We protect consumers and provide impartial, fair advice and information.

We try to make sure you are treated fairly by your service provider by making sure:

- you're informed of your consumer rights;
- measures are in place for vulnerable and disabled consumers;
- a user-friendly complaints handling process is in place;
- service providers' practices comply with consumer protection laws, and taking enforcement action, where required.

Our website also has helpful Consumer Tools, including: , and for phone broadband and TV plans.

What is the DPC?

The DPC (Data Protection Commission) is the national data protection authority in Ireland. We are responsible for making sure that your personal data is used by companies in compliance with data protection laws.

The most well-known law that we regulate is the General Data Protection Regulation, or the GDPR.

We also have powers related to other important regulatory frameworks including the Irish ePrivacy Regulations (2011) and the Law Enforcement Directive.

What does the DPC do?

The DPC specifically focuses on the protection of your personal data. Personal data is any piece of information that helps someone to know who you are, such as your full name, your email address, or a photo or video of you. It can even include information about what you search for online or the kinds of posts you like on social media.

The DPC's core tasks involve:

- handling complaints lodged by individuals who have concerns about how their personal data is being used;
- carrying out investigations and inquiries as to whether data protection laws are being complied with by companies;
- cooperating with data protection authorities in other EU Member States;
- providing guidance on best practices in data protection to organisations, companies and the public.

An Coimisiún um Chosaint Sonraí Data Protection Commission

Economic Regulators Network

In 2025 the DPC joined Ireland's Economic Regulators Network (ERN). The ERN is an informal forum that facilitates cooperation between economic regulators on issues of common interest, in order to contribute to a better and more integrated regulatory environment in Ireland. The current membership of the ERN consists of several Irish regulators, namely, CnaM, the CCPC, ComReg, the Central Bank of Ireland (CBI), the Commission for Regulation Utilities (CRU), the National Transport Authority (NTA), and the Irish Aviation Authority (IAA). Given the central role that personal data plays in the digital economy, the DPC has become a member of the ERN by virtue of its regulatory role.

International Network of Digital Regulation

The DPC, through its membership of Ireland's Digital Regulators Group, continued to actively engage in meetings of the International Network of Digital Regulation Cooperation (INDRC) throughout 2025. This network currently comprises the digital regulation coordination bodies from Australia, Canada, Ireland, the Netherlands and the United Kingdom, and meets every six months to foster discussion between international regulators on coherence across digital regimes in their own jurisdictions, and to gather insights into how they are approaching these issues.

Cross-Regulatory Interplay and Cooperation

At EU level, the DPC continued to actively participate in the EDPB's Cross-Regulatory Interplay and Cooperation (CIC) expert subgroup which was established in late 2024. This group works to build on synergies between the regulatory frameworks of data protection, competition and consumer protection law and exchange information and promote best practices as regards cross-regulatory governance and cooperation, in line with the EDPB's 2025 Helsinki Statement on enhanced clarity, support and engagement.[5]

Digital Markets Act High-Level Group

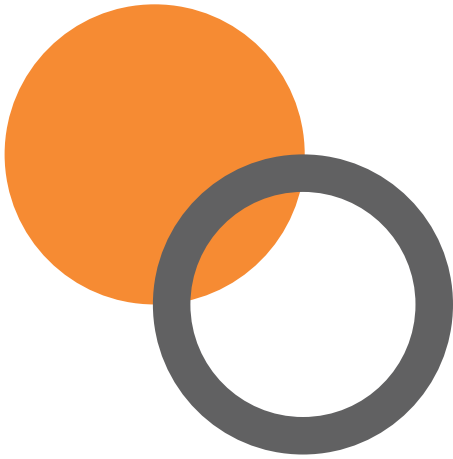
The DPC was delighted to be reappointed as an EDPB representative on the DMA High-Level Group in April 2025. This group is composed of nominated representatives from the Body of the European Regulators for Electronic Communications (BEREC), the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the European Competition Network (ECN), the Consumer Protection Cooperation Network (CPC Network), and the European Regulatory Group of Audiovisual Media Regulators (ERGA). The purpose of this group is to ensure effective enforcement of the DMA, give expert advice, and ensure regulatory alignment across different EU legislation.

The DPC also continued to actively engage within the Data-Related Obligations subgroup to the DMA HLG following its reappointment as an EDPB representative to this group in 2025.

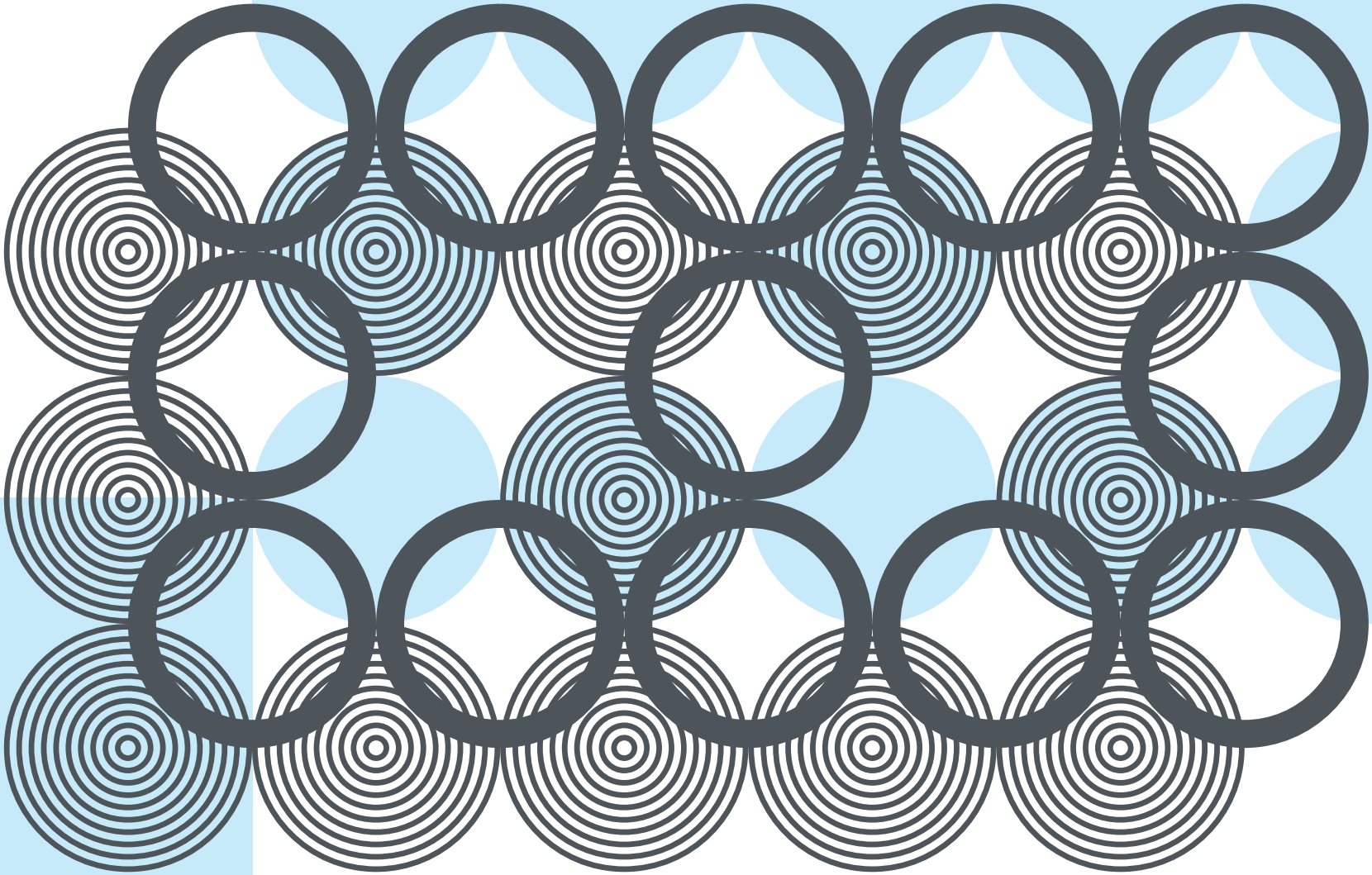
Regulation (EU) 2024/900 of the European Parliament and of the Council on the Transparency and Targeting of Political Advertising

October 2025 witnessed the coming into effect of Regulation (EU) 2024/900, referred to as the Transparency and Targeted Political Advertising Regulation (TTPA). The TTPA aims to empower citizens to make informed choices in elections by enhancing transparency and accountability in political advertising. This Regulation was transposed into Irish law via S.I. No. 474 of 2025, the 'European Union (Political Advertising) Regulations 2025'.

Under S.I. No. 474, the DPC has been designated as a competent authority in respect of Articles 18 and 19 of the TTPA, which relate to targeting techniques and ad delivery techniques in the context of online political advertising. An Coimisiún Toghcháin and Coimisiún na Meán have also been designated competent authorities under this statutory instrument. The DPC will work closely with both authorities in 2026 to facilitate cooperation in the performance of respective functions, with Regulation 7 of S.I. No 474 providing a basis for cooperation agreements between all three organisations.



5 See www.edpb.europa.eu/system/files/2025-07/edpb-statement-20250702-enhanced-clarity-support-engagement_en_0.pdf



Children's Data Protection Rights

8. Children's Data Protection Rights

Children's Policy

From external stakeholder engagement and cross-regulatory cooperation to the launch of a major public awareness-raising campaign, the protection of children's personal data remained a top priority and area of focus for the DPC in 2025.

Pause Before You Post campaign

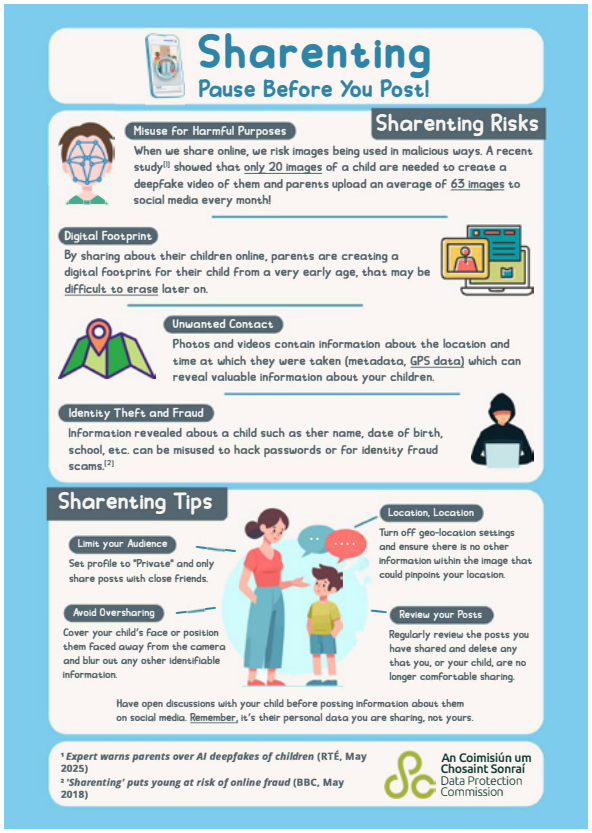
In November 2025, the DPC launched a national public awareness campaign entitled ***Pause Before You Post***. The purpose of this initiative is to highlight the growing risks associated with 'sharenting'—the habitual online sharing of children's personal information, photos, and videos by parents.

The DPC was delighted to engage with our French counterpart, the Commission Nationale de l'Informatique et des Libertés (CNIL) on this campaign. Both Data Protection Authorities are committed to safeguarding children online and supporting parents' digital literacy; this joint effort directly advances the strategic priorities of both organisations.

The importance of addressing this issue was underscored by a 2024 digital parenting survey, conducted by the international Digital Education Working Group of the Global Privacy Assembly. The survey identified sharenting as a topic of concern with potential harmful implications for children's rights and personal data.

The primary objective of the *Pause Before You Post* campaign was to highlight the inherent risks of parents posting their children's personal data online. The DPC worked with an external agency on the creative concept and a 40-second video was produced for broadcast on national television and in cinemas for a 6-week period in November and December. Since its publication, the campaign has reached a wide audience, generating over **150 million views** globally, including **45 million views** across the DPC's social channels.

Internationally, the campaign generated extensive traction with coverage and discussion in countries such as the United States, Australia, Brazil, the United Kingdom, Nigeria, and South Africa. It was featured and debated on podcasts and television programmes, **sparking widespread global conversation on the inherent risks of parents sharing their children's personal data online.**



International Headlines

Domestically, the campaign featured across all major Irish news outlets and prompted significant national discussion on the issue. Research conducted by the DPC's agency partner, Core, shows that **seven in ten parents of primary school–going children in Ireland have seen the advertisement in some form**. Further analysis indicates that it is the most watched Irish advertisement of the past five years.

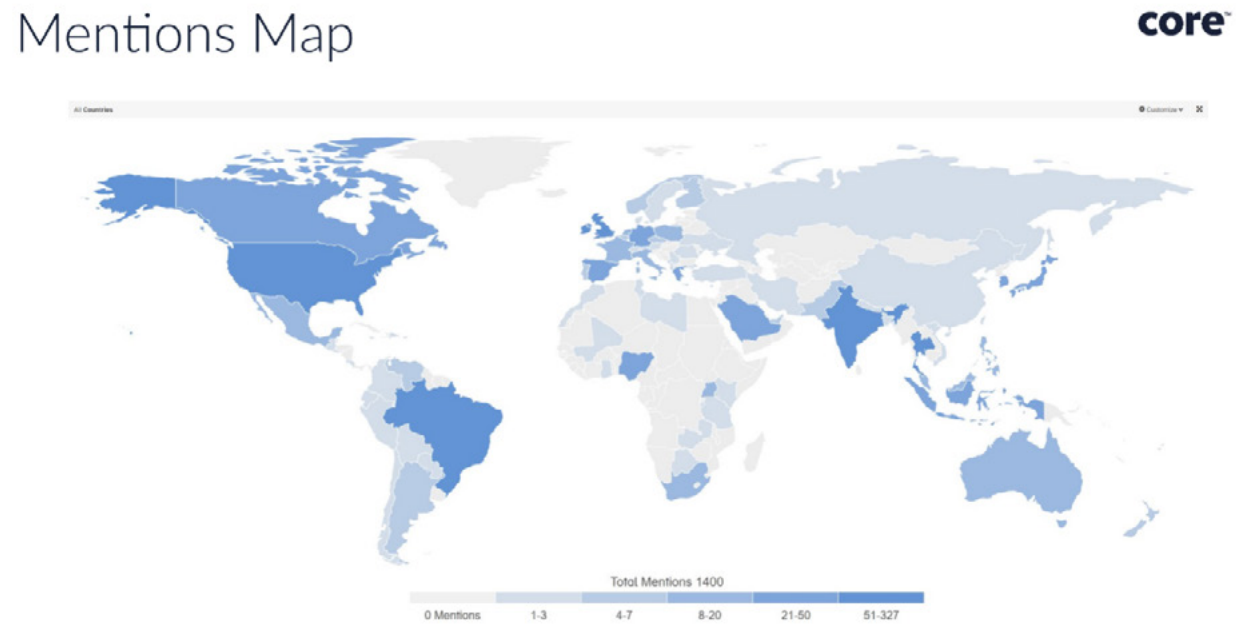
The impact and success of this initiative exceeded expectations as its message has resonated strongly with parents, privacy professionals, children's rights organisations, the media and NGOs alike.

To further delve into the topic of sharenting, **the DPC also commissioned a survey** of over 1,000 parents to be carried out in Ireland and France to gain insights into the social media use and information-sharing practices of parents in relation to their children. The field work for the survey was carried out in both countries in October/November 2025, prior to the launch of the advertisement, and the results will be published in 2026.

> 'Pause before you post' – Irish advertisement on online safety and 'sharenting' goes viral
>
> – Irish Independent

> This 'terrifying' Irish ad about online child safety plays out like a dystopian horror movie
>
> – The Journal

Pause Before You Post



Map showing mentions of the advertisement around the world provided by Core.

External Speaking Engagements

Over the course of 2025 the DPC contributed to events addressing latest developments and trends in the field of children's data protection and online safety. This included panel discussions on global strategies for child safety and privacy (IAPP Washington, April 2025), balancing innovation with responsibility and empowering young users to navigate the internet safely (Venice Privacy Symposium, May 2025), and the intersection of AI and the protection of children in the digital world, which saw the DPC, Coimisiún na Meán and CyberSafeKids come together to discuss this critical topic.

The DPC was also grateful for the opportunity, this year, to engage with Ireland's **Online Health Taskforce**. This taskforce was established by the Minister for Health in 2024 to develop a public health response to harms caused to children and young people by certain types of online activity, with its members compromising experts in the field of child safety. The DPC gave a presentation to the taskforce in June of 2025 on the DPC's ongoing work on the protection of children's personal data online.

The DPC attended numerous events throughout 2025 in the area of children's data protection in order to develop and maintain knowledge, and to meet with important stakeholders in the sector. These events covered many children-centred topics such as AI literacy, age assurance, algorithms, and data protection by design and default. Events attended included Ireland's *Safer Internet Day* stakeholder event hosted by Webwise, Google's *Growing Up in the Digital Age*, Meta's *Youth Privacy Forum*, Privacy Laws & Business's whole-day event on children's data protection issues, and the *Global Age Assurance Summit.*

The DPC also continued to participate as a member of a number of external working groups focused on children's data protection issues, including the UK Information Commissioner's Office (ICO)'s International Age Assurance Working Group which held a number of meetings and 'teach-ins' throughout the year. The DPC is also an active member of the Global Privacy Assembly's Digital Education Working Group, chaired by the CNIL, and in 2025, we joined the working group's taskforce on digital parenting as part of European Year of Digital Citizenship Education.

Engagement with Statutory Bodies

The DPC met with relevant statutory bodies to discuss developments in the area of children's data protection issues. One such example is the Office of the Australian Information Commissioner (OAIC), who approached the DPC to gain insights into our experience around the development of the DPC's 'fundamentals' guidance, as they had been tasked with developing a children's code in Australia. The DPC was delighted to facilitate the OAIC's request to use associated educational materials in the context of a public consultation they intended to roll out across Australian schools.

In October 2025, the DPC and Coimisiún na Meán signed a Cooperation Agreement and issued a Joint Statement on Children entitled Advancing the Safety of Children and the Protection of Their Personal Data Online. The Cooperation Agreement enables both regulators to work closely together, including for the purposes of cooperating on matters of common interest and one such area of common interest is the need to ensure that the rights and best interests of children are respected and upheld by the online services that An Coimisiún and the DPC regulate.

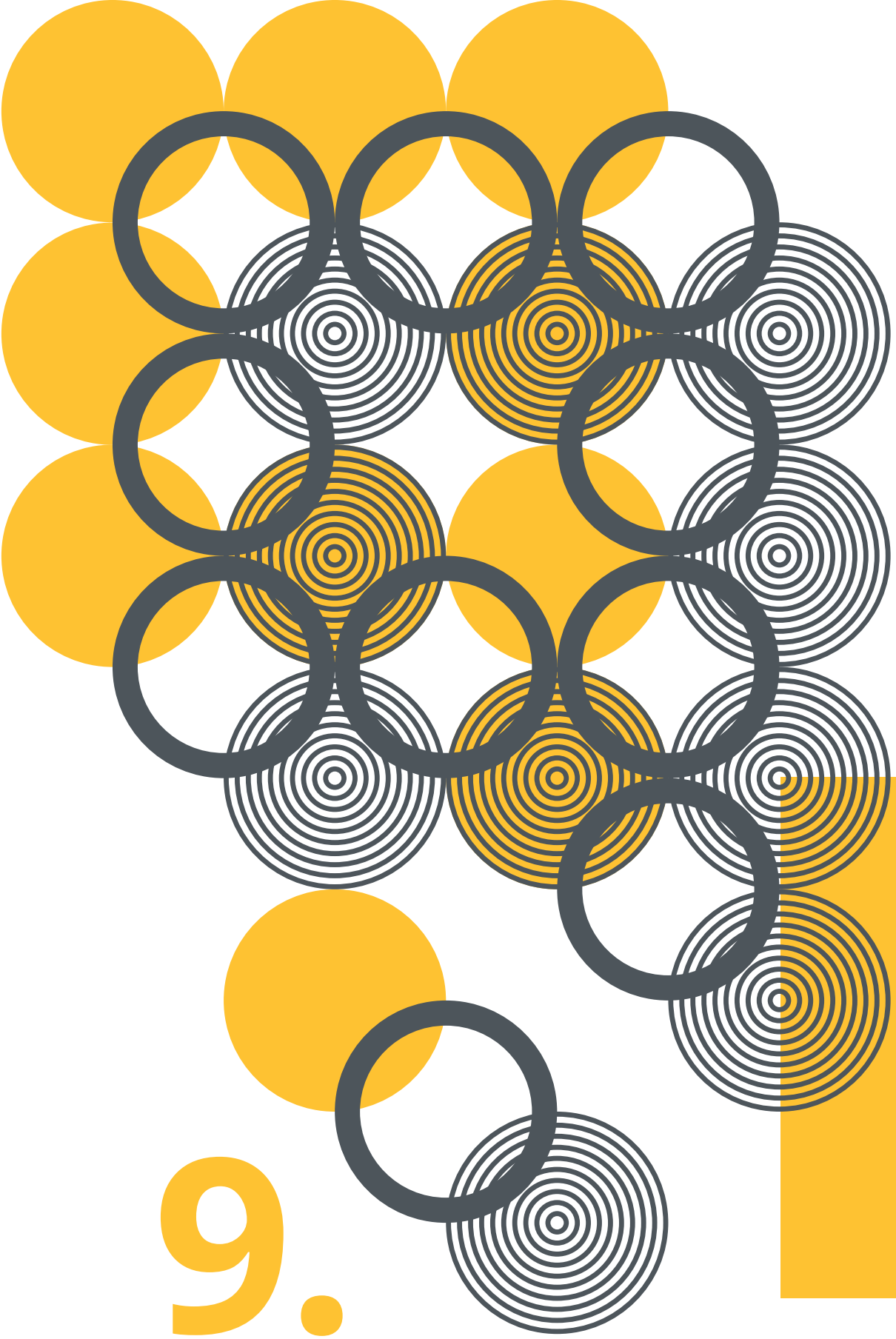
The joint statement highlights that future cooperation may include sharing insights on emerging risks to the safety and protection of children's personal data online, joint work on educational resources relating to the protection of children online, and other areas of mutual interest. Work on this will continue into 2026.

Advancing the Safety of Children and the Protection of Their Personal Data Online

Work on Children's Issues within the European Data Protection Board

The DPC's focus and dedication to the complex issue of age assurance in the digital environment continued at an EU level throughout 2025. The DPC contributed to the drafting of the Statement being prepared by the EDPB on general data protection principles and criteria for age assurance systems. This Statement, establishing 10 guiding principles to ensure that age assurance methods respect the fundamental rights of individuals and uphold the values of the GDPR, was published in February 2025. The Statement also aims to ensure a consistent European approach to age assurance, to protect minors while complying with data protection principles.

Statement of Age Assurance



9. Data Protection Officers

9. Data Protection Officers

The position of Data Protection Officer (DPO) as set out under the GDPR is an essential pillar for ensuring both compliance and accountability on the part of data controllers. Designated DPOs under Articles 37-39 of the GDPR both advise their organisations on data processing matters and monitor compliance such as organisational adherence to data protection policies and data processing agreements. DPOs often play a key part in training in their organisation, which helps to build a culture of data protection awareness and contributes to better outcomes for data subjects in how their personal data is processed.

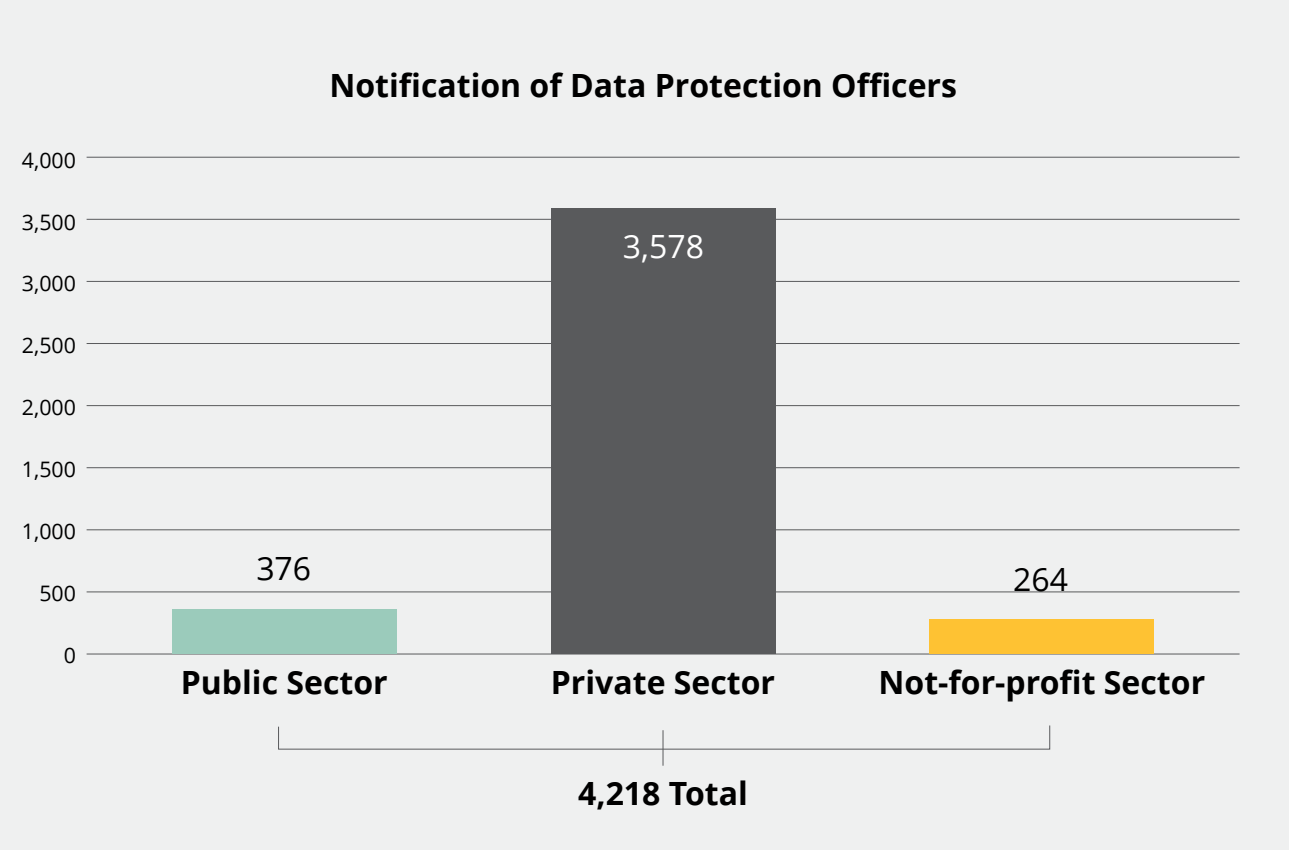
Where a DPO has been designated by an organisation it is required that they are adequately supported by management and resourced to allow them to carry out their tasks, and failure to do so is an infringement of the GDPR. Adequate resourcing means that the DPO should have access to necessary financial resources, infrastructure, supports staff, and training. Where DPOs may also carry out other functions in the organisation, it must be ensured that they have adequate capacity to carry out their DPO tasks, allowed to act independently within the organisation in the performance of their duties, and that any other work does not give rise to a conflict of interests.

For certain sectors and organisations, the appointment of a DPO is mandatory under the GDPR (public bodies, controllers carrying out large scale, regular and systematic monitoring of data subjects; controllers carrying out large scale processing of special categories of personal data or data relating to criminal convictions and offences). Where the appointment of a DPO is a statutory requirement, it is particularly important that controllers meet their obligations to support and resource the function, due to the nature and scale of personal data processing. During the course of 2025 the DPC undertook a number of supervisory examinations of the resourcing of DPOs and will continue to do so in 2026.

DPOs also play an important role as the primary contact point for the DPC in their organisation, and as such are an important stakeholder group. The DPC continued to support DPOs and raise awareness of the importance of their role in 2025. During 2025 the DPC supported designated DPOs and data protection compliance teams across all sectors including;

- The Health Research Data Protection Network;
- Sports Sector DPOs and compliance officers;
- Charity and Voluntary Sector DPOs and compliance officers;
- The Civil Service DPO Network;
- The LGMA Local Authorities DPO Network.

As part of the requirements of GDPR, the DPC must be notified of the formal designation of a DPO by an organisation. As of the end of the 2025 the DPC has been notified of the **designation of 4,218** DPOs broken down by sector as follows:



Deputy Commissioner David Murphy delivered a presentation at a Civil Service DPO Meeting held in the DPC office in Pembroke Row, June 2025.

DPC DPO Network

The DPC DPO Network is an initiative of the DPC, designed to support DPOs and privacy professionals across Ireland. The DPC DPO Network endeavours to deliver high-quality support through the facilitation of networking opportunities and dissemination of information relating to events and new guidance, with a key aim of raising awareness of the GDPR and importance of ensuring compliance with data protection legislation.

In 2025, the DPC DPO Network furthered its work promoting data protection awareness through participation in a number of events, including the following:

- the DPC DPO Network Team hosted an information stand at the Wheel's Charity Summit in Croke Park;
- the DPC DPO Network Team hosted an information stand at the PDP AI and Data Compliance Update Summit at the offices of William Fry Solicitors; and
- the DPC DPO Network Team hosted an information stand at the National Ploughing Championships 2025 in Tullamore as part of the Government of Ireland Village, in the *Supporting People/Supporting Business* marquee.

Each of these events provided an opportunity for individuals to engage with the DPC, allowing the DPC DPO Network to offer support and to signpost the helpful DPC guidance available.

10.

International Activities

10. International Activities

European Data Protection Board and Supervisory Bodies

Each European Union (EU) Member State and European Economic Area (EEA) country[6] has a national data protection supervisory authority responsible for enforcing data protection laws and regulation within their jurisdiction. The European Data Protection Board (EDPB) is an independent body responsible for ensuring that the GDPR and Law Enforcement Directive are consistently applied in EU and EEA. The EDPB comprises a chairperson, two deputy chairpersons and members of each national data protection authority and the European Data Protection Supervisor. It meets at monthly plenary and expert subgroup meetings and has the following main tasks:

- to issue opinions, guidelines, recommendations and best practices to promote a common understanding of the GDPR and the Law Enforcement Directive;
- to advise the European Commission on any issue related to the protection of personal data in the Union;
- to contribute to the consistent application of the GDPR, in particular in cross-border data protection cases; and
- to promote cooperation and the effective exchange of information and best practices between national supervisory authorities.

In 2025, the DPC attended and actively participated in over **140** meetings including all monthly EDPB plenary meetings, as well as expert subgroup meetings.

Continued Cooperation with other EDPB Supervisory Authorities 2025

Recognising the importance placed on cooperation in cross-border matters under the GDPR, the DPC continued its engagement with its fellow European Data Protection Supervisory Authorities.

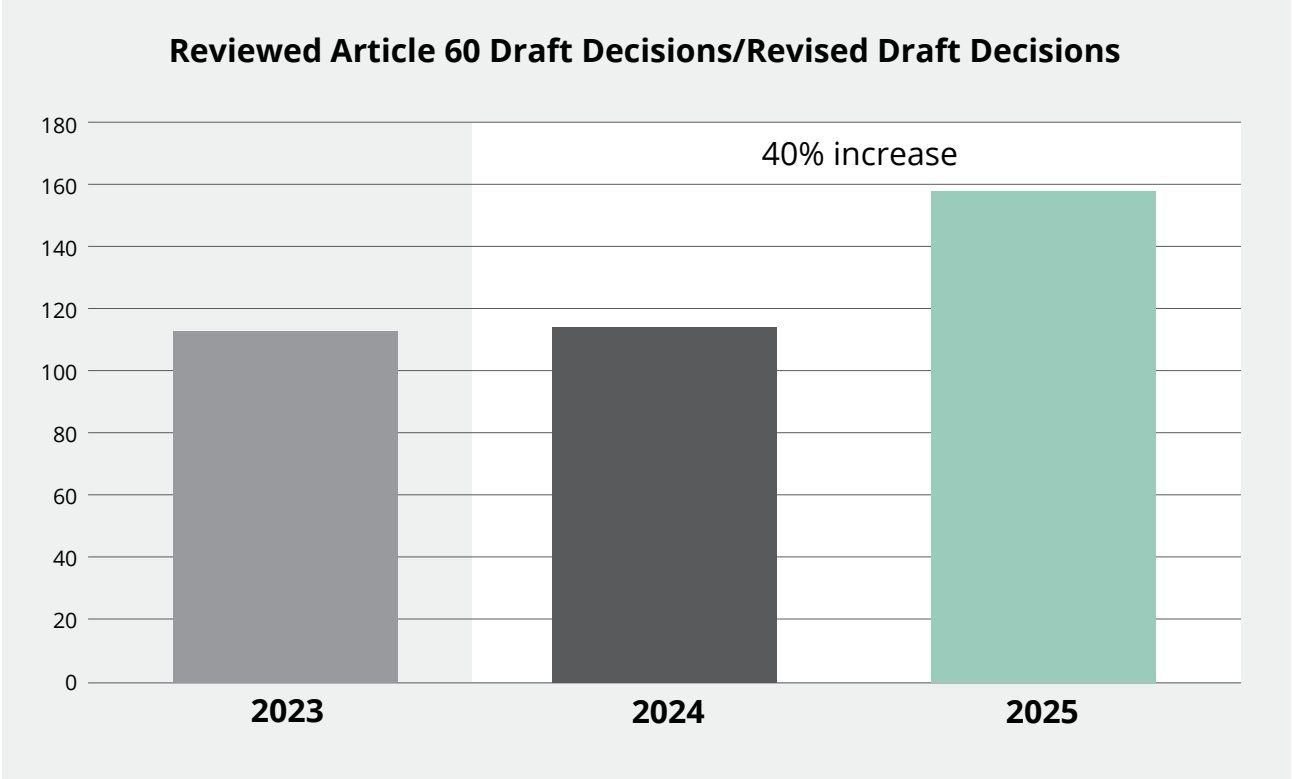
As part of the on-going co-operation and communication between the DPC and the other EU/EEA supervisory authorities in 2025, the DPC received **1,015** voluntary and formal mutual assistance requests[7] from other European regulators.

In 2025, the DPC submitted the following to the GDPR Article 60[8] cooperation process:

- **88 Provisional Decisions** in cross-border complaint and own-volition inquiries;
- **7 Final Decisions** in cross-border complaint and own-volition inquiries;
- **163 notifications** of amicable resolutions achieved in cross-border complaints; and
- **28 Dismissals**, where the DPC was LSA and four where the supervisory authority submitting the complaint to the DPC were required to draft a Final Decision to dismiss the complaint.

Through enhanced cooperation, the DPC engaged with its peer regulators at all levels during 2025, with a focus on ensuring that EDPB supervisory authorities were kept informed of DPC activities on draft and final decisions at all stages of proceedings.

6 European Economic Area. The EEA includes Iceland, Liechtenstein and Norway.
7 Article 61 of the GDPR – *Mutual assistance.*
8 Article 61 of the GDPR - *Cooperation between the lead supervisory authority and the other supervisory authorities concerned.*



As a Concerned Supervisory Authority, the DPC reviewed **158 Article 60 Draft Decisions/revised Draft Decisions** from other lead supervisory authorities which represented a **40%** increase on the Draft Decisions reviewed in the previous year. It also engaged in **27 Informal Consultations** submitted to it by peer DPAs during the year.

The DPC also facilitated numerous bilateral engagement meetings with members of EDBP supervisory authorities at all levels on various topics including complaints, inquiries, best practices and matters of individual concern to specific supervisory authorities.

As part of its engagement with supervisory authorities at a European level, the DPC:

- held commissioner-level engagements with various EDPB supervisory authorities, including visits to Finland, France, Germany, and Italy as well as the United Kingdom;
- participated in the high-level meeting of the European Data Protection Board, at which the Helsinki Statement was adopted;
- participated in the European Case Handling Workshop in Pristina, Kosovo;
- represented the European Data Protection Board at the High-Level Group for the Digital Markets Act;
- represented the European Data Protection Board at the High-Level Group Sub-Group for data related obligations of the Digital Markets Act;
- represented the European Data Protection Board at Working Group 6 – Protection of Minors of the European Board for Digital Services;
- welcomed the Austrian Data Protection Authority for a study visit to the DPC;
- welcomed secondees from the French and Norwegian Data Protection Authorities; and
- was a secondee to the Norwegian Data Protection Authority.

Central and Eastern Europe Data Protection Authorities (CEEDPA) Conference

In June, 2025, representatives from the DPC attended the Central and Eastern Europe Data Protection Authorities (CEEDPA) Conference, hosted in Krakow by the Polish DPA.

The conference had very insightful presentations and discussions on the topic of quantum technology, presented by various speakers including physicists, computer scientists and regulators. The DPC had valuable engagements with our counterparts in Central and Eastern European DPAs on the topic of SME compliance with the GDPR.

EDPB AI Audit Bootcamp

In October 2025, representatives from the DPC attended the EDPB bootcamp, focusing on auditing in the context of AI models and systems. The bootcamp consisted of a collection of workshops and presentations, led by the EDPB and various SAs.

European Case Handling Workshop in Pristina, Kosovo

In November 2025, representatives from the DPC's national and cross-border complaint handling teams attended the European Complaint Handling Workshop (ECHW) 2025, which took place in Pristina, Kosovo.

This workshop, which was hosted by the Information and Privacy Agency of Kosovo and funded by the Council of Europe, brought together over 70 representatives of data protection authorities from 23 European countries, and allowed for the valuable exchange of experience and knowledge on the topics faced across all authorities.

Commissioners Dale Sunderland and Des Hogan, along with representatives from other European Data Protection Authorities at the EDPB meeting in Helsinki, July 2025.

Helsinki Statement[9]

In July 2025, Commissioners Hogan and Sunderland attended a high-level meeting of EU Data Protection Commissioners in Helsinki. At this meeting, the EDPB adopted a landmark Statement on enhanced clarity, support and engagement.

The Helsinki Statement outlines new initiatives to make GDPR compliance easier, in particular for micro, small and medium organisations, strengthen consistency and boost cross-regulatory cooperation.

Helsinki Statement

According to the EDPB Chair, Anu Talus: '*The EDPB aims to ensure that compliance with the GDPR can be more easily achieved. By placing fundamental rights into the core of their digital transformation, organisations can ensure that technological advancements and the respect for European values go hand in hand, ultimately building a stronger and more resilient digital economy… The EDPB is committed to helping organisations in achieving GDPR compliance with greater ease and efficiency. Through timely and concise guidance and ready-to-use tools, like a common data breach notification template, checklists, how-to's and FAQs, we will continue to make GDPR alignment achievable and accessible for all'.*

This Statement sets out how the EDPB will:

- strengthen its dialogue with stakeholders;
- enhance consistency of the application and enforcement of the GDPR; and
- further proactively engage with other regulators to support the new cross-regulatory landscape.

9 For further information see https://www.edpb.europa.eu/our-work-tools/our-documents/statements/helsinki-statement-enhanced-clarity-support-and-engagement_en

Commissioners Dale Sunderland and Niamh Sweeney met with Michael McGrath, EU Commissioner for Democracy, Justice, the Rule of Law and Consumer Protection.

Brussels Attaché

Following a successful pilot phase that began in mid-2023, the DPC has decided to maintain its full-time presence in Brussels via its Brussels-based Attaché. The ability of the DPC to have a permanent presence in Brussels on a day-to-day basis has been highly valuable, and this has continued throughout 2025.

During the year, the Attaché supported the DPC's regular engagement with Brussels-based stakeholders through structured, ongoing interaction, including the European Parliament, the European Commission, the EDPB Secretariat, and peer supervisory authorities. This work aligns with the DPC's emphasis on engagement with all such stakeholders associated with the EU institutions, and beyond.

The Attaché also maintained regular engagement with civil society and regulated entities, including through participation in public events and targeted meetings, where appropriate. In parallel, daily liaison was maintained with teams across the DPC to ensure timely internal feedback and coordination arising from Brussels-based engagements.

A notable engagement during 2025 was the organisation of a meeting in March between the Commissioners and Ireland's MEPs, at which the work of the DPC, both domestically and as the lead supervisory authority for many large multinational companies based in the EU/EEA, was outlined. Ongoing engagement with MEPs with a particular interest in data protection remained a priority.

The Commissioners also met with EU Commissioner Michael McGrath and with Ireland's Permanent Representative to the EU, Aingeal O'Donoghue, with discussions with the latter focusing in particular on Ireland's forthcoming Presidency of the Council of the European Union in the second half of 2026. In addition, the Commissioners met with members of the French National Assembly in Brussels, contributing to the development of a report concerning TikTok, with a focus on minors.

Consistent with the DPC's broader focus on public engagement, the Attaché participated in over 30 public events during the year (including conferences, panel discussions, and roundtables). The Attaché also continued active participation in EDPB work and attended 22 EDPB expert sub-group meetings, in addition to attendance

at EDPB Plenary. Another important aspect of the Attaché's work was following progress on the new Procedural Harmonisation Regulation, which was agreed by the EU co-legislators in November 2025, and aims to harmonise procedural rules in cross-border cases under the GDPR, to which the One-Stop-Shop mechanism applies.

The Attaché will continue to represent the DPC in Brussels, reflecting the ongoing importance the DPC places on engagement and collaboration.

Looking ahead, priorities will include engagement, which may increase during Ireland's 2026 Council Presidency and continued monitoring of key EU policy files expected to be negotiated by Member States and the European Parliament, including the Commission's proposed Digital Omnibus and AI Omnibus.

EDPB Key Concepts Project

The Key Concepts Project, launched by the EDPB, aims to collect data on all Data Protection Authorities' activities across members in a uniform way. From the perspective of the EDPB, the objectives of the project include:

- ensuring the availability of data for the regular evaluation and review of the GDPR (Art. 97);
- obtaining an accurate view of the Supervisory Authorities' actual work and supporting their initiatives (including requests of additional resources); and
- improving transparency and contributing to a better understanding of the Supervisory Authorities' activity and positions.

The DPC supports this project and looks forwards to seeing its activities reflected in these data sets when published by the EDPB.

Commissioner Des Hogan in conversation with Pascale Davies of Euronews at the Web Summit 2025 in Lisbon, Portugal.

From left to right: ICO Commissioner John Edwards, DPC Commissioner Dale Sunderland, CNIL President Marie-Laure Denis and, Chairperson of Korea's Personal Information Protection Commission, Haksoo Ko signed a joint declaration at the AI Action Summit held in Paris.

Cooperation with International Supervisory Authorities in 2025

Further to engagement at a European level, the DPC engaged with international supervisory authorities, including bilateral engagements with: the UK Information Commissioner's Office; Office of the Australian Information Commissioner; US Federal Trade Commission and the Personal Information Protection Commission, Korea.

The DPC signed a joint declaration along with Australia, Korea, France and the United Kingdom, at an OECD hosted event to reaffirm their commitment to implementing data governance that promotes innovative and privacy-protecting AI.

The DPC participated in:

- international meeting of DPAs, Washington, USA;
- the Global Privacy Assembly in Seoul, Korea;
- the Privacy Symposium in Italy;
- the British, Irish and Islands Data Protection Authorities (BIIDPA) annual meeting in Guernsey;
- Participation at the AI Action Summit, Paris; and
- Participation at the EU Digital Summit, Brussels.

Global Privacy Assembly[10]

In September 2025, the DPC participated in the Global Privacy Assembly.

The Global Privacy Assembly's mission is to provide leadership at an international level in data protection and privacy by connecting the efforts of authorities from around the world. The 2025 conference was hosted by the Personal Information Protection Commission of the Republic of Korea. The DPC's participation in the annual conference is an opportunity for the DPC to share knowledge, develop policy positions and influence the development of global privacy standards. The conference had both open and closed sessions, which were only attended by accredited members and observers of the Global Privacy Assembly.

The DPC spoke on four different panels at the conference across the open and closed sessions:

- Mechanisms and Policy Instruments to Support AI Innovation;
- Mastering Investigation Strategies and Choosing the Right Enforcement Tools;
- Re-using Health Data: Balancing AI Health Innovation and Privacy in a Cross-Border Context; and
- Promoting a Safe Digital Childhood.

In a joint signing ceremony, the DPC welcomed additional signatories from peer DPAs to the joint declaration on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI which the DPC had signed with Australia, Korea, France and the UK in February 2025.

The DPC used the conference as an opportunity for in-person meetings with international DPAs and held numerous bilateral meetings over the five-day conference, including with Australia, Korea, US and Dubai.

From left to right: Deputy Commissioner Gráinne Hawkes, Commissioner Des Hogan, Irish Ambassador to the Republic of Korea; Michelle Winthrop and Commissioner Dale Sunderland at the Global Privacy Assembly in Seoul, September 2025.

From left to right: Commissioner Dale Sunderland, Chairperson PIPC: Hacksoo Ko and Commissioner Des Hogan at the Global Privacy Assembly in Seoul, September 2025.

The DPC was also very proud to co-sponsor the three resolutions adopted by the closed session of the Global Privacy Assembly:

- Resolution on the Collection, Use and Disclosure of Personal Data to Pre-Train, Train and Fine-Tune AI Models;
- Resolution on Meaningful Human Oversight of Decisions Involving AI Systems; and
- Resolution on Digital Education, Privacy and Personal Data Protection for Responsible Inclusive Digital Citizenship.

10 For further information see https://globalprivacyassembly.com/

From left to right: Commissioners Hogan and Sunderland accepting a Global Privacy Assembly Award, September 2025.

In addition to the participation on panels and engagements with international Data Protection Authorities, the DPC was honoured to be shortlisted for a Global Privacy Assembly Award for enforcement in relation to its work in the area of the use of surveillance systems by county councils.

Certification

In Ireland, the DPC is the supervisory authority responsible for approval of data protection criteria in certification schemes, while the Irish National Accreditation Board (INAB) is responsible for the accreditation of Certification Bodies (CBs) that intend operating such schemes.

The DPC appreciates that the appeal of data protection certification measures across Europe appears to have been limited to date. To address this, in 2025, the DPC joined an EDPB working group focused on improving certification brand awareness and take-up of such schemes.

A 'Register of certification mechanisms, seals and marks can be found on the EDPB's website: www.edpb.europa.eu. There are currently three approved European Certification Schemes, the rest being national schemes.

Whilst no certification bodies in Ireland have sought accreditation to offer certifications under any of these EU certification schemes to date, certification bodies have been set up in other members states; and controllers and processors are encouraged to explore the possibility of seeking to be certified by those certification bodies under these schemes.

The DPC continued to work closely with its EU colleagues at the European Data Protection Board (EDPB) during 2025, on the assessment of a number of national and EU certification schemes in addition to improving internal procedures and developing further guidelines for stakeholders.

The DPC attended an EDPB Certification workshop in Berlin in June, where work continued on multiple projects, including discussions on how best to implement a certification scheme to enable international transfers as envisaged under Article 46(1)(f). In addition, the DPC acted as co-reviewer on a national certification scheme for another supervisory authority for the first time.

EDPB Coordinated Enforcement Framework (CEF) 2025

In 2025, the DPC participated in the Coordinated Enforcement Framework (CEF) action led by the EDPB on the right to erasure under Article 17 of the GDPR. As part of the initiative, the DPC surveyed 40 controllers across both public and private sectors to assess the implementation of Article 17.

The main objectives of this coordinated action were to ensure that the right to erasure can be effectively exercised by individuals in Europe and understand how controllers comply with this right in practice. In addition, the EDPB identified good practices and the most important related challenges, with the aim of providing further guidance on this topic. The exercise identified three substantial issues:

- some controllers reported that they do not have procedures or policies in place to handle erasure requests;
- controllers indicated that they must consult with multiple stakeholders before the right can be exercised; and
- it was identified that not all controllers provide training to staff members on how to handle erasure requests.[11]

International Transfers - Binding Corporate Rules

The DPC frequently takes a lead EU role in the assessment and approval of Binding Corporate Rules (BCR) applications from multinational companies. BCRs are a set of binding data protection polices which underpin transfers when group members established in the EU transfer data to group members outside the EU.

A typical application consists of a large volume of documentation, comprising all the policies required to demonstrate the commitments being made along with the contractual binding mechanism and any other documents the group considers necessary to supplement their application.

The review can take some time and also will involve seeking the views of two other SAs during the co-review phase and the views of all SAs during the co-operation phase. We then co-ordinate and collate these responses, discussing them with the applicant to come to a draft that all SAs are satisfied with. Once we reach this stage an Opinion of the EDPB is sought under Article 64(2) and the DPC can formally approve the application once that Opinion is received.

11 Further information on the 2025 CEF action can be found at edpb_cef-report_2025_right-to-erasure_annex_en.pdf

2025 BCRs

The DPC was BCR lead in relation to **13** BCR applications from **eight** different companies. **Four** of these applications were submitted to the EDPB seeking an Article 64 Opinion and subsequently approved by DPC in 2025 — Controller and Processor BCR application for Shopify International and Controller and Processor BCR application for Intec Billing Ireland Limited on behalf of the group CSG Systems International Inc (CSG Group).

The DPC also assisted other European Data Protection authorities by acting as co-reviewer for another SA on **nine** BCR applications from **six** different companies and participated on drafting teams as rapporteurs for Article 64 Opinions on **seven** BCR applications from **five** different companies.

BCR Annual Updates

Once the BCR applications are approved, the DPC continues to have a significant ongoing oversight role. Each BCR holder is required to submit an update of their BCR on an annual basis which will require review. **In 2025 the DPC was lead SA on 33 approved BCRs for 21 different BCR holders.** The list of these approved BCR files is published on the DPC website.

BCR EDPB opinions

In addition, the EDPB issued a total of 25 Article 64 opinions on BCR applications in 2025 and the DPC reviewed each of these applications.

DPC participation at the EDPB International Transfers Expert Sub-group (ITESG)

Transfers of personal data to third countries or international organisations is a critical area of protection for EU/ EEA citizens under Chapter V of the GDPR.

In 2025, staff from the **DPC attended 11 meetings** of the EDPB ITS ESG in 2025. This sub-group of the EDPB meets to consider, advise and prepare guidance documentation on matters concerning International Transfers. In addition, staff from the DPC attended additional meetings with ITS colleagues and other export sub-groups for dedicated meetings on matters such as UK Adequacy, Brazil Adequacy and Certification.

Case Study: BCR Application in Focus

Shopify International Limited

Shopify is a subscription-based e-commerce platform used by retailers. When Shopify processes human resource data, or information relating to its consultants, contractors, customers, merchants, their representatives, partners, or service providers, that data may be handled by operational teams based in third countries; Because of this, Shopify must ensure that all international data transfers comply with the requirements of Chapter V of the GDPR prior to any transfers taking place. The group determined that a BCR would be the best option to provide adequate safeguards when it needed to transfer data within the group for scenarios where it acted as both a Controller and a Processor.

Shopify International Limited, on behalf of the group Shopify, approached the DPC to act as BCR lead to seek approval for their Controller and Processor BCRs. These were handled as two separate BCRs because each received its own Article 64 opinion. Shopify International limited is the EEA headquarters and their EEA data protection compliance team is centred in Ireland. The DPC assessed the application material provided to ensure the criteria required to act as Lead BCR under WP263 was being met. Once satisfied with the information provided during the initial application process, the DPC informed all SAs that it was happy to act as the BCR lead and provided them with opportunity to object. As there were no objections, the DPC advised Shopify it could act as their BCR lead and requested the full suite of documentation

The DPC reviewed the BCR documentation and provided comments back and forth with the applicant until the DPC were satisfied that the BCR was meeting the requirements set out in the elements and principles of the 01/2022 recommendations and WP257. Issues that typically arise during BCR assessment phases are where the applicants fail to demonstrate where they are making the commitments. As part of the assessment of all BCR files, the DPC will advise on where the text requires amendment often providing drafting suggestions and signposting what part of the recommendations need to be reflected more fully.

The EDPB issued two positive Opinions, 17/2025 and 18/2025, in September 2025 on this BCR file and the **DPC confirmed its approval** by way of a National Decision issued to the applicant in October 2025.

11.

Human Resources, Communications and Corporate Governance

11. Human Resources, Communications and Corporate Governance

From left to right: Minister for Justice, Home Affairs and Migration, Jim O'Callaghan, Taoiseach Micheál Martin, Commissioner Des Hogan and Commissioner Dale Sunderland officially open the DPC's new headquarters in Dublin, May 2025.

New DPC Premises, 6 Pembroke Row, Dublin 2

The DPC identified and acquired, with the assistance of the Office of Public Works (OPW), a new fit-for-purpose Dublin office which provides flexibility to allow staff to work in a mixture of environments, such as breakout rooms and collaboration areas, in both private and open-plan areas. This has helped to embed collaborative and interdisciplinary modes of working within the DPC and provides sufficient meeting room resources to facilitate our supervisory/regulatory functions when meeting with stakeholders. This multi-year project was completed on 29 May 2025, when Taoiseach Micheál Martin officially opened the DPC new headquarters.

Human Resources

Recruitment

During 2025, the DPC continued to expand and strengthen its workforce in response to its evolving regulatory remit and the growing operational demands at both national and EU level. Recruitment activity remained sustained and wide-ranging throughout the year, reflecting both organisational growth and the increasing specialisation required to support the DPC's regulatory, legal, technological, and international functions.

Over the course of the year, **66** new staff members joined the organisation, 22 staff exited, and 25 internal promotions were progressed. Recruitment was achieved through a strategic mix of external talent attraction and internal career progression including; Public Jobs competitions, external campaigns delivered in partnership with a recruitment consultant, internal confined recruitment campaigns, and the Civil Service Mobility Scheme.

A number of targeted recruitment competitions were run during 2025 to address priority capability needs across the organisation. These included:

- Confined Executive Officer (EO);
- Confined Higher Executive Officer (HEO);
- ICT Regulatory Technologist (HEO);
- Legal Analyst (HEO);
- Assistant Principal (AP) Regulatory Technologist; and
- Senior Regulatory Lawyer (AP).

These competitions reflect the DPC's continued focus on strengthening specialist legal, technical, and regulatory expertise, alongside developing leadership capacity at middle and senior management levels.

By year-end 2025, the DPC had reached a total headcount of **295**. Recruitment activity will continue into 2026.

	2022	2023	2024	2025
New Joiners	45	44	70	**66**
Leavers	45	24	27	**22**
Internal Promotions	33	15	21	**25**

DPC Total Workforce	
Date	**No.**
1st January 2023	196
1st January 2024	213
1st January 2025	251
1st January 2026	**295**

Employee Engagement and Organisational Culture

Employee engagement and culture development remained a key focus during 2025. The Employee Engagement Forum (EEF) led a range of initiatives aimed at strengthening communication, connection, and shared understanding across the organisation.

A significant milestone during the year was the development of the DPC Employee Statement of Values. This was informed by consultation with staff and a facilitated workshop process. The Statement articulates shared values and behavioural expectations intended to support a positive workplace culture and alignment with the organisation's mission. The EEF also facilitated engagement activities across both office locations, in Dublin and Portarlington and experienced increased levels of correspondence from staff during the year, reflecting growing awareness and participation.

Industrial and Employee Relations

Constructive engagement with staff representative unions remained a central feature of the DPC's employee relations framework throughout 2025. Under the Scheme of Conciliation and Arbitration for the Civil Service, four quarterly Departmental Council meetings were held during the year, providing a structured forum for engagement on a wide range of organisational and workforce matters between management and recognised unions.

Discussions during the year included recruitment and workforce planning updates, the development of internal policies, and other matters relating to conditions of service. In parallel with formal industrial relations structures, the DPC provided ongoing, case-by-case employee relations advice and support to line managers and staff, supporting the consistent application of policy and fair procedures in an increasingly complex operating environment.

Across recruitment, employee relations, and HR operations, the DPC continued to support the organisation through a period of sustained growth, increased regulatory complexity, and significant organisational change.

John Mee (Outhouse LGBTQ+ Centre) presented a talk to the DPC on the importance of creating safe spaces for LGBTQ+ people in the workplace, June 2025.

Equality, Diversity & Inclusion (EDI) Committee

The EDI Committee continued to play a central role in fostering an inclusive and respectful workplace culture across the DPC in 2025, supporting the Workforce of the Future pillar of the Public Service Transformation 2030 Strategy. Representing staff across the organisation, the EDI Committee provided a platform for dialogue, learning, and staff-led initiatives that celebrate diversity and promote inclusion and belonging.

Throughout the year, the committee worked closely to deliver a wide range of impactful initiatives. Awareness and learning were further promoted through podcasts, workshops and events. These initiatives included staff-led discussions, guest speakers from external organisations such as Outhouse Dublin, Pavee Point, and Engaging Dementia, and the sharing of practical resources to support accessibility, wellbeing and inclusion in the workplace.

The EDI Committee also engaged actively at organisational level through panel discussions at Comms Day, participation in the Dublin Pride Parade, attendance at the National Diversity and Inclusion Conference, and a fireside chat with the Public Service EDI Policy Lead. Feedback from staff throughout the year was overwhelmingly positive, with many highlighting EDI Committee initiatives as key moments of learning and engagement. Collectively, these activities reflect the EDI Committee's ongoing commitment to embedding equality, diversity and inclusion at the heart of how the DPC works, ensuring all staff feel supported and valued.

Organisational Review

In 2025, the DPC commissioned Indecon to conduct an independent organisational review to support ongoing organisational development and to ensure that structures, governance arrangements, and ways of working remain fit-for-purpose in the context of the DPC's expanding remit and scale of operations.

The review was designed to provide an objective assessment of the organisation's current operating model, including consideration of organisational structures, roles and responsibilities, internal interfaces, and governance arrangements. It also sought to identify opportunities to support the organisation's continued effectiveness and resilience as regulatory responsibilities continue to evolve at both national and EU level.

The review process involved extensive engagement with staff across the organisation, including workshops, interviews, and facilitated engagement sessions in both Dublin and Portarlington. This engagement provided an opportunity for staff to contribute their perspectives and experiences as part of the review process. The final report was being drafted at year-end.

Learning, Development, and Wellbeing

During 2025, the DPC continued to invest in learning and development to support an engaged, capable, and connected workforce. A combination of structured development programmes, bespoke training, and individual learning pathways was delivered to strengthen capability across all grades and functions.

Leadership and professional development remained a key focus. A number of Principal Officers participated in leadership development programmes, and a Higher Executive Officer (HEO) Development Programme was launched to support the development of future leaders within the organisation. Individual learning and development needs were identified and supported through the Performance Management and Development System (PMDS).

Participation in learning and development activity remained strong throughout the year:

- 43 employees were approved for funding under the Refund of Fees Scheme to pursue accredited academic qualifications;
- 656 One Learning courses and webinars were completed by staff; and
- Funding was provided for 38 short-term and Continuing Professional Development (CPD) programmes.

In addition to centrally coordinated programmes, the DPC's People & Learning team worked closely with business units to deliver bespoke training aligned to organisational priorities.

International collaboration continued through participation in the EDPB secondment programme. During the year, the DPC hosted colleagues from Supervisory Authorities in France and Norway, while one DPC employee undertook a secondment to Datatilsynet in early 2025. The DPC also welcomed its first student placement from the Trinity College Dublin law programme.

Recognising that wellbeing underpins sustainable performance, a range of wellbeing initiatives focusing on financial, physical, and mental health were delivered during the year. These initiatives support the DPC's ongoing efforts to build a resilient, skilled workforce capable of meeting the demands of an evolving national and EU regulatory environment.

2025 Gender Pay Gap Report

The DPC values diversity, equality, and gender parity in our workplace. It is committed to fostering an inclusive environment where everyone has equal opportunities to progress and succeed. Its 2025 Gender Pay Gap Report reflects this commitment, outlining its workforce profile and the ongoing actions it is taking to promote fairness and reduce pay disparities. This year's statistics show continued improvement, with both the mean and median gender pay gaps narrowing compared to last year. The DPC remains focused on supporting balanced representation at all levels, strengthening recruitment and promotion practices, and embedding a strong culture of equality, diversity and inclusion across the organisation. This report provides a transparent overview of the DPC's progress and the measures in place to further advance gender equity within the DPC.

The DPC published its 2025 Gender Pay Gap Report based on 2024-2025 data with a snapshot date on 20 June 2025. The report provides an examination of the reported pay gap and the steps being taken to address it. At the snapshot date the DPC had a total of 272 employees with female employees being 54.40% (147) and male employees being 45.95% (125).

For the reporting period, the DPC had a mean gender pay gap of 5.80% in favour of men and a median pay gap of -0.42% in favour of women. The DPC is dedicated to continuous progress on equality, inclusivity, and closing the gender pay gap. The report reflects the DPC's sustained approach, underpinned by national policy and evolving legislative requirements.

Gender Pay Gap Report

Enterprise and Operations ICT

The DPC ICT transformation of physical and digital infrastructure continued in 2025. The build-out of ICT equipment in the new DPC Offices on Pembroke Row was completed. This included the installation of over 200 workstations and AV equipment in meeting rooms. Work also began on fitting out a technology lab that will be used for research and investigatory activities.

During 2025, the onboarding continued of all regulatory case handling teams onto the DPC's new case management system whilst an upgrade of the system to the latest version was also delivered. Work also progressed on building a separate record management system. By year-end all systems were in place to complete the transformation of users and activities from legacy systems.

Communications

Throughout 2025, the DPC continued promoting awareness of data protection rights through effective outreach, stakeholder engagement, and transparent communication. A core objective of the DPC is to ensure that individuals understand their data protection rights and how they can exercise control over the use of their personal data.

A New Structure

During 2025 a new DPC communications structure was introduced, comprising of three dedicated strands: external communications; internal communication; and education and awareness. This audience-focused model has proven highly effective, enabling clearer, more targeted communication and strengthening alignment between communications activity and organisational objectives.

Strengthening Collaboration

2025 saw the establishment of the DPC Communications Working Group, a monthly forum designed to enhance cross-organisational collaboration. The group has made a valuable contribution to improving both internal and external communications, and supporting ongoing improvements to the DPC website.

Internal Communications Days were a key highlight of 2025. These off-site away days are designed to bring staff together from across the organisation, providing structured opportunities for networking, knowledge-sharing and collaboration. This is particularly valuable in the context of hybrid working arrangements, differing in-office schedules, and the DPC's presence across several geographical locations including Dublin, Portarlington, and Brussels.

Communications, Education and Awareness

External communications activity was strong throughout 2025, with the DPC responding to a high volume of national and international media queries on data protection matters. During the year, the DPC published **26 news items** and **three blog posts and three pieces of guidance on its website**, generating significant coverage across print, broadcast and online media.

New Guidance produced by the DPC in 2025

The DPC's social media platforms continued to play an important role in raising awareness and supporting the organisation's work in 2025.

The DPC expanded its digital presence with the launch of Bluesky and the relaunch of Instagram social media accounts, helping to reach new audiences. Combined follower numbers increased by over **41,000** during the year to **93,300**, an **80% increase** on 2024. Engagement remained strong on existing platforms, X and LinkedIn. LinkedIn recorded an average engagement rate of **9.2%** during the year, reflecting growing public interest in data protection and the work of the DPC.

Most notably, the *Pause Before You Post* campaign page 91-92 which focused on protecting children's data rights reached a wide audience in 2025, generating over **45 million views** across the DPC's social channels.

A major milestone in 2025 was the commissioning and publication of a **Public Attitudes Survey**. The findings from this poll offered a clear window into how people perceive data protection and the role of the DPC. The results showed a strong public awareness and a widespread appreciation of the importance of safeguarding personal information, especially as new technologies, products, and services continue to evolve. At the same time, the survey underscores ongoing concerns about how organisations handle personal data and highlights differing expectations across age groups and regions. The findings from this research are already informing the organisation's engagement and awareness-raising strategy.

More information on the Public Attitudes Survey can be found on the DPC website.

DPC Public Attitudes Survey

70% trust the DPC to uphold their rights to have their personal data protected.

61% were concerned with the use of AI.

As part of Ireland's Digital Regulators Group, the DPC contributed to an important inter-regulatory education initiative which resulted in the publication of a **Short Guide to Digital Regulation**. This resource was developed to support public understanding of the digital regulatory landscape in Ireland, clarifying the roles and remits of the various regulators and promoting greater transparency and accessibility in digital regulation. The guide has performed very well across the DPC's social media channels, with particularly high engagement rate on LinkedIn of **50.2%**.

The DPC also managed and implemented the design and launch of the **Adult Safeguarding Toolkit**, including production of 10 infographics, as well as an associated press conference and stakeholder engagement event.

Adult Safeguarding Toolkit

The Case Studies section of the DPC website has been further developed in close collaboration with the Applications and Data Team within the DPC. This upgrade has improved accessibility and usability for stakeholders.

A new dedicated webpage on the DPC's website, providing guidance on the protection of children was developed and launched, strengthening the DPC's online resources in this key area.

DPC Commissioners and staff contributed to over **100 speaking engagements** during the year, supporting stakeholder engagement at both national and international level.

Guidance on the Protection of Children

Corporate Governance

DPC Audit and Risk Committee

In line with the Corporate Governance Standard for the Civil Service (2015), and also with regard to the Code of Practice for the Governance of State Bodies (2016), the DPC established its own Audit and Risk Committee, as a Committee of the DPC, effective from 1 January 2020.

The second term of the Audit and Risk Committee commenced on 1 January 2023 and runs for three years.

The members of the Committee are:

- Conan McKenna (chairperson);
- Aisling McKeon;
- Tara McDermott; and
- Graham Doyle.

Three meetings of the Audit and Risk Committee were held in 2025.

Internal Audit function

The Internal Audit function in the DPC is provided by an external service provider who provides regular reports to the DPC Audit and Risk Committee on internal audits carried out during the year.

Official Languages Act 2003

The DPC continues to provide, and improve Irish language services with enhancements of services. The DPC's fifth Language Scheme under the Official Languages Act 2003 commenced on 21 December 2020 and will remain in effect until the introduction of language standards following the Official Languages (Amendment) Act 2021.

Ethics in Public Office Act 1995 and Standards in Public Office Act 2001

The DPC was established under the Data Protection Act 2018 and operates in accordance with the provisions of that Act. Measures are in place to ensure that the staff of the DPC, holding designated positions, comply with the provisions of the Ethics in Public Office Act, 1995 and the Standards in Public Office Act, 2001.

Regulation of Lobbying Act 2015

The Lobbying Act 2015 together with its associated code of conduct, regulations and guidelines aims to ensure that lobbying activities are conducted in accordance with public expectations of transparency. The Commissioners for Data Protection are Designated Public Officials (DPOs) under this Act, as noted on the DPC website.

Interactions between lobbying bodies and DPOs must be reported by the lobbyists. The Standards in Public Office Commission (SIPO) has established an online register of lobbying at www.lobbying.ie to facilitate this requirement.

Engagement with Oireachtas members

In accordance with the Department of Public Expenditure, NDP Delivery and Reform, Circular 25 of 2016, the DPC provides a dedicated mailbox to address the queries of Oireachtas members and to receive feedback.

Section 42 of the Irish Human Rights and Equality Commission Act 2014

The DPC seeks to meet its obligations under Section 42 of the Irish Human Rights and Equality Commission Act 2014 and has put in place measures to ensure that consideration is given to human rights and equality in the development of policies, procedures and engagement with stakeholders in fulfilling its mandate to protect the fundamental right to data protection.

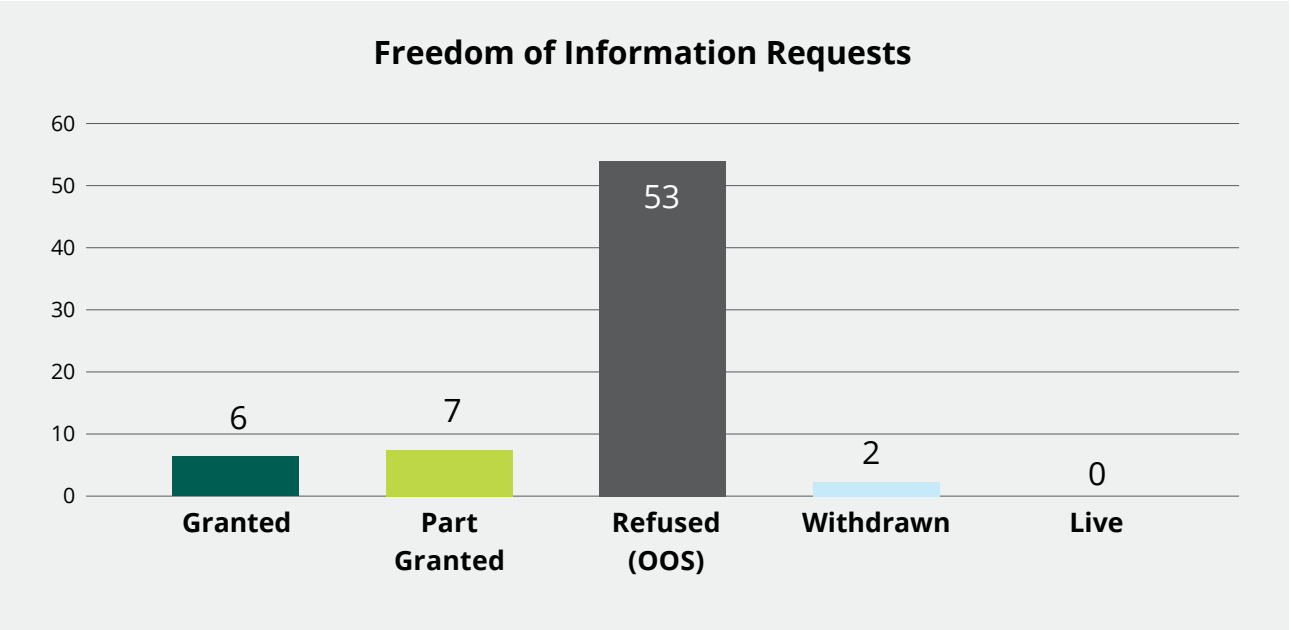
Accessibility Officer

To support customers who may require assistance when engaging with the services provided by the DPC, the Accessibility Officer may be contacted via the channels listed on the DPC website, and in writing to the:

Accessibility Officer,
Data Protection Commission
6 Pembroke Row,
Dublin 2,0
D02 X963,
Ireland
Email: DPCAccessibilityOfficer@dataprotection.ie

Customer Charter

The DPC's Customer Charter and accompanying Quality Customer Service Action Plan and Managing Unreasonable Behaviour and Contacts Policy for 2024–2026 are published on the DPC's website. There is a designated customer service comments mailbox for customers to engage with the DPC. Any and all comments received are taken into consideration as part of the on-going review of delivering quality customer service.



Freedom of Information (FOI)

In 2025, the DPC received a total of **68 FOI requests**. Six were granted, seven were partially granted, 53 were deemed out of scope, and two were deemed withdrawn. The DPC's regulatory activity is exempted from FOI requests in order to preserve the confidentiality of the DPC's supervisory, investigatory and enforcement activities. Nevertheless, the DPC is committed to providing transparent information to the public around the administration of its office and use of public resources.

Parliamentary Questions (PQs)

The DPC was consulted by the Department of Justice, Home Affairs and Migration in relation to **65 PQs** in 2025. The DPC provided observations in response to 30 of these questions (35 were not directly applicable to the DPC).

Elected Representative Correspondence

The DPC received **14 pieces of correspondence** from elected representatives in 2025, across all business areas.

Access to Information on the Environment

The DPC received one request in 2025 under the AIE Regulations.

Appendix 1

Appendix 1: Report on Protected Disclosures Received by the Data Protection Commission in 2025

The policy operated by the DPC under the terms of the Protected Disclosures (Amendment) Act 2022 (the Act) is designed to facilitate and encourage all workers to raise genuine concerns about possible internal wrongdoing in the workplace with regard to the processing of personal data and compliance with the data protection legislative frameworks, so that these concerns can be investigated following the principles of natural justice and addressed in a manner appropriate to the circumstances of the case.

Under the Act a 'worker' is defined as an individual working in the private or public sector who acquired information on relevant wrongdoings in a work-related context and includes:

- employees and former employees;
- persons who provide or provided services to another party under contract;
- agency and former agency workers;
- board and former board members (including non-executive members);
- shareholders and former shareholders;
- trainees and former trainees;
- volunteers and former volunteers;
- job applicants;
- individuals involved in pre-contract negotiations; and
- members and former members of the Defences Forces (including the Reserves).

Section 22 of the Protected Disclosures Act 2014, substituted by section 30 of the Protected Disclosures (Amendment) Act 2022, requires public bodies to prepare and publish, by 01 March in each year, a report in relation to the previous year in an anonymised form.

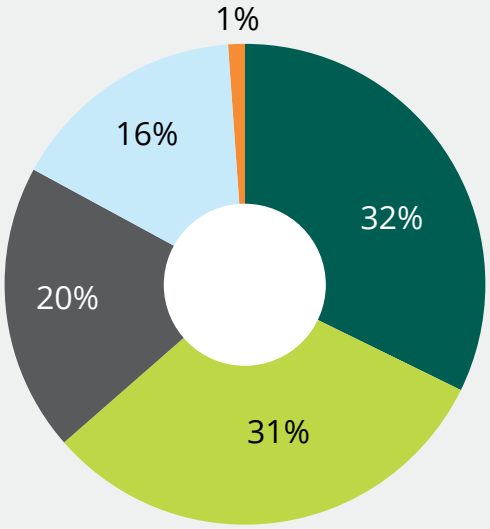
Pursuant to this requirement, the DPC confirms that in 2025:

87 potential protected disclosures (set out in the graphs below) were received from individuals external to the DPC in relation to issues pertaining to data protection within other entities. These issues were raised with the DPC in its role as a 'prescribed person' as provided for under section 7 of the Protected Disclosures Act (listed in SI 367/2020). In addition, one internal potential protected disclosure was received.

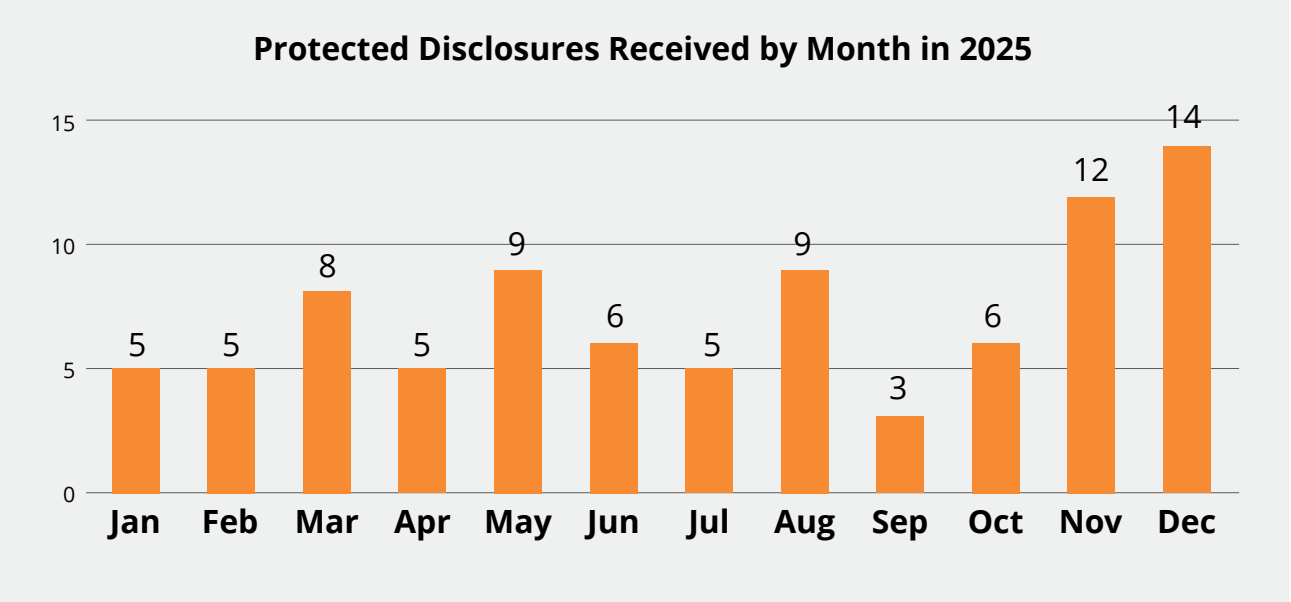
Of the 87 potential protected disclosures:

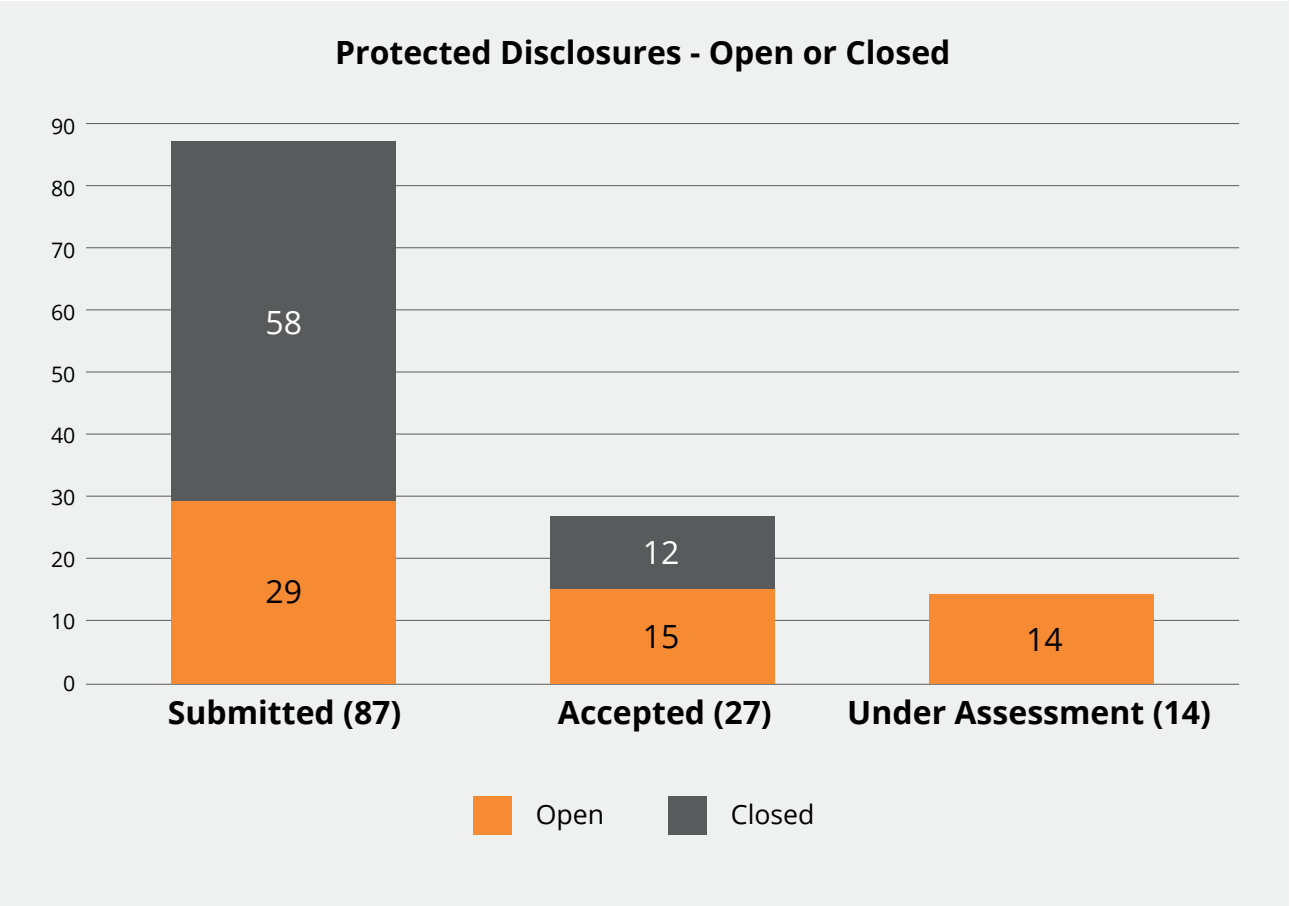
- 28 (32%) of the potential disclosures were assessed as warranting no further follow-up.
- 27 (31%) of the potential disclosures were assessed as warranting further follow-up.
- 17 (20%) of the potential disclosures were submitted anonymously.
- 14 (16%) were awaiting completion of assessment at year end as the DPC is awaiting further information from the reporting person in order to ensure the report qualifies as a Protected Disclosure.
- Seven potential disclosures submitted on average per month.

Outcome of Consideration



- Assessed as warranting no further follow-up. (28)
- Assessed as warranting further follow-up. (27)
- Referred to another more relevant procedure. (17)
- Awaiting completion of assessment at year end. (14)
- Repetitive report containing no meaningful new information. (1)


Protected Disclosures Received by Month in 2025
15
10
5
0
5
5
8
5
9
6
5
9
3
6
12
14
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec


Protected Disclosures - Open or Closed
90
80
70
60
50
40
30
20
10
0
58
29
12
15
14
Submitted (87)
Accepted (27)
Under Assessment (14)
Open
Closed

Appendix 2

Appendix 2: Energy Report 2025

Overview of Energy Usage

General

The DPC continues to monitor its energy consumption and ways to assist in the reduction of energy usage. We continue to participate in SEAI online monitoring.

The DPC took possession of its new head office building in January 2025 and finalised the fit out of the office for staff occupation on the 28 April. The existing buildings in Fitzwilliam Square and South Leinster Street were then closed down and returned to the OPW.

The new head office has a BER rating of A3 and provides 2,481m^2 of space compared to approximately 1,300m^2 available between the Fitzwilliam Square and South Leinster Street offices.

Note: The final figures for 2024 will not be available until April 2026, when the figures for both 2024 and 2025 will become available to the DPC.

Dublin
6 Pembroke Row

The new head office of the DPC is located at 6 Pembroke Row, Dublin 2. Energy consumption for the office is both electricity and gas.

As a modern building, the new office is expected to provide greater energy efficiency compared to the Georgian building in Fitzwilliam Square and the South Leinster Street office built in 2010, which had a BER C2 rating. Annual projected savings for electricity consumption is 104,000kWhs.

Portarlington

The Portarlington office of the DPC has an area of 444m^2 and is located on the upper floor of a two-storey building, built in 2006.

Energy consumption for the office is electricity for lighting and equipment usage and natural gas for heating. The energy rating for the building is C1.

Actions undertaken

The DPC participates in the SEAI online system for the purpose of reporting its energy usage in compliance with the European Communities (Energy End-use Efficiency and Energy Services) Regulations 2009 (S.I. No 542 of 2009).

The energy usage for the office for 2023 (last validated SEAI figures available) is as follows:

	Electrical	Natural Gas
Dublin		
Fitzwilliam Square Office.	61,653 kWh	
South Leinster Street Office	76,712 kWh	
Portarlington	28,400 kWh	18,589 kWh

The DPC is undertaking to achieve ISO50001 for the Pembroke Row office.

Overview of Environmental Policy/ Statement for the Organisation

The DPC is committed to operate in line with Government of Ireland environmental and sustainability policies.

Outline of environmental sustainability initiatives includes:

- purchase of single use plastics ceased since January 2019;
- ongoing replacement of fluorescent lighting with LED lighting in Portarlington office as units fail or require replacement bulbs;
- installation of sensor lights in refurbished area of Portarlington office;
- sensor lighting in use in South Leinster Street office;
- introduction of government energy conservation plans; and
- sensor lighting introduced in bathrooms Portarlington Office.

Reduction of Waste Generated

- DPC uses a default printer setting to print documents double-sided;
- DPC has also introduced dual monitors for staff to reduce the need to print documents to review/compare against other documentation during case work;
- DPC provides general waste and recycling bins at stations throughout the offices; and
- DPC has signed up for use of brown food waste bins.

Maximisation of Recycling

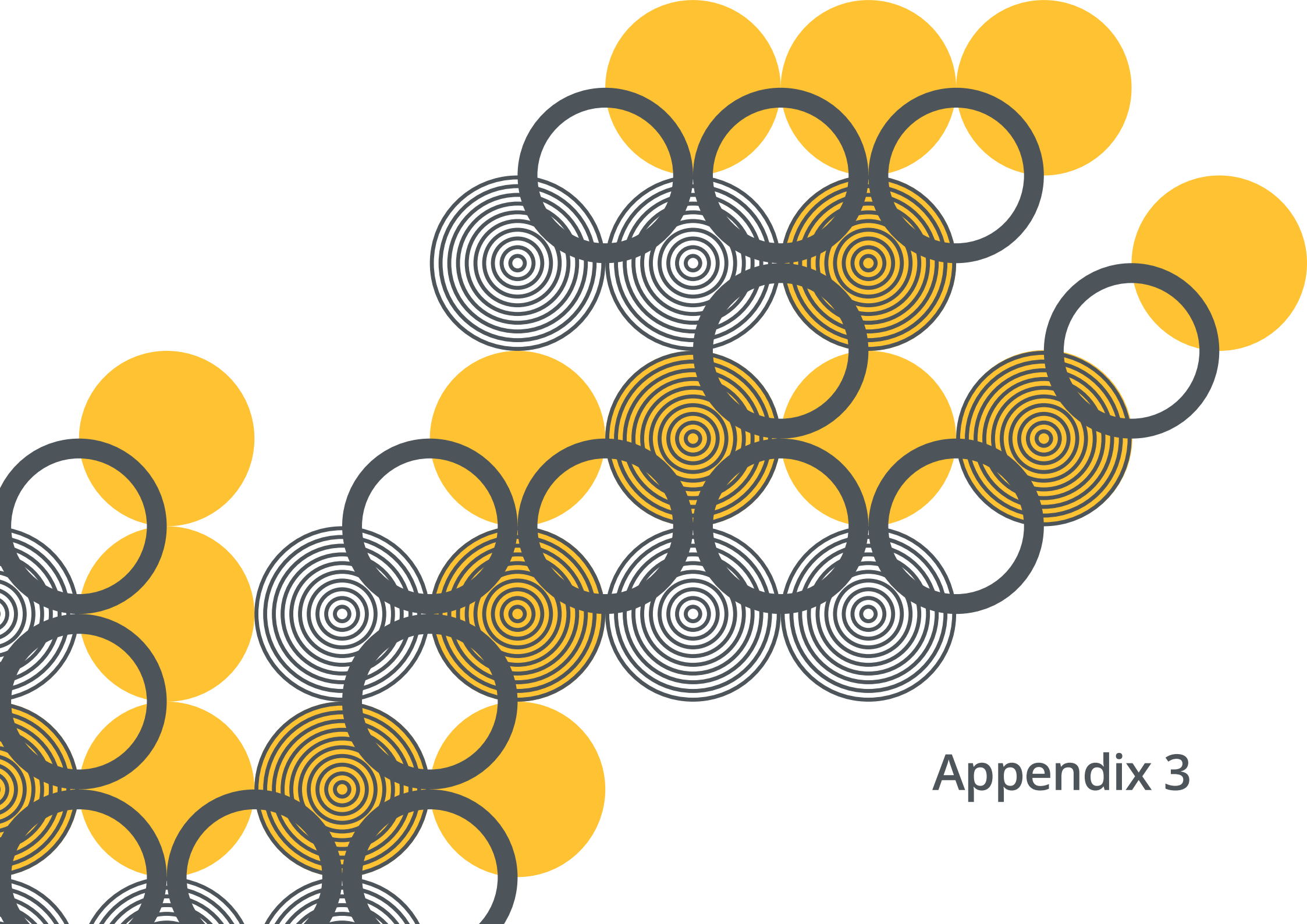
DPC policy is to securely shred all waste paper. Consoles are provided at multiple locations throughout the offices. Shredded paper is recycled.

Sustainable Procurement

PC procurements and processes are fully compliant with sustainable procurement. Catering contracts stipulate the exclusion of single use plastics.

Green Team

The DPC has reconstituted its Green Team with training provided to all 11 members.



Appendix 3

Appendix 3: Statement of Internal Controls

DPC Statement of Internal Controls the Financial Statement of the Data Protection Commission for the year 1 January 2025 to 31 December 2025 and its Statement of Internal Controls for the same period are in preparation by the DPC and will be appended to this report following the completion of an audit in respect of 2025 by the Comptroller and Auditor General.

Index

Notes

Notes

Notes

Data Protection Commission
6 Pembroke Row
Dublin 2
D02 X963
Ireland

(01) 765 01 00
1800 437 737
www.dataprotection.ie

An Coimisiún um Chosaint Sonraí
Data Protection Commission