

# Annual Report

2024



Coimisiún  
Cosanta Sonraí  
Data Protection  
Commission



## 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	4
Timeline of 2024	8
Executive Summary	10
Mission, Vision and Values at the DPC	14
1. Roles and Responsibilities	17
2. Contacts, Queries & Complaints	20
3. Breaches	32
4. Decisions and Inquiries	35
5. Litigation	60
6. Supervision	71
7. Children's Data Protection Rights	90
8. Data Protection Officers	95
9. International Activities	100
10. Human Resources, Communications and Corporate Governance	109
<b>Appendix 1:</b> Report on Protected Disclosures received by the Data Protection Commission in 2024	114
<b>Appendix 2:</b> Report on Energy Usage at the Data Protection Commission	120
<b>Appendix 3:</b> Statement of Internal Controls	123
Index	125

# Foreword

The Data Protection Commission's (DPC) regulation of Artificial Intelligence (AI) model training attracted a lot of public interest in 2024, but the Commission was active on several other fronts during what proved to be a very busy year.

- Four large scale inquiries were brought to a conclusion;
- Inquiries concluded into CCTV usage and data breaches on the domestic front;
- New inquiries were commenced into issues concerning AI models, biometrics, and the security of sensitive health data;
- Follow-up enforcement actions against two large technology platforms resulted in improved outcomes for children's personal data;
- A harmonised Europe-wide position was reached by the end of the year on how to comply with the General Data Protection Regulation (GDPR) when developing and deploying AI; and
- A range of other activities were also undertaken in the performance of our mandate.

This work and the results achieved in 2024, documented in this report, were made possible by the efforts and commitment of the DPC's staff. The year saw the DPC's workforce increase from 210 in January 2024 to 251 by December as our workload also expanded. Further staff increases will be required to meet the increased demands of implementing the GDPR and the EU Digital rulebook.

## Protecting our personal data

When fellow Commissioner Dale Sunderland and I took up office in February 2024, we laid a significant emphasis on the DPC's values as we engaged with the organisations we regulate, with our stakeholders and with our peer regulators. Internally, those values entail focusing on how DPC colleagues respect and support each other; externally, we acknowledge the values the DPC should exhibit as a regulator - fairness, consistency and transparency – and these should be inherent as we go about our work.

The EU Charter of Fundamental Rights and the GDPR establish the protection of personal data as a fundamental right and core value of the European Union. This right applies regardless of whom is processing our personal data - an individual, a Government agency or a private company. The GDPR has now been in force for seven years, and it continues to be the standard and benchmark for organisations, setting the guardrails for responsible, ethical and lawful use of personal data, and establishing strong

rights for individuals. When interpreted and applied in a balanced and proportionate manner that respects the essence of the right to data protection, the GDPR facilitates responsible and safe processing, and free flow of personal data which is vital for sustainable growth and prosperity in societal and economic terms.

The DPC aims to promote responsible personal data use and to foster innovation in its role both as Ireland's Data Protection Authority and the EU Lead Supervisory Authority (LSA) in cases where a company has its main establishment in Ireland. Through our Supervision and Engagement function, the DPC regularly engages with commercial organisations prior to market launch, as well as with public sector bodies developing and deploying public services, and shaping new legislation. The GDPR gives organisations the freedom to shape the specifics of their approach to meeting data protection obligations, but it also requires organisations to be accountable for their choices both to individuals and regulators. Proactive engagement and intervention can mitigate data protection risks and harms to individuals as well as ensuring that personal data is used in ways that are responsible, lawful and people-centred without giving carte blanche or advance approval of plans to any organisation.

## Fast paced evolving AI developments

There are potentially immense benefits to society arising from AI technologies but it is critical that new technological developments are introduced in a way that protects individuals, especially children and the vulnerable, from harm. As the European LSA for a number of large technology, social media and internet platform companies, the DPC engaged intensively throughout 2024 with a range of companies developing Large Language Models (LLMs). We made interventions in a number of cases where the DPC identified deficiencies and failures in plans to train AI models using personal data of EU/ EEA citizens which could expose users to significant risks and harms.

In order to bring greater clarity to the application of data protection requirements in AI model training and deployment, and to reach a harmonised EU position and level playing field for industry, the DPC for the first time requested a statutory opinion from the European Data Protection Board (EDPB) on AI model development. This initiative saw EU/ EEA regulators work intensively together in the EDPB over a 14-week period to achieve a unified position in December 2024.





### National and EU cooperation

In order to deepen engagement with our peer European and international data protection and privacy authorities, the DPC appointed a Deputy Commissioner responsible for EDPB and international affairs to lead DPC work in this area. In the context of EU Digital legislation being introduced, the DPC appointed a Deputy Commissioner to head a new inter-regulatory cooperation function with the aim of deepening engagement with both national and EU level regulators in other regulatory spheres. New digital legislation is intended to take effect without prejudice to the GDPR thereby creating an imperative for data protection authorities to work more closely and effectively with other digital regulators. Ireland's Digital Regulators Group is a good and effective example of this concept working in practice. Despite bringing additional complexity and volume to the DPC's workload, inter-regulatory cooperation has been set as a DPC priority in the interests of regulatory clarity and consistency.

Following the introduction of the EU AI Act during the year, the DPC was designated by Ireland as a fundamental rights body under the new legislation and it is also proposed that it will have a role as a market surveillance authority. New functions were also given to data protection authorities under the EU Political Advertising Regulation adopted in March 2024 which will give the DPC an important role in ensuring that during elections personal data is only used for advertising in accordance with the Regulation. In addition, negotiations on the EU's Procedural Harmonisation Regulation on the GDPR continued, aimed at streamlining cross-border complaint-handling and investigation processes.

In recognition of the DPC's European-wide responsibilities as an LSA, the resourcing of the DPC has been consistently supported by the Government. In light of new responsibilities and a significantly additional workload for the DPC as a result of the AI Act and other digital regulations, as well as the already substantial and increasing workload associated with our EU lead authority role and across all functions more generally, it is critical that we continue to receive funding increases enabling the expansion of our workforce. The Government's continuing support will be critical to the DPC's ability to meet its EU-wide responsibilities and the delivery of effective regulation in support of the digital economy.

### Helping individuals and organisations

During the year, the DPC continued to experience a high level of data protection concerns and complaints submitted by individuals to the DPC, which the office dealt with as expeditiously as possible. We continued to seek early resolutions of issues in the interest of the individuals concerned but also issued enforcement orders in cases where the organisations concerned did not respond in a satisfactory manner. Prosecutions taken under the E-privacy regulations for unsolicited marketing emails were an example of this.

Organisations also contacted the DPC looking for practical assistance which we provided through guidance and engagement.

Data breach notifications rose 11% during 2024. As set out in the report, the role of, and value placed on, the Data Protection Officer (DPO) in organisations is central to assisting the organisation to meet its GDPR obligations. The DPO is an independent role in gatekeeping data protection standards in organisations, and the extent to which a DPO is resourced and to whom they report internally can tell the regulator much about an organisation's approach to data protection. In November, the DPC hosted its DPO network conference in Croke Park which provided a forum for data protection professionals working in large and small organisations to share insights and challenges.

### Cross Border Inquiries and other enforcement

Enforcement is a central element of the regulatory environment that can achieve real outcomes and protections for individuals and, as such, works in parallel with the DPC's guidance, engagement and preventative work. This report details the conclusion of four large-scale cross-border inquiries in 2024 with no objections being raised by our peer DPA colleagues. In addition, three national inquiries were concluded. During the year, the DPC also commenced three new inquiries into Google (AI model training), the HSE (safety of sensitive personal data) and Ryanair (use of biometric data), responding both to concerns identified by the DPC and to complaints from other parties.

The year also saw the DPC follow up on earlier Inquiry decisions into the use of children's personal data. In inquiries related to TikTok and Instagram (see Annual Report 2023), the DPC had specified corrective measures it required the companies involved to address as part of the Inquiry findings. Notwithstanding the fact that the companies were appealing these decisions, the corrective measures orders continued to have effect and the DPC monitored enforcement of these, leading to successful outcomes including children's personal data now being set as private rather than public by default. This is an important measure to safeguard children from identity theft, impersonation and exposure to various forms of harmful interaction.

### Guidance and standard setting

Giving guidance and setting data protection standards – both nationally and with international peer regulators – is an important function of a data protection authority. In 2024 the DPC provided observations on 56 pieces of proposed legislation. The Commission also progressed a number of important sectoral engagements. It is incumbent upon the regulator to listen to and understand sectoral concerns and challenges which data protection obligations can present, as we wish to encourage data protection as an enabler of safe and responsible data use. Acknowledging the challenge for schools, particularly small primary schools, to understand their data protection obligations, we published a Schools

Toolkit in December having consulted with stakeholders in the education sector.

The DPC worked closely with a number of organisations involved in adult safeguarding during the year to understand their concerns, and we drafted guidance to assist these groups in implementing robust data protection safeguards whilst ensuring that barriers to identifying and responding to safeguarding concerns were minimised. The DPC also surveyed sports organisations and retailers during the year and we plan further outreach to organising bodies and stakeholders to improve awareness and data protection compliant practices in these sectors.

The GDPR is working well and is standing the test of time, but we must not lose sight of its essence which is to ensure that the individual right to data protection is respected and individuals do not suffer risks and harms as a result of their personal data being improperly used. As we seek to ensure the GDPR remains central in the development of new technologies, which will become increasingly commonplace in the public sector as well as the private sector, the DPC is committed to fair, proportionate, clear and consistent regulation to deliver real benefits and safeguards for individuals, whilst enabling responsible and people-centred innovation.



**Dr. Des Hogan**  
Chairperson,  
Commissioner for Data Protection



# Timeline of 2024

## Q1

- DPC publishes New Guidance on Managing your Digital Footprint
- Changing of the Guard! Following Helen Dixon departure from the DPC after two five year terms, Dr. Des Hogan and Dale Sunderland commence their roles as Commissioners of the DPC

## Q2

- DPC commence inquiry into the HSE concerning the storage and retention of personal data
- Following DPC engagement, Meta pauses plans to train LLM using public content shared by adults on Facebook and Instagram

## Q3

- DPC publishes new blog guidance AI, LLMs and Data Protection
- Following DPC High Court enforcement, X (Formerly Twitter) agrees to suspend its processing of personal data for the purpose of training AI tool "Grok"
- DPC inquiry concludes, fines Meta Platforms Ireland €91 million



# Q3

- Inquiry into Google AI Model launched by DPC
- DPC requests an Article 64.2 opinion from the EDPB on the use of personal data for the development and deployment of Artificial Intelligence ("AI") models.

# Q4

- DPC inquiry concludes with correct measures, fines LinkedIn €310 million
- DPC hosts the "Support DPO Success" Conference in Croke Park, Dublin
- DPC inquiry concludes, fines Meta Platforms Ireland €251 million
- Publishing new guidance "Data Protection Toolkit for Schools"
- DPC welcomes EDPB Opinion on the use of personal data for the development and deployment of Artificial Intelligence ("AI") models.

# Executive Summary

From 1 January 2024 to 31 December 2024 the DPC:

Received over

**32,000**

Contacts



Received

**24,306**

electronic contacts <sup>1</sup>

**6,751**

phone calls



**1,095**

postal contacts



Processed

**11,091**

new cases

Resolved

**10,510**

cases

**2,357**

progressed through the formal complaint-handling process.



<sup>1</sup> Electronic communications comprise both emails to the DPC's info@ account and webforms submitted through the DPC website.

Total valid breach notifications received by the DPC in 2024 was

7,781

an eleven percent (11%)  
increase on 2023



Of those breach notifications  
received in 2024

81%

were concluded by year end

50%

of notified cases arose as a  
result of correspondence  
being sent to the wrong  
recipient



DPC Inquiries and Decisions in 2024:

Issued over

€652

million in  
administrative fines



4

Large Scale  
Inquiries  
concluded

89

Statutory Inquiries  
on-hand as of  
31 December



4

Preliminary  
Draft  
Decisions

7

Draft  
Decisions

11

Finalised  
Decisions

115

notifications  
of amicable  
resolutions

**In 2024 the DPC announced the commencement on new national and cross-border inquiries into**

Biometrics



Artificial Intelligence models

Security of sensitive health data



**Follow-up enforcement actions with companies arising from previous cross-border inquiries resulted in**



Improved outcomes for children's personal data and safety

**Since 1 January 2024 the DPC:**

Received

**1,175**

GDPR Article 61 Mutual and Voluntary Mutual Requests for assistance from other European Regulators



Participated in over

**180**

European Data Protection Board (EDPB) meetings



Provided input and observations on

**56**

pieces of proposed legislation



The lead SA reviewing

**16**

Binding Corporate  
Rules (BCR) applications  
for

**11**

Different companies



Introduced

**2**

New Functions  
Inter-Regulatory Affairs  
EDPB & International Affairs

**80**

Speaking events



**146**

Electronic direct  
marketing investigations  
resulted in

**8**

Companies  
prosecuted



Produced  
data protection  
toolkit for schools



DPC spearheaded  
questions to EDPB  
regarding:

AI Opinion

# Mission, Vision and Values at the DPC

## Mission

Upholding 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 amalgamating the expert capacities of its staff to ensure operational effectiveness.

## Vision

The DPC is committed to being an independent, internationally influential and publicly dependable 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 will play a leadership role in bringing legal clarity to the early years of the General Data Protection Regulation. The DPC will apply a risk-based regulatory approach to its work, so that its resources are always prioritised on the basis of delivering the greatest benefit to the maximum number of people. The DPC will also be 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.

## Values

The DPC is an autonomous regulator, with responsibility for regulating both private and public sector organisations, as well as safeguarding the data protection rights of individuals. In the conduct of these duties, the DPC is committed to act always in a way that is: Fair, Expert, Consistent, Transparent, Accountable, Forward Looking, Engaged, Independent and Results-driven.

We are always

Fair

Expert

Consistent

Transparent

Accountable

Forward Looking

Engaged

Independent

Results-driven



## Regulatory Strategy

In December 2021, the DPC published its Regulatory Strategy for 2022-2027, which is the roadmap for the DPC to deliver 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. In late 2024, the DPC commenced a mid-point re-evaluation of its Regulatory Strategy. This re-evaluation will conclude in 2025.



---

# 1

---

## Roles and Responsibilities





# Roles and Responsibilities

## Functions of the DPC

The DPC is the national independent authority in Ireland responsible for upholding the fundamental right of EU persons to have their personal data protected. Accordingly, the DPC is the Irish supervisory authority 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 right to the protection of one's personal data is set out in EU law in the EU Treaties and in the EU Charter of Fundamental Rights. In 2016, the EU adopted a new legal framework in the GDPR to give effect to this right. 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
- to act as EU Lead Supervisory Authority for data controllers with their main establishment in Ireland.

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

In addition to its functions under the GDPR, the DPC continues to perform its regulatory functions under the **Data Protection Acts 1988 and 2003**, in respect of complaints and investigations 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 44

The DPC is funded by the Exchequer and does not derive monetary gain from fines imposed. The Chairperson of the Commission is the Accounting Officer for the Commission's Vote – Vote 44.

The DPC's 2024 estimate provision was **€28.126M** of which €18.862M was allocated for pay related expenditure, and €9.439M of which was allocated to non-pay expenditure.

The funding for 2024 represented an increase of €2.047M on the 2023 allocation.



The DPC Senior Management Team from left to right: Cian O'Brien, David Murphy, Dr Des Hogan, Jennifer Dolan, MB Donnelly, Diarmuid Goulding, Dale Sunderland, Ultan O'Carroll, Gráinne Duffy, Elizabeth Finn, Graham Doyle, Fleur O'Shea, Cathal Ryan, Ian Chambers, Labhras Sammin, Andrew Carroll, Gráinne Hawkes, Niall Cavanagh.

## DPC's Senior Team

The DPC's Senior Management Committee (SMC) comprises the Commissioners for Data Protection, Director 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).

### During 2024, the SMC comprised:

- Dr Des Hogan Chairperson, Commissioner for Data Protection (from February 2024);
- Dale Sunderland, Commissioner for Data Protection (from February 2024);
- Cian O'Brien, Director and Deputy Commissioner with responsibility for Large-Scale Inquiries including Investigations & Cross Border Complaints;
- 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, Breach, Complaints and Information;
- Jennifer Dolan, Deputy Commissioner, Head of Inter Regulatory Affairs & E-Privacy Prosecutions;
- MB Donnelly, Deputy Commissioner, Head of Strategy, Governance, Finance 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;
- 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;
- 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.

*\* Former Commissioner for Data Protection, Helen Dixon, was a member of the SMC until February 2024.*

---

# 2

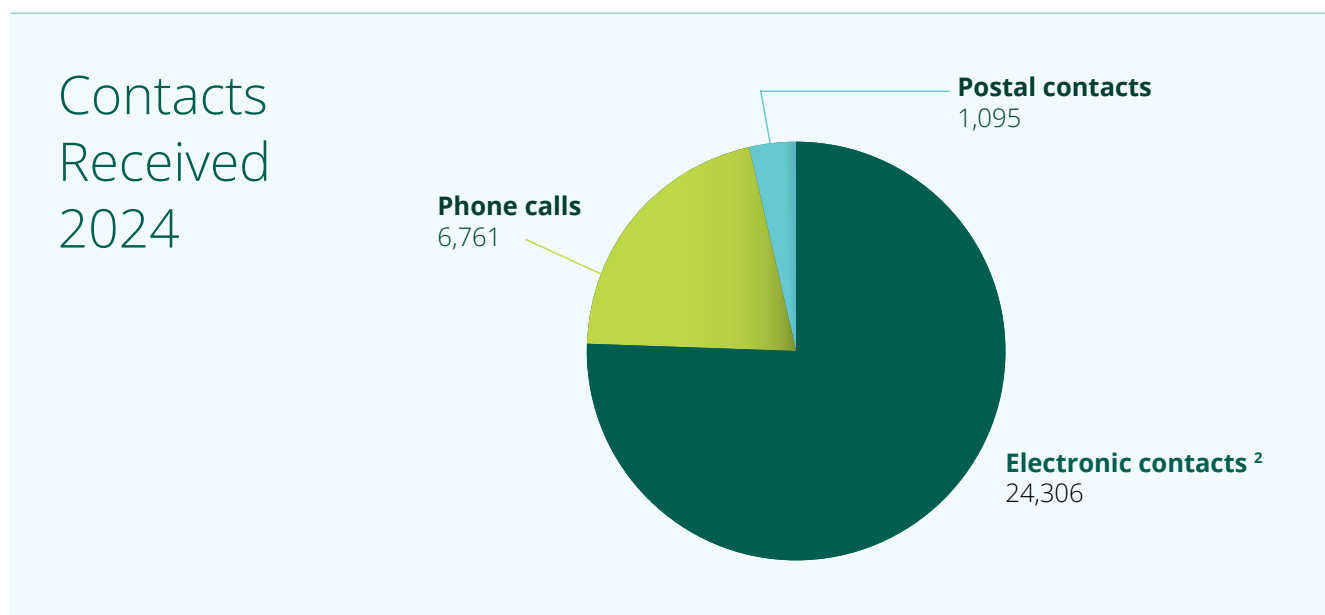
---

Contacts, Queries  
& Complaints



# Contacts, Queries & Complaints

Individuals and organisations contact the DPC in a variety of ways, including the DPC Helpdesk phone lines, online web forms, email and post.



## Contacts/Queries

### Between 1 January 2024 and 31 December 2024:

The DPC received over **32,000** contacts. This figure consists of **24,306** electronic contacts<sup>1</sup>, **6,751** phone calls and **1,095** postal contacts.

The cases raised with the DPC reflect common challenges that individuals face when exercising their data protection rights. Subject Access Requests (SARs) dominate the list, whether due to non-response or dissatisfaction with the response provided by the organisation in question. Concerns relating to consent, personal data disclosure, and domestic CCTV highlight the public's continuing awareness of data protection issues in both personal and organisational contexts.

When individuals contact the DPC raising a concern, the DPC generally engages directly with the organisation whose behaviour is at issue, 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 that details the issue and the positions of both parties. This documentation helps streamline the assessment of a matter raised by an individual.

The DPC strives to ensure that individuals are supported in understanding their rights under the GDPR, while also encouraging organisations to be transparent and accountable in their data processing activities. In resolving cases the DPC often reviews an organisation's compliance efforts.

The DPC provides a dedicated telephone service for the public's queries about data protection. The information desk serves primarily as a resource for clarifying basic queries. For complex or complaint-related issues, individuals and organisations are advised to submit their concerns in writing via email to [info@dataprotection.ie](mailto:info@dataprotection.ie) or by post to:  
**6 Pembroke Row, Dublin 2, D02 X963, Ireland**

Additionally, individuals who face barriers in contacting the DPC in writing can avail of the DPC Accessibility Officer's support at: [DPCAccessibilityOfficer@dataprotection.ie](mailto:DPCAccessibilityOfficer@dataprotection.ie)

This ensures that the DPC's services remain inclusive and accessible to all.

<sup>1</sup> Electronic communications comprise both emails to the DPC's info@ account and webforms submitted through the DPC website.



In 2024, the Top 5 queries received through **Electronic and Postal contacts** were

Non-response to Subject Access Request

Consent as legal basis to process personal data

How to make a Subject Access Request

Domestic CCTV

Further process of personal data by an organisation



Top 5 queries to the DPC **Telephone Information desk**

General guidance regarding GDPR legislation

Domestic CCTV

Guidance on how to make a Subject Access Request

Concerns regarding the processing of personal data

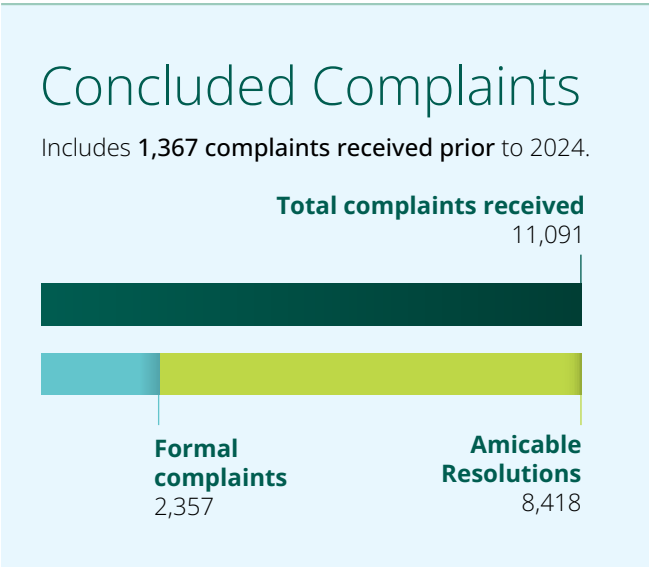
How to submit a breach notification



### Complaints

During 2024, the DPC received **11,091** new cases<sup>1</sup>. **2,673** of which progressed to the formal complaint-handling process, including **194** electronic direct marketing complaints.

Overall, the DPC concluded **2,357** formal complaints in 2024, including **1,367** complaints received prior to 2024. In addition to **8,418** cases resolved through amicable means.



Complaints are assessed to determine if the issue is a complaint as defined under the Acts (namely that the matter relates to the processing of the individual's personal data and that there has been an infringement of the individual's data protection rights). The DPC must also assess whether the DPC is the appropriate authority to examine the complaint or if the complaint falls under the remit of another data protection regulator.

### Complaint Handling

The DPC processes complaints under four main legal frameworks:

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

Top 3 Issues in complaints received under the GDPR (65% of overall cases)	% of total
Subject Access Request	34
Fair Processing	17
Right to Erasure	14

<sup>1</sup> 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 have a complaint element. The figure does not include contacts from the media, speaking invitations, breach notifications or prior consultation.

### 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. This is an important right which gives rise to the largest number of national complaints to the DPC annually, accounting for over **thirty four per cent (34%)** of all complaints.

Under Article 15 of the GDPR, sets out the obligations organisations must comply with upon receipt of a subject access request. Article 15 essentially comprises of eight different elements as listed to the right.

## Largest share of national complaints

Right to request sufficient, transparent and easily accessible information about the processing of personal data (GDPR Article 15)

Access Requests

34%

Non Access Requests



## Subject Request Obligations

1. Confirmation as to whether or not the organisation is processing personal data concerning you.
2. Access to your personal data.
3. Access to the following information on the processing:
  - a. the purposes of the processing of your personal data;
  - b. the categories of your personal data;
  - c. the recipients or categories of recipients of your personal data;
  - d. the envisaged duration of the processing or the criteria for determining the duration;
  - e. the existence of your right to rectification, erasure, restriction of processing and objection to processing;
  - f. the right to lodge a complaint with a supervisory authority;
  - g. any available information on the source of your personal data, if not collected from you;
  - h. the existence of automated decision-making, including profiling and other information relating thereto.
4. Information on safeguards pursuant to Art. 46 where your personal data is transferred to a third country or to an international organisation.
5. The obligation of the organisation to provide a copy of your personal data undergoing processing.
6. Charging of a reasonable fee by the organisation based on administrative costs for any further copies requested by the you.
7. Provision of information in electronic form.
8. Taking into account the rights and freedoms of others (Article 15(4) restriction).

By the end of 2024, the DPC had received **914** new complaints solely related to the right to access and concluded **904**.

The failure of organisations to reply to individuals regarding their subject access request within the required timeframe, combined with the application of redactions or exemptions by the organisation, accounts for many of the complaints received by the DPC.

While the redactions or exemptions are for the most part appropriately applied, the complaints stem from insufficient explanations by the data controller as to why they are being applied. It is not sufficient for an organisation to merely itemise the exemptions, restrictions or relevant articles of the legislation. The reason the exemption is being applied should be clearly explained to the individual. Any exemptions applied should be documented, for example, in the form of a table. Organisations must always be able to explain to the DPC why they have applied specific exemptions.

Accordingly, issues arise where the organisation does not:

- Respond to the individual in relation to the subject access request within one-month of receipt of the request or within two further months if there is a delay, and the reason for the delay is explained to the individual; and/or
- Explain clearly to the individual why the data requested cannot be released to them

For further information on handling subject access requests, organisations should review the DPC Guidance here:

[Subject Access Requests: A Data Controller's Guide QR 1](#)



QR 1

### Erasure requests

The right to have your personal data deleted is also known as the “right to erasure” or the “right to be forgotten”. This is not an absolute right and only applies in specific circumstances including when:



## Right To Erasure Circumstances

- The organisation no longer needs your data for the original reason they collected or used it for.
- You initially consented to the organisation using your data, but have now withdrawn your consent and where there is no other legal ground for the processing.
- You have objected to the use of your data, and your interests outweigh those of the organisation using it.
- The organisation has collected or used your data unlawfully.
- The organisation has a legal obligation to erase your data.
- The data was collected from you as a child for an online service.

Erasure requests account for an increasingly large volume of complaints to the DPC, which stood at **fourteen percent (14%)** of complaints submitted. The majority of cases that come before the DPC arise because the organisation in question did not respond to the request in a timely manner and/or did not clarify with the individual the reasoning as to why the right to erasure was not applicable in the specific



circumstances. The DPC has seen an increase in the number of complaints submitted relating to erasure requests related to medical data. The DPC published a detailed FAQ related to this topic in an effort to assist individuals in understanding, in particular, why the erasure of medical data is particularly problematic (see link below).

Reasons for refusing an erasure request may include:

- Exercising the right of freedom of expression and information;
- Complying with a legal obligation or for the performance of a task carried out in the public interest or where processing is required as part of the official authority assigned to the organisation;
- Public interest in the area of public health;
- Archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and/or
- Establishment, exercise or defence of legal claims.

An organisation must be able to clearly and concisely explain to an individual why their personal data cannot be erased and for how long the organisation will continue to process the personal data in question.

The more effective the communication between an individual and organisation, the more likely it is to result in complaints being resolved prior to the DPC's involvement, or through the amicable resolution process facilitated by the DPC.

Further guidance on erasure is available at

[12 Steps to GDPR Compliance](#) **QR 2**

[Amending or Erasing Medical Records](#) **QR 3**

**QR 2****QR 3**

### Complaint Outcomes

In accordance with section 109 of the 2018 Act, the DPC will take such actions as it considers appropriate in relation to a complaint, which are the rejection or dismissal of a complaint, the issuing of an enforcement notice, the commencement of a complaint based inquiry, the issuing of a reprimand or any other action the DPC considers appropriate.

In 2024, the DPC continued to receive a large volume of complaints, with amicable resolution continuing to be an effective means to resolve complaints. The DPC encourages organisations to engage in a meaningful way with the process in the interest of achieving early outcomes for the complainants concerned.

### Enforcement

The DPC utilises its powers of enforcement against an organisation when it becomes apparent that the organisation is failing in its obligations under data protection legislation. The most common example is where an organisation does not engage at all with either the individual or the DPC.

The DPC issued **eight Enforcement Notices** throughout 2024. The majority of notices relate to non-response to access requests.

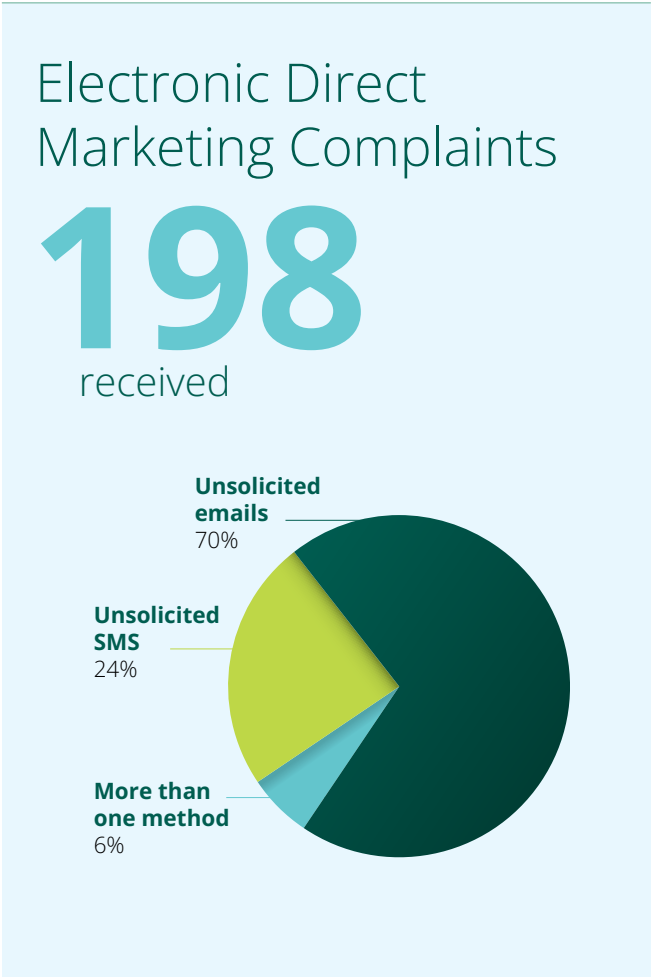
In 2024, the DPC conducted a number of site visits related to small enterprises to engage with the organisations to remind them of their GDPR obligations and point them towards guidance available from the DPC and other sources. This has proven to be very productive in terms of resolving matters expeditiously. It also allows information regarding data protection obligations to be provided in a cooperative and supportive manner.

***Complaint case studies are being published separately to this Annual Report.***

Electronic Direct Marketing Complaints

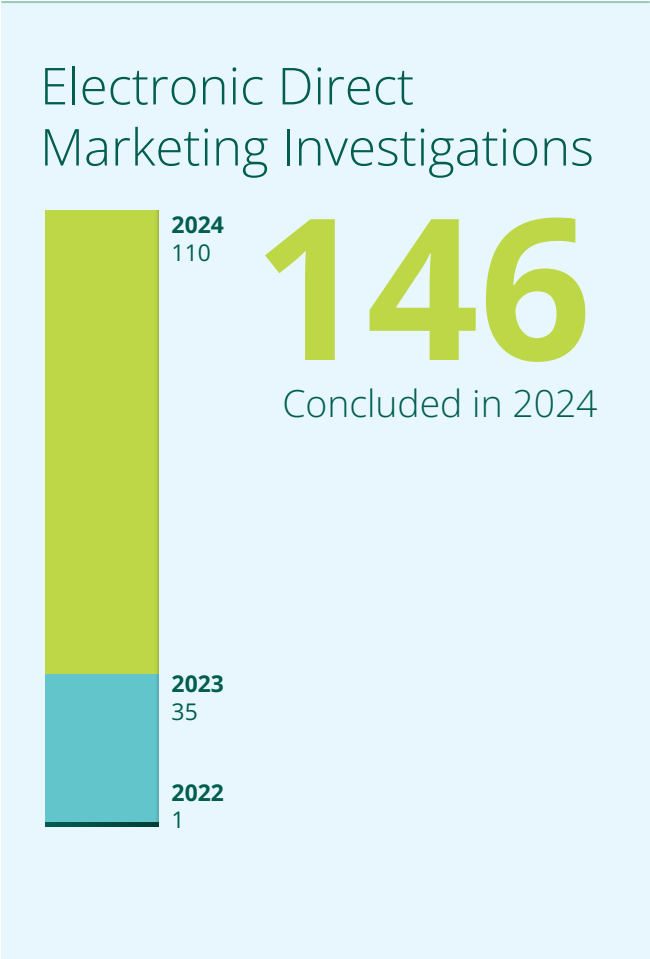
The DPC actively investigates and prosecutes offences relating to electronic direct marketing under Statutory Instrument 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (“the ePrivacy Regulations”). The ePrivacy Regulations transposes Directive 2002/58/EC (“the ePrivacy Directive”) into Irish law.

In 2024, the DPC received **198 new complaints** in relation to electronic direct marketing. Seventy per cent (70%) of complaints related to unsolicited email communications, twenty four per cent (24%) to unsolicited SMS text messages, and six (6%) involved more than one form of electronic direct marketing method, for example the complaint related to both unsolicited SMS text messages and emails from the same organisation.



**146** electronic direct marketing investigations were concluded in 2024. This figure comprises:

- 1 complaint from 2022,
- 35 complaints from 2023; and
- 110 complaints from 2024.



In 2024, the DPC issued **49 warning letters** to companies on foot of unsolicited marketing communications, and **prosecuted eight companies** for the sending of unsolicited marketing communications to individuals without consent.

49

warning letters on  
foot of unsolicited  
marketing  
communications

8

companies prosecuted  
for sending unsolicited  
marketing  
communications

In all prosecution cases, the Court directed the companies to make charitable contributions in lieu of a conviction and fine. These charitable donations amounted to **€9,725 across all eight cases**. In all cases, the companies were instructed to discharge the DPC's legal costs.

These cases, published on the DPC website, highlight the DPC's ongoing commitment to enforcing the ePrivacy Regulations and holding data controllers accountable for the processing of personal data in marketing practices. Those engaged in electronic marketing activities should take note of the consequences, which may arise if they breach the regulations. It is critical that before embarking on electronic marketing campaigns, companies carry out robust testing and checks with their service providers to ensure that they have the valid and up-to-date consent of the individuals on their marketing lists and that their opt-out mechanisms are fully functional.

All of the companies prosecuted by the DPC in 2024 had each received a prior warning to correct inadequate processes and procedures for electronic marketing. The companies and sectors involved included an advertising agent, a telecommunications network, and companies within the hospitality and travel sector, as well as the cosmetics and fitness industry.

***Case studies detailing these prosecutions are being published separately to this Annual Report.***



In October 2024, Commissioner Des Hogan delivered the key-note address at the Law Society's annual In-house and Public Sector Conference on the theme "From Law to Leadership".



In November 2024, DPC Commissioners Des Hogan and Dale Sunderland participated in a fireside chat at IAPP's Europe Data Protection Congress in Brussels on the topic of "Changes at Ireland's DPC: An Introduction to the New Commissioners", moderated by Kate Colleary of Pembroke Privacy.

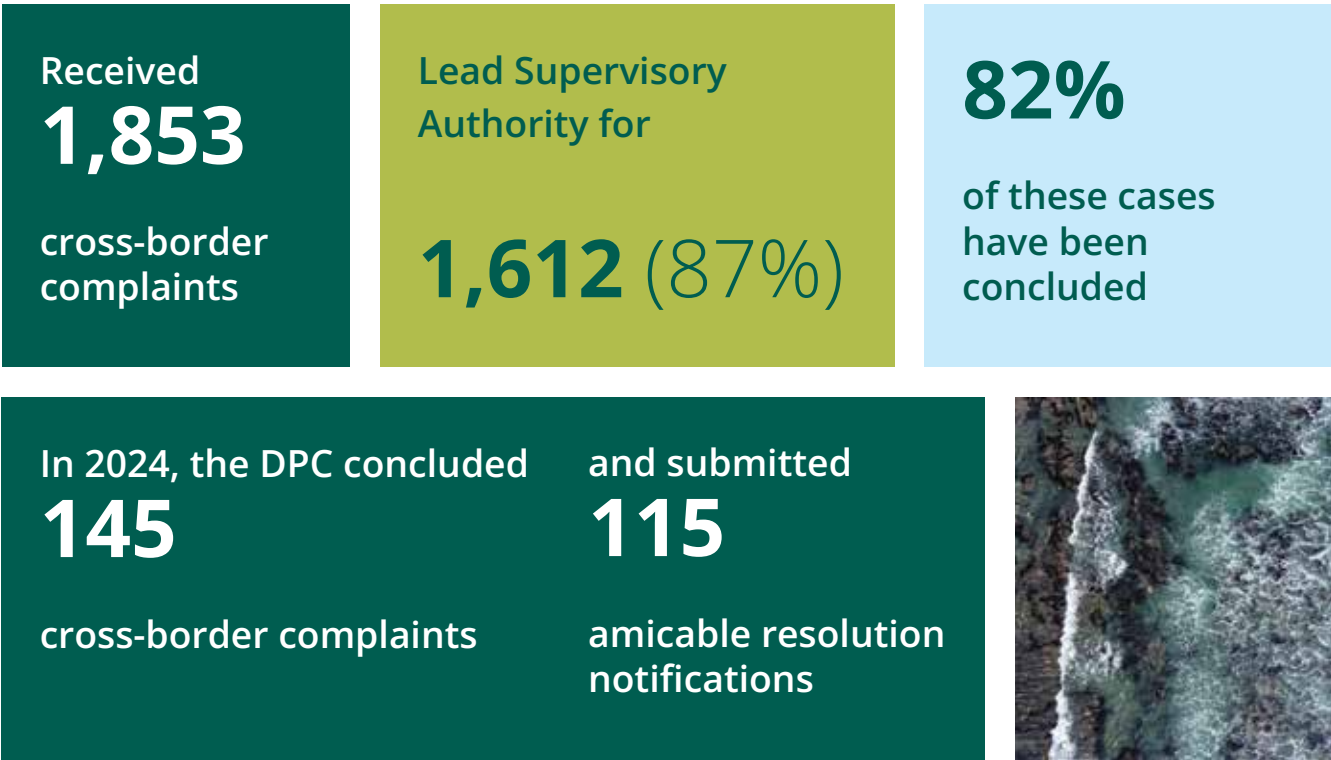
One-Stop-Shop Complaints

The One-Stop-Shop mechanism (OSS) was established under the GDPR with the objective of streamlining how organisations conducting business in more than one EU member state engage with data protection authorities (called “supervisory authorities” under the GDPR).The OSS allows these organisations to be subject to direct oversight by a single lead supervisory authority (LSA), where they have a “main or single establishment”, rather than being subject to separate regulation by the data protection authorities of each member state. The main or single establishment of an organisation is generally its place of central administration and/or decision making in the EU/EEA. Under the OSS mechanism, the Data Protection Authority which received the complaint acts as a concerned supervisory authority (CSA). The CSA is the intermediary between the LSA and the individual. An individual in an EU/EEA state may thus lodge a complaint directly with the supervisory authority that is the LSA or they may lodge it with their local/ national authority, which will transmit it to the LSA. In this way the DPC acts as a regulator for EU citizens.

Since the implementation of the GDPR, the DPC has received a total of **1,853 cross-border complaints**, for which the DPC has been established as the Lead Supervisory Authority for **1,612 (eighty seven per cent (87%))** of which **1,327 (Eighty two per cent (82%))** of the valid cross-border complaints, for which the DPC is the LSA, have now been concluded. Since May 2018, **sixty three per cent (63%)** of cross-border complaints, where the DPC is LSA, were lodged by complainants with another EU/EEA supervisory authority and then transferred to the DPC via the OSS mechanism. **Thirty seven per cent (37%)** of cross-border complaints were lodged with the DPC directly.

In 2024, the DPC concluded **145 cross-border** complaints and submitted **115 notifications** (through the GDPR Article 60 cooperation mechanism of cases where an amicable resolution had been achieved. Details of these cases can be found published on the EDPB website.

Since the implementation of the GDPR the DPC:



## 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 entities which are “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.

Since May 2018, **eighty four per cent (84%)** of complaints examined by the DPC under LED have been related to Subject Access Requests. The second most common complaint type examined under LED, at seven per cent (7%), are those requesting rectification or erasure. The majority of requests are directed towards AGS in its role as the most prominent law-enforcing agency in the state.

In 2024, the DPC received **33 LED complaints and concluded 19 LED complaints** (including complaints received prior to 2024 but not concluded within those calendar years).

Further information on LED is available at the DPC website:

[Law Enforcement Directive Data Protection Commission QR 4](#)



QR 4

## Direct Intervention

The DPC’s Direct Intervention Unit 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.

Some of the matters prioritised by the Direct Intervention Unit in 2024 included:

- Processing of health data by organisations for purposes other than that for which it was originally processed;
- Processing of health data by nursing homes and lack of appropriate safeguards for vulnerable residents; and
- Organisations requesting excessive data for the provision of services to adults in vulnerable situations.

The DPC’s Direct Intervention Unit also contributed to the creation of targeted DPC guidance reflecting matters which come to the DPC’s attention. One such example of this is the updated “CCTV Guidance for Data Controllers” which now includes an in-depth section on the use of CCTVs in restrooms and areas where there is an increased expectation of privacy. This guidance has assisted controllers in complying with their GDPR obligations and has led to a reduction in concerns being raised with the DPC regarding the use of CCTV in such areas.

In line with its Regulatory Strategy 2022-2027, the DPC continues to uphold the rights of those vulnerable groups who may require additional assistance in ensuring their rights are protected.

[CCTV Guidance Data Controllers QR 5](#)



QR 5



## Complaints under the Data Protection Acts 1988 & 2003

The DPC received two valid complaints that fell to be considered under the Data Protection Acts 1988 & 2003 in 2024. The DPC issued **12 decisions in 2024** consisting of:

- 6 complaints being partially upheld;
- 3 complaints being upheld; and
- 3 complaints being rejected

## Domestic CCTV Complaints

The DPC continues to receive significant volumes of complaints related to the operation of domestic video surveillance systems. In 2024, the DPC **received 157 such complaints**. The DPC has published guidance focused on the use of such systems: [Domestic CCTV](#). **QR 6**

It is important to note some key data protection principles, which relate to the operation of such systems and the extent to which data protection laws apply:

- **The household exemption**

Data protection law does not apply to the processing of personal data where the personal data is kept by an individual and is concerned solely with the management of his/her personal, family or household affairs or kept by an individual for recreational purposes (Article 2(2)(c) of the GDPR). This applies as long as the personal data is not used in connection with a professional or commercial activity or made publicly available. With regards to domestic video surveillance systems, European case law has established that the act of continuously recording footage outside the confines of one's own property falls outside the household exemption, and that the GDPR therefore applies in full.

- **Lawful basis**

Where CCTV is being operated outside the household exemption the act of data processing, which is the recording of individuals walking past the operator's residence or otherwise capturing personal data, requires a lawful basis. Insofar as the lawful bases for the processing of personal data are found under Article 6 of the GDPR, it is for CCTV operators to identify and demonstrate their lawful basis for processing prior to conducting any recording outside of the household exemption.

- **Compliance with other obligations**

The operation of CCTV systems outside of the household exemption is subject to a number of other obligations, such as the requirement to have signage in place stating that CCTV is in operation, and which include the contact details of the CCTV operator to ensure that GDPR rights requests can be made by individuals. CCTV operators are also required to comply with and respond to access and erasure requests, amongst other rights provided for by the GDPR, as well as to have a retention schedule in place with regards to the personal data which they are processing.

It is the advice of the DPC that anyone operating a CCTV camera in their home should ensure that the operation of the camera falls within the household exemption. By doing so they would not then be subject to the usual obligations that data controller would be obliged to consider as required by the GDPR.



**QR 6**



---

# 3

---

## Breaches



# Breaches

Organisations are obliged to notify data breaches to the DPC. Such notifications usually come through an organisation's Data Protection Officer (DPO). The DPO can distinguish minor from major breaches. The DPC works closely with DPOs to mitigate data breaches where they occur. Early responses can be invaluable in addressing financial, legal and reputational risks to organisations as well as in vindicating the rights of the data subjects concerned.

In 2024, the DPC received **7,781 valid data breaches**. This represented an **eleven per cent 11% increase** (794) on the overall data breach numbers received by the DPC in 2023. Of the notifications received, **7,346** were **GDPR** notifications and, of those:

- **3,958** related to the private sector;
- **3,137** to the public sector; and
- **251** came from the voluntary and charity sector.

**Fifty per cent (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 2024 related to unauthorised disclosures in incidents affecting single individuals or small groups, accounting for **sixty per cent (60%)** of total notifications.

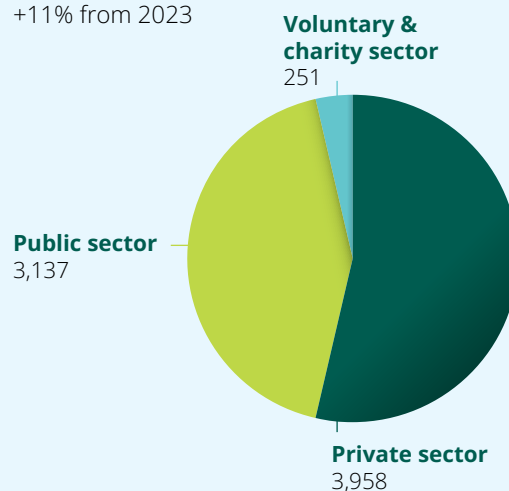
Of the breach notifications received in 2024, **eighty one per cent (81%)** were concluded by year-end.

In keeping with the trend of previous years, public sector bodies and banks accounted for the “top ten” organisations with the highest number of breach notifications recorded against them. Insurance and telecom companies featured prominently in the top twenty. 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 via its supervisory function 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.

## Valid Data Breaches 2024

7,781

+11% from 2023



50%

breaches  
result of  
correspondence  
sent to wrong  
recipient

81%

breach  
notifications  
received  
concluded

**Breach Notifications: Nature of Breach for cases received 2024**

Nature of Breach	Total as %
Unauthorised disclosure - postal material to incorrect recipient	32%
Unauthorised disclosure - email incorrect recipient	14%
Accidental/unauthorised alteration of personal data	10%
Loss or destruction of personal data - accidental	8%
Hacking	5%

**EPrivacy Breaches:**

The DPC received **428 e-privacy data breach notifications** (an increase of over one hundred and ninety three per cent (193%) on the 146 figure for 2023) under the ePrivacy Regulations, accounting for just over six per cent (6%) of total breach cases notified in 2024.

This increase in notifications follows on from a similar trend in 2023, in which the DPC saw a rise in ePrivacy breach notifications as a result of the entry into force of the Electronic Communications Code Regulations in September 2022 and the expanded definition of the term “electronic communications service”.

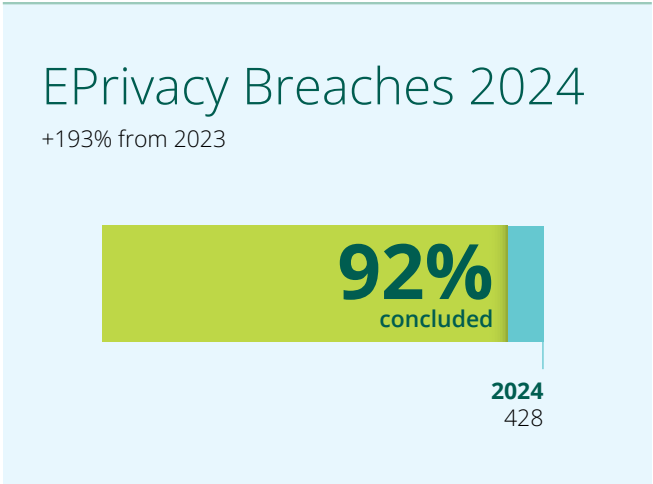
The most frequent cause of ePrivacy breaches reported to the DPC arose as a result of:

- Incorrect recording of details due to human error, which resulted in a breach (e.g. email addresses/phone numbers recorded incorrectly);
- Communications directed to the wrong recipients (postal addresses/Eircodes recorded incorrectly or postal details not updated by individuals);
- Social engineering/ phishing schemes (third parties gaining access to customer accounts, including access to personal details).

The majority of breaches reported were in relation to a single individual and involved personal data being disclosed in an unauthorised manner, or correspondence being inadvertently misdirected to the wrong recipients.

Only one per cent (1%) of the breaches reported involved more than 100 individuals.

**Ninety two per cent (92%)** of the 428 breaches were concluded by year end.



**Law Enforcement Directive Breaches**

The DPC also received **79** valid breach notifications in relation to the LED, (Law Enforcement Directive (EU) 2016/680), which was transposed into Irish law by the 2018 Act.

**Data Breach Complaints**

Data breach complaints arise where an individual makes a complaint to the DPC, having become aware of a breach of their personal data. In 2024, the DPC handled **20 complaints** relating to alleged personal data breaches which were not resolved through an amicable resolution process.

***Breach case studies are being published separately to this Annual Report.***

---

# 4

---

## Decisions and Inquiries





# 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 2024, the DPC had **89 Statutory** Inquiries on-hand, including **53 Cross-border Inquiries**.

## Decisions that were taken in 2024

Organisations	Decision Issued	Fine Imposed	Corrective Measure Imposed
<b>Airbnb Ireland UC</b>	31 January 2024	N/A	Reprimand re Articles 5(1)(c) and 6 of the GDPR.
<b>Apple Distribution International Limited</b>	29 February 2024	N/A	No infringements found.
<b>Groupon Ireland Operations Limited</b>	8 March 2024	N/A	Reprimand re Articles 5(1)(c), 6(1), 12(2), 15(1), 15(3) and 17(1) of the GDPR.
<b>Apple Distribution International Limited</b>	8 March 2024	N/A	Order to bring processing into compliance and Reprimand re Articles 13(1)(c) and 13(1)(d) of the GDPR.
<b>Mediahuis Ireland Group Ltd (formerly Irish News and Media plc)</b>	7 June 2024	N/A	No infringements found.
<b>Meta Platforms Ireland Limited</b>	26 September 2024	€91 million	Reprimand re Articles 5(1)(f), 32(1), 33(1), and 33(5) of the GDPR.
<b>LinkedIn Ireland Unlimited Company</b>	22 October 2024	€310 million	Order to bring processing into compliance and Reprimand re Articles 5(1)(a), 6(1), 13(1)(c) and 14(1)(c) of the GDPR.

Organisations	Decision Issued	Fine Imposed	Corrective Measure Imposed
Sligo County Council	13 November 2024	€29,500	Temporary ban on CCTV at a number of locations. Order to bring processing into compliance and Reprimand re: Articles 5(1)(a), 5(1)(c), 5(1)(e), 5(1)(f) 13, 24, 25, 30, and 32(1) of the GDPR. Sections 71(1)(a), 71(1)(c), 71(1)(e), 71(1)(f), 71(10), 72, 72(1), 72(2), 75, 75(1), 75(3) 76(2), 78, 79, 81, 82(2), 84 and 90(1) of the Data Protection Act 2018.
Maynooth University	22 November 2024	€40,000	Reprimand re: Articles 5(1)(f), 32(1) and 33(1) GDPR. Order to bring processing into compliance with Article 32(1).
Meta Platforms Ireland Limited (Token Breaches – Art. 33)	12 December 2024	€11 million	Reprimand re: Article 33 of the GDPR.
Meta Platforms Ireland Limited (Token Breaches – Art. 25)	12 December 2024	€240 million	Reprimand re: Article 25 of the GDPR.

## Confirmation of Administrative Fines

When the DPC imposes a fine on a controller, that fine must be confirmed before the Courts. In 2024, the DPC imposed over **€652 million in administrative fines**. This included fines imposed on LinkedIn, Meta Platforms Ireland Limited, Sligo County Council and Maynooth University. All fines imposed by the DPC must be confirmed in Court before they are collected. Once collected, fines are remitted to the central exchequer in Ireland. In 2024, the DPC collected and remitted a total of €582,500 in administrative fines to the central exchequer in Ireland. This included an administrative fine of €22,500 on the Department of Health, which was confirmed in the Dublin Circuit Court in 2024.

**€652** million in administrative fines

---

## Domestic Decisions that concluded in 2024

---

---

### Mediahuis Ireland Group Ltd (formerly Irish News and Media plc)

The DPC issued the Final Decision in this inquiry in June 2024. This was a complaint-based inquiry in which the DPC evaluated the balance between the complainant's personal data rights and the rights of a media organisation to freedom of expression. The DPC concluded, after consideration of the facts and the submissions of the complainant and the data controller, that the exemption for freedom of expression provided for in section 43(1) of the 2018 Act applied. The DPC found no infringement and dismissed the complaint.

*Details of this decision can be found on page 38 of this report.*

---

### Sligo County Council

The DPC issued the Final Decision in this inquiry in November 2024. The Decision followed a data protection audit into the processing of personal data, by or on behalf of the Council, through the use of CCTV, automated number plate recognition systems and any other technologies that may be used to monitor individuals. The Decision found the Council infringed Articles 5(1)(a), 5(1)(c), 5(1)(e), 5(1)(f), 13, 24, 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, 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 processing personal data, including through CCTV cameras and an administrative fine in the amount of €29,500.

*Details of this decision can be found on page 39 of this report.*

---

### Maynooth University

The DPC issued the Final Decision in this inquiry in November 2024. The inquiry related 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.

*Details of this decision can be found on page 40 of this report.*

## Summary of DPC Decision Concerning Mediahuis Ireland Group Limited

In March 2021 the DPC received a complaint against Mediahuis Ireland Group Limited ("MIG"), the publisher of newspapers including the Sunday Independent, the Irish Independent and the Herald. The complainant alleged that MIG had breached her data protection rights by its processing of the complainant's personal data and special category personal data (specifically, data concerning her health). The complainant listed articles and videos published by MIG that discussed the complainant and her personal injury court action that she had commenced against a hotel. The complaint highlighted that these contained information that could have come only from court documents that were not publicly available and that had not yet been made public in a hearing in court. The complaint alleged breaches of provisions of the GDPR including the data protection principles (Article 5) and a lack of a lawful basis for processing (Article 6). The complainant also claimed that MIG had breached her rights to transparency by failing to give her information concerning its processing of her data when required (Article 14).

In response, MIG asserted that its right to freedom of expression and information for journalistic purposes, which is expressly protected by Article 85 of the GDPR and section 43 of the 2018 Act, provided a full answer to the complaint. MIG noted that section 43 of the 2018 Act exempts processing from certain provisions of the GDPR where it is undertaken in exercise of the right of freedom of expression and information. Based on this, it took the position that the DPC did not have power to inquire into the details and extent of MIG's coverage of the complainant's personal injuries case or related matters. The DPC did not accept that argument.

The DPC noted that the right to freedom of expression and information is not an absolute right, and the exemption under section 43 of the 2018 Act applies only to the extent that complying with the relevant provisions of the GDPR would be incompatible with exercising that right for (in this case) journalistic purposes. To determine whether the processing was covered by the exemption, the DPC had to assess its purpose and whether complying with the

relevant GDPR provisions would be incompatible with MIG exercising its freedom of expression right. The inquiry was an appropriate means of doing this. The DPC also made clear that the inquiry would not seek to uncover journalists' sources.

There was no dispute that MIG's exercise of its right to freedom of expression was for journalistic purposes, so the central issue was the compatibility of that exercise with the rights protected by the relevant provisions of the GDPR. Consistent with the approach taken by the European Court of Human Rights, the Court of Justice of the European Union and the Irish Courts, the DPC conducted a balancing exercise to assess MIG's right to freedom of expression against the competing data protection rights of the complainant.

The DPC considered submissions of the complainant and MIG, and its own examination of Irish, EU and European Court of Human Rights case law. The DPC concluded that to uphold the GDPR rights asserted by the complainant would restrict journalism in a way that would be detrimental to MIG's ability to report on matters of public interest, and to the public's right to be informed. The DPC took account of the broad nature of "the public interest" in relation to journalism, and to the complainant's public profile as an elected representative in a political party with a stated position on insurance costs and personal injury claims. While the information may have been sourced from documents intended to be used in court, this did not necessarily prevent reporting on them. The DPC found that section 43 applied to MIG's processing of the complainant's personal data, and that the complaint should therefore be dismissed under section 112(1)(b) of the 2018 Act. The Decision can be found on the DPC website at

[Inquiry concerning Mediahuis Ireland Group Limited \(MIG\) June 2024 QR 1](#)



QR 1

## Summary of DPC Decision Concerning Sligo County Council

On 13 November 2024, the DPC issued a Final Decision following an inquiry into certain processing of personal data by Sligo County Council. This inquiry was one of a number of own-volition inquiries into a broad range of issues pertaining to surveillance technologies deployed by State authorities. This inquiry sought to assess whether Sligo County Council was processing personal data in compliance with the GDPR and the Data Protection Act 2018. The inquiry examined a number of the Council's processing operations including its use of CCTV cameras in public places used for the purposes of prosecuting crime or other purposes. The findings made in the decision include:

- Findings that Sligo County Council lacked a valid legal basis for processing of personal data from CCTV and Automated Number Plate Recognition (ANPR) cameras.
- Findings that Sligo County Council failed to erect appropriately worded and located signage in respect of the processing of personal data collected via CCTV cameras.

The other findings in the decision include infringements relating to Sligo County Council's obligations to carry out data protection impact assessments, to maintain data logs for specific accesses to CCTV recordings, and to implement appropriate technical and organisational measures.

The corrective measures exercised by the DPC were as follows:

- 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 can 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
- An administrative fine of €29,500

The Decision can be found on the DPC website at [Inquiry into Sligo County Council - November 2024 QR 2](#)



QR 2



## Summary of DPC Decision Concerning Maynooth University

On 22 November 2024, the DPC made a Final Decision following an inquiry into a personal data breach in Maynooth University. The inquiry related a personal data breach notified by Maynooth University in November 2018. The breach affected the email accounts of university employees, and allowed unauthorised persons to gain control of up to six accounts. The unauthorised persons used control of one account to assist in perpetrating a fraud, leading to a financial loss by one of the persons affected. The subsequent investigation and actions by the University allowed that person to be reimbursed. The DPC assessed Maynooth University's technical and organisational measures for ensuring the security of personal data that it processed, and also examined compliance with the controller's obligation to notify breaches promptly.

The DPC's Decision found that Maynooth University:

- Infringed Articles 5(1)(f) and 32 of the GDPR by failing to ensure appropriate security personal data that it processed, and to implement appropriate technical and organisational measures to ensure such security; and
- Infringed Article 33(1) of the GDPR by failing to notify the DPC of the data breach within 72 hours.

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.

Maynooth University was ordered to complete:

- a. The implementation of multifactor authentication for all user accounts.
- b. A review of anti-spam configuration and policies, including regular review and updates as the risk landscape changes.
- c. Regular security updates of software.
- d. A robust password management policy including processes, methods and techniques for secure storing of user passwords.
- e. Mandatory data protection and cyber security training for all staff, appropriate to their role and level of risk, and updated as the risk landscape changes.
- f. Development of policies to respond to data breaches and data security incidents in ways that are appropriate to the risks posed and that ensure compliance with Maynooth University's obligations as a data controller under the GDPR.

The Decision can be found on the DPC website at [Inquiry into Maynooth University - November 2024 QR 3](#)



QR 3

---

## Domestic cases that reached a key investigative stage in 2024

---

---

### City of Dublin Education and Training Board (SUSI)

This own-volition inquiry commenced in 2019 after CDETB notified a personal data breach in which the personal data associated with website applications for student grants were made available to unauthorised persons.

CDETB operates a website (<https://www.susi.ie>) on which third-level students can find information relating to their eligibility for a higher education grant. Student Universal Support Ireland (SUSI) was created in 2012 as a business unit of CDETB (then known as the City of Dublin Vocational Education Committee) following CDETB's designation as the single awarding authority for new grants under the Student Support Act 2011. In November 2018, CDETB discovered that its web server was retaining personal data in the form of contact forms and uploaded documents. Prior to that discovery, the data controller had assumed that personal data being submitted through its website were being emailed to the relevant SUSI team and were not being retained locally on its web server. CDETB also detected malicious malware contained on its web server in October 2018.

The DPC commenced a statutory inquiry in July 2019. The DPC wrote to CDETB in March 2024, notifying CDETB of the commencement of the decision-making stage of the inquiry and provided CDETB with the Final Inquiry Report from the evidence gathering stage of the inquiry. The matter was ongoing at year's end.

---

### Department of Social Protection re SAFE/PSC Facial Matching

This own-volition inquiry considers whether certain processing of personal data by the Department of Social Protection, in the context of registering to obtain a Public Services Card, is compliant with the GDPR and with the Data Protection Act 2018. The DPC issued its Draft Decision in November 2023 and received submissions on it from the Department in February 2024. The matter was ongoing at year's end.

---


## Permanent TSB

The DPC commenced this inquiry following three separate breach notifications from Permanent TSB (PTSB) in May 2022. All three personal data breach notifications concern circumstances where a malicious actor attempted to gain access to a data subject's bank account by calling PTSB's Open 24 call centre. The inquiry is examining the organisational and technical measures implemented 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 provided a statement of issues to PTSB in January 2024 and received submissions from PTSB in February 2024. The matter was ongoing at year's end.

---

## Health Service Executive

In 2023, the Health Service Executive (HSE) notified the DPC of two occasions of personal data breaches concerning unauthorised access to physical medical records at two separate HSE facilities. In both instances, unauthorised third parties accessed storage facilities operated by the HSE, and published video footage on social media platforms of physical files stored at these facilities. In May 2024, the DPC commenced an own-volition inquiry into this matter. The inquiry is addressing the HSE's compliance with GDPR obligations concerning data protection governance, security of processing, communication of data breaches to data subjects, and the GDPR principles of storage limitation, integrity and confidentiality, and accountability.



---

## 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 2024

---

### Meta Platforms Ireland Limited (Meta): passwords stored in “plaintext”

The DPC adopted its Final Decision in this inquiry in September 2024. This inquiry examined whether Meta complied with its GDPR obligations in relation to personal data breaches and secure processing of user passwords. The inquiry was commenced in response to a breach of security identified by Meta in 2019, where user passwords were inadvertently stored in “plaintext” on Facebook’s internal systems (i.e. without cryptographic protection or encryption). The Decision found that Meta had infringed Articles 33(1) and 33(5) of the GDPR by failing to notify the DPC of a personal data breach and by failing to document the personal data breaches involving the storage of user passwords in plaintext. The Decision also found that Meta infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate measures to ensure the appropriate security of users’ passwords.

**The Decision included a reprimand and administrative fines totalling €91 million.**

*Details of this decision can be found on page 46 of this report.*

---

## LinkedIn Ireland Unlimited Company

The DPC adopted its Final Decision in this inquiry in October 2024. The inquiry assessed the lawfulness, fairness and transparency of LinkedIn's processing of the personal data of its EU/EEA members for the purposes of behavioural analysis and targeted advertising. The inquiry was commenced in August 2018 following the receipt of a complaint made by the French NGO, La Quadrature Du Net, on behalf of affected data subjects under the procedure provided for in Article 80(1) of the GDPR. The Final Decision found that LinkedIn infringed Articles 5(1)(a), 6(1), 13(1)(c) and 14(1)(c).

As a result of those infringements, the **Final Decision included a reprimand, an order to bring processing into compliance and administrative fines totalling €310 million.**

*Details of this decision can be found on page 47 of this report.*

---

## Meta Platforms Ireland Limited (Meta): Token Breach Article 33

This was one of two own-volition inquiries opened by the DPC in relation to a personal data breach reported by Meta Platforms Ireland Limited (then known as Facebook Ireland Ltd) in September 2018. The breach arose from the operation of user tokens on the Facebook platform, which had been exploited to allow unauthorised access to user accounts. **Approximately 29 million Facebook users globally were affected by this breach, of whom approximately 2.8 million were based in the EU/EEA.** This inquiry focused on compliance with the controller's obligation to notify personal data breaches to its supervisory authority and to provide relevant information in accordance with Article 33 of the GDPR. In its Decision, the DPC concluded that Meta had infringed Article 33(3)(a) and (c) of the GDPR, as well as Article 33(5) of the GDPR.

The DPC issued its Decision in December 2024, **reprimanding Meta and ordering it to pay administrative fines totalling €11 million.**

*Details of this decision can be found on page 48 of this report.*



## Meta Platforms Ireland Limited (Meta): Token Breach Data Protection by Design and Default

This was a second own-volition inquiry concerning the breach notified by Meta Platforms Ireland Limited in September 2018 concerning user tokens. The inquiry was commenced by the DPC in October 2018 and focused on the controller's obligation under Article 25 of the GDPR to ensure data protection by design and default. In its Decision issued on 12 December 2024, the DPC concluded that Meta had failed to implement appropriate technical and organisational measures and safeguards to ensure data protection and to protect data subject's rights, as required by Article 25(1) of the GDPR. The DPC also found that Meta had infringed Article 25(2) of the GDPR by not ensuring that, by default, only the minimum personal data are processed or made available to other persons without intervention by the data subject.

The DPC issued its Decision in 12 December 2024, **reprimanded Meta and imposed administrative fines totalling €240 million.**

*Details of this decision can be found on page 49 of this report.*



DPC Commissioners Des Hogan and Dale Sunderland along with Deputy Commissioners Graham Doyle and Gráinne Hawkes met with European Data Protection Supervisor (EDPS) Wojtek Wiewiorowski and Team.

## Summary of DPC Decision concerning Meta Platforms Ireland Limited (Meta): own volition inquiry concerning the storage of passwords in “plaintext”

On 21 March 2019, Meta Platforms Ireland Limited informed the DPC that it had inadvertently stored passwords of social media users in “plaintext” on its internal systems (i.e. without cryptographic protection or encryption). On being made aware of these incidents in January 2019, Meta had formed the view that the inadvertent logging of plaintext passwords did not constitute a personal data breach within the meaning of the GDPR. On 24 April 2019, the DPC commenced an own-volition inquiry in response to this issue.

In a Final Decision adopted in September 2024, the DPC made findings of infringement of the GDPR against Meta concerning its obligations in relation to personal data breaches, and concerning Meta’s obligations to implement measures to ensure secure processing of user passwords. The DPC was satisfied that the storage of passwords in “plaintext” in Meta’s internal systems constituted a personal data breach within the meaning of the GDPR. On this basis, the DPC found that Meta had infringed Article 33(1) of the GDPR by failing to notify the DPC without delay of a specific personal data breach **(concerning tens of millions of passwords of EU users)** which was discovered by Meta on 31 January 2019.

The DPC also found that Meta had infringed Article 33(5) of the GDPR, by failing to document two personal data breaches as discovered on 7 January 2019 and 31 January 2019.

Finally, the Decision found that Meta had infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate measures to ensure a level of security appropriate to the risk, including the ability to ensure the ongoing confidentiality of user passwords.

The DPC submitted a draft decision to the other Concerned Supervisory Authorities across the EU/EEA in June 2024, in accordance with Article 60 of the GDPR. **No relevant and reasoned objections to the draft decision were raised by the other authorities** and all EU/EEA regulators were therefore deemed to be in agreement with the decision of the DPC.

The Final Decision reprimanded Meta for the infringements of the GDPR, and **imposed administrative fines totalling €91 million**. This decision has been appealed by Meta.

The Decision can be found on the DPC website at [Inquiry into Meta Platforms Ireland Limited - September 2024](#) **QR4**



QR 4

## Summary of DPC Decision concerning LinkedIn Ireland Unlimited Company: lawfulness, fairness and transparency of the processing of user data for behavioural analysis and targeted advertising

In October 2024, the DPC adopted its Final Decision finding that LinkedIn infringed Articles 5(1)(a), 6(1), 13(1)(c) and 14(1)(c) of the GDPR. The Decision concerned the lawfulness, fairness and transparency of the processing of the data of members of the LinkedIn platform for the purposes of behavioural analysis and targeted advertising. The processing of personal data for these purposes encompassed personal data provided directly to LinkedIn by its members (first-party data) and personal data relating to its members obtained by LinkedIn via third party partners (third-party data). The processing additionally included the development of aggregated analytics reports by LinkedIn, based on data received from third party partners via a tracking pixel combined with first party data. These analytics reports were provided by LinkedIn to third party partners to enable them to more effectively target LinkedIn members.

The Decision followed a complaint-based inquiry, which was commenced on 20 August 2018, following a complaint made by the French non-profit organisation, La Quadrature Du Net. The complaint was initially made to the French Data Protection Authority, and thereafter provided to the DPC, in its role as the lead supervisory authority for LinkedIn. The DPC submitted a draft decision to the other Concerned Supervisory Authorities across the EU/EEA in July 2024. **No relevant and reasoned objections to the draft decision of the DPC were received** and all EU/EEA regulators were therefore deemed to be in agreement with the decision of the DPC.

The Final Decision recorded a number of findings of infringement of the GDPR. First, the DPC concluded that LinkedIn did not validly rely on Article 6(1)(a) of the GDPR (consent) to process the third party data of its members for the purpose of behavioural analysis and targeted advertising on the basis that the **consent obtained by LinkedIn was not freely given, sufficiently informed or specific, or unambiguous**. Second, the DPC determined that LinkedIn did not validly rely on 6(1)(b) of the GDPR (contractual necessity) or Article 6(1)(f) of the GDPR (legitimate interests) to process the first party personal data of its members for behavioural analysis and targeted advertising. Third, the DPC determined that LinkedIn did not validly rely on the legitimate interest legal basis to process third party personal data of its members for analytics.

The DPC additionally concluded that LinkedIn's processing of personal data for behavioural analysis and targeted advertising was not conducted in a fair manner, and that LinkedIn **did not meet its transparency obligations** in respect of the information it provided to data subjects regarding its reliance on Article 6(1)(a), Article 6(1)(b) and Article 6(1)(f) of the GDPR as lawful bases. The DPC concluded that this failure to provide sufficient transparency information, combined with **a number of unfair practices, was misleading and impacted the autonomy of users to exercise control over their personal data**.

The DPC imposed **administrative fines totalling €310 million** on LinkedIn in respect of the infringements identified in the Final Decision. Furthermore, the DPC imposed a reprimand on LinkedIn and made an order that it bring its processing into compliance with the GDPR within a period of months. LinkedIn has appealed this decision.

The Decision can be found on the DPC website at [Inquiry into LinkedIn Ireland Unlimited Company - October 2024 QR5](#)



QR 5

<sup>4</sup> La Commission Nationale de l'Informatique et des Libertés ("CNIL").

## Summary of DPC Decisions Concerning Token Breach by Meta Platforms Ireland Limited (Meta)

The DPC opened these two joined inquiries in October 2018 in response to a personal data breach that Meta Platforms Ireland Limited (then called Facebook Platforms Ireland Limited) (Meta) notified to the DPC on 28 September 2018.

The breach arose from the use of user tokens in certain features of the Facebook platform. User tokens are codes that can be used to identify a particular user during an online session, to give them access to data at appropriate levels of security and to control the features to which the user has access.

The breach involved tokens generated by a Facebook feature called “View As”, which allowed a user to see their own page as other users would see it. Using this with two other Facebook features – the “Happy Birthday composer” and Facebook’s video uploader service – allowed unauthorised persons to obtain user tokens identifying themselves as other Facebook users. Using those tokens, the unauthorised persons could access personal data on or through the Facebook platform as if they were the users identified by those tokens. Meta’s US parent company, Facebook, Inc. (now Meta Platforms Inc.) identified an anomalous increase in activity linked to its video uploading service and determined that this was caused by unauthorised persons using the features mentioned above to generate user tokens. The DPC was notified of this by email early on the morning of 28 September 2018.

Meta’s investigations determined that the vulnerability arose from a new video uploading function introduced in July 2017. Meta engineers patched and resolved the vulnerability on 28 September 2018.

The first inquiry examined Meta’s compliance with Article 33 of the GDPR, which requires controllers to notify breaches to their supervisory authority. The DPC found that Meta had notified the breach promptly and within the 72 hours prescribed by Article 33(1). However, the DPC determined that Meta had not provided all information required for compliance with Article 33(3). The notification was insufficient in relation to identifying the cause of the breach, its nature and likely consequences, the categories of data subjects affected and type of personal data records affected. The DPC submitted a draft decision to the other Concerned Supervisory Authorities across the EU/EEA in September 2024, in accordance with Article 60 of the GDPR. **No relevant and reasoned objections to the draft decision of the DPC were received** and all EU/ EEA regulators were therefore deemed to be in agreement with the decision of the DPC.

In the Final Decision dated 12 December 2024, the DPC determined that Meta was not in a position at the time of notifying to provide certain other information required under Article 33(3) of the GDPR to be provided “where possible”, and so found no infringement in that regard. Finally, the DPC determined that Meta had not maintained internal documentation of the breach to the standard required by Article 33(5) of the GDPR. The DPC issued a **reprimand to Meta and ordered it to pay an administrative fine of €8 million** for its infringement of Article 33(3) of the GDPR and of **€3 million** for its infringement of Article 33(5) of the GDPR.

In the second inquiry, the DPC examined Meta's compliance with Article 25 of the GDPR, which requires data protection by design and default. The DPC submitted a draft decision to the other Concerned Supervisory Authorities across the EU/EEA in September 2024, in accordance with Article 60 of the GDPR. **The other authorities raised no relevant and reasoned objections to the draft decision** and were therefore deemed to be in agreement with the decision of the DPC.

In the Final Decision dated 12 December 2024, the DPC found that the unauthorised persons' use of compromised access tokens had resulted from Meta's failure to implement measures to ensure that its processing provided appropriate security of personal data as required by the integrity and confidentiality principle set out in Article 5(1) (f) of the GDPR. As a result, the DPC found that Meta had infringed Article 25(1) of the GDPR, which requires such measures in both the design and operation of processing. Article 25(2) of the GDPR requires that, by default, only personal data necessary for each specific purpose of

the processing are processed, and that controllers must implement appropriate technical and organisational measures to ensure this. The DPC found that the Meta design decisions relating to generation of the user tokens exploited in this breach allowed those tokens to have an unduly wide range of access, rather than being restricted to the limited functions for which they were intended to be used. The DPC therefore found that Meta had infringed Article 25(2).

In the second inquiry, **the DPC reprimanded Meta and imposed an administrative fine of €130 million** for the infringement of Article 25(1) of the GDPR, and **€110 million in respect of the infringement of Article 25(2) of the GDPR.**

Further information on this Decision can be found on the DPC website at

[Irish Data Protection Commission fines Meta €251 Million - December 2024](#) **QR6**



QR 6

---

Cases which commenced or where submissions on a Draft Decision, Preliminary Draft Decision or a Statement of Issues were invited from the relevant parties during 2024

---

### **MTCH Technology Services Limited** (MTCH) and the Tinder service

This own-volition inquiry concerns MTCH's compliance with the right of data subjects to access their data under Article 15 of the GDPR and the right to erasure under Article 17 of the GDPR. Specifically, the inquiry examines whether MTCH is in compliance with its obligations concerning data subject access requests, and whether MTCH's processing of users' personal data in the context of data erasure requests is in compliance with the principles and obligations of the GDPR. Submissions were received from MTCH in response to the Preliminary Draft Decision. The matter was ongoing at year's end.

---

### **Meta Platforms Ireland Limited (Meta):** behavioural analysis and targeted advertising

This inquiry concerns a complaint in relation to the lawfulness of the processing of personal data of users of the Facebook service for behavioural analysis and targeted advertising. The complaint in question was lodged by a French digital advocacy organisation, La Quadrature du Net with the French Data Protection Authority, through Article 80 of the GDPR whereby a data subject can mandate a not-for-profit body to lodge a complaint and act on his/her behalf. The DPC completed its final inquiry report in July 2024. It received additional submissions from the data controller in August 2024. The matter was ongoing at year's end.





---

## Google PaLM2 AI inquiry

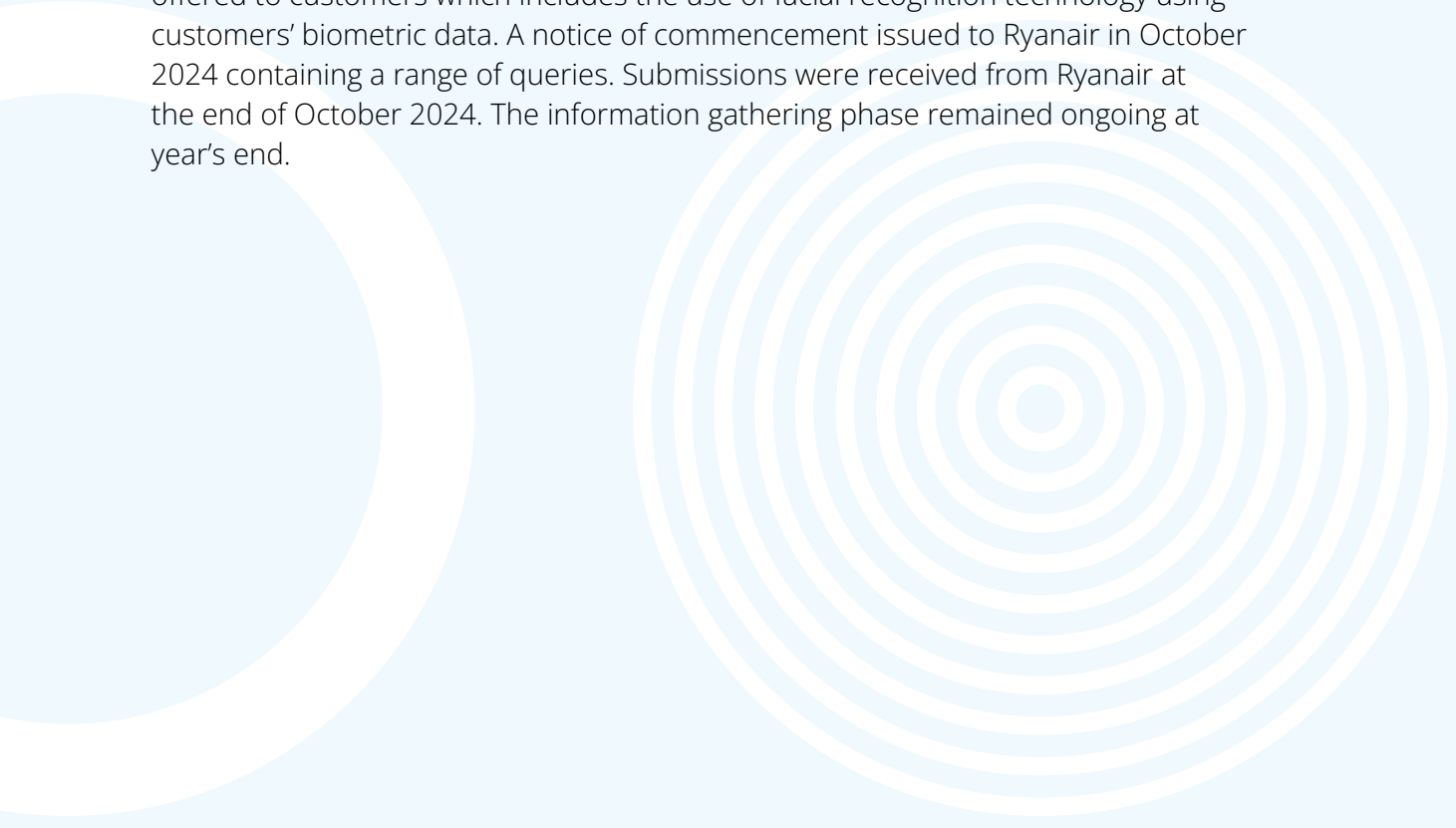
This is an own-volition inquiry commenced by the DPC in September 2024 relating to Google's processing of the personal data of EU/EEA data subjects associated with the development of its foundational AI model, Pathways Language Model 2 (PaLM2). The inquiry concerns whether Google complied with any obligations that it had to undertake a data protection impact assessment, pursuant to Article 35 of the GDPR, prior to engaging the personal data processing. A notice of commencement issued to Google in September 2024 containing a range of queries. Submissions were received from Google in October 2024. The information gathering phase remained ongoing at year's end.

---

## Ryanair DAC inquiry

This is an own-volition inquiry commenced by the DPC in October 2024 relating to Ryanair's processing of personal data (biometric data) as part of the Customer Verification Processes for customers who book Ryanair flights from third party websites or Online Travel Agents.

The inquiry concerns Ryanair's practice of requesting additional ID verification from customers who book travel tickets via third party websites, as opposed to booking directly on Ryanair's website. The DPC had received a number of complaints from Ryanair customers across the EU/EEA regarding the verification methods being offered to customers which includes the use of facial recognition technology using customers' biometric data. A notice of commencement issued to Ryanair in October 2024 containing a range of queries. Submissions were received from Ryanair at the end of October 2024. The information gathering phase remained ongoing at year's end.



---

## Cases involving **individual complainants** concluded by DPC through EU Co-Operation procedure in 2024

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 2024, the DPC **concluded 115 such cases**. Details of these cases can be found published on the EDPB Article 60 case register. In addition, the DPC also **concluded four (4) decisions concerning cross-border complaints** in 2024.

---

## Complaint-based cross-border decisions that concluded in 2024

---

### Airbnb Ireland UC: Lawful processing of personal data for identity verification

This inquiry, commenced in December 2022, concerns a complaint in relation to the lawful processing of personal data for the purpose of identity verification and the principle of data minimisation.

An individual contended that Airbnb had unlawfully requested a copy of their identity document in order to verify their identity to carry out an erasure request after they had discontinued with the Airbnb registration process. The individual also alleged that during the course of registration with the Airbnb platform, Airbnb had sought a copy of their identity to complete the registration process. The individual provided Airbnb with their email address and phone number.

The individual requested Airbnb erase all of their personal data and ensure that no data was transferred to third parties, however in response Airbnb sought a copy of the individual's ID to verify their identity in order to carry out the erasure request and then further clarified they were seeking a copy of a Government issues identity document. The individual considered that this requirement did not have any legal basis and that it was an infringement of their right to erasure of their personal data. Ultimately, Airbnb authenticated the individual's identity through account login and the erasure request was processed.

The scope of the inquiry included whether Airbnb had a lawful basis for requesting a copy of the complainant's ID in order to verify their identity so that they could delete this account; whether the request for this information infringed the principle of data minimisation; and whether the principle of transparency and provision of certain information at the point the person data were collected were complied with. No relevant and reasoned objections were received from concerned supervisory authorities following submission of the DPC's draft Decision to the co-operation mechanism provided by Article 60 of the GDPR. The Decision of January 2024 found that the legitimate interest relied upon by Airbnb as the legal basis for the processing of the individual's ID under Article 6(1)(f) of the GDPR (including to verify the authenticity of the request and to ensure user accounts are not deleted inappropriately), did not constitute a valid legal basis. While the DPC recognised the existence of these interests, it found that in the circumstance of this inquiry, Airbnb had not demonstrated that its request for the complaint's ID was necessary or proportionate for the completion of the erasure request and could be achieved through other means such as account login.

The DPC also found that Airbnb's requirement that the complainant verify their identity by submitting a copy of their ID in order to make an erasure request constituted an

infringement of the principle of data minimisation, pursuant to Article 5(1)(c) of the GDPR. The DPC was satisfied that Airbnb complied with the principle of transparency and provision of information under Article 13(1) of the GDPR. The DPC issued a reprimand in light of the infringements identified in accordance with its powers under Article 58(2)(b) of the GDPR.

Airbnb subsequently discontinued the practice of requesting a copy of ID in order to verify erasure requests. In addition, following an order made in a previous DPC decision Airbnb confirmed to the DPC that it has revised its internal policies and procedures to only request a user provide ID where less privacy intrusive verification methods are not available to prevent further infringements of Article 5(1)(c) of the GDPR occurring to data subjects in the future similar to those that occurred in this instance.

---

## Apple Distribution International Limited: Lawfulness of retaining personal data following an erasure request

This inquiry, commenced in November 2022, concerns a complaint that an erasure request in respect of a user's Apple ID was not properly complied with, and the contention that Apple unlawfully retained the individual's email address associated with their Apple ID. This inquiry examined the legal basis on which Apple relied to retain the hashed value of the individual user's email address following action taken by Apple to give effect to the erasure request.

No relevant and reasoned objections were received from concerned supervisory authorities following submission of the DPC's draft Decision to the co-operation mechanism provided by Article 60 of the GDPR. The DPC's Decision issued in March 2024 found that Apple was and is entitled to validly rely on the "legitimate interest" legal basis for processing under Article 6(1)(f) of the GDPR for the purpose of retaining a hashed value of the user's email address following the erasure request, including in order to prevent the recycling of namespaces by users, and to protect its users against fraud and security breaches by third parties. The DPC was satisfied that Apple's reliance on the "legitimate interest" legal basis did not amount to a contravention of Article 6 of the GDPR, and further that Apple had complied with the user's erasure request and that it had not infringed Articles 12 and 17 of the GDPR. However, the Decision did identify transparency infringements and determined that Apple had infringed Articles 13(1)(c) and 13(1)(d) of the GDPR in failing to inform the user of its intention to retain the hashed value of their email address and of the lawful basis and legitimate interests for doing so.

The DPC issued a reprimand in light of the infringements found, ordering Apple to address the transparency deficiencies for users in the document entitled "Apple ID Deletion Terms and Conditions" by early June 2024. It also ordered Apple to provide details of the completion of the project it was carrying out a review of the retention period for the deletion of users' hashed email addresses by 31 December 2024. Apple duly confirmed completion of that project in December 2024.

---

This case illustrates how a DPC complaint based inquiry found that a data controller seeking to give effect to an individual's GDPR rights failed to do so. The DPC's intervention and engagement resulted in an order for the controller to revise its terms to ensure transparency and provision of information to users, and ensured time limits for erasure or a periodic review are in place.

## Apple Distribution International Limited: Access Request for Personal Data held on a locked account

This inquiry commenced in February 2023 in relation to an access request sent to Apple looking to obtain data on a cloud-based account on the controller's services. The complainant claimed Apple had ignored their request and they logged a complaint with the DPC.

As part of the engagement process, Apple stated that it had responded to the complainant's access request without delay and Apple's teams had attempted to assist the complainant to verify their entitlement to obtain access to the cloud account. As the complainant was not able to progress through the security steps required to access the account, Apple did not provide any personal data to the complainant.

Apple outlined that it had provided the complainant with information in compliance with Article 15(1) and Article 15(2) of the GDPR by directing the complainant to its relevant policies.

In relation to the "locked out" account, with which the complainant claimed their personal data was associated, Apple said it had an established process for ensuring account security and for verifying entitlement to access data associated with a unique account username. Apple considered that this allowed them to satisfy the requirement for controllers to both confirm the identity of natural persons in the circumstances set out in Article 12(6) of the GDPR, and to fulfil their security obligations under Article 32 of the GDPR.

In this case, the complainant was unable to access emails associated with an address connected to the cloud account. Additionally, the complainant did not have a rescue email address that could be used to assist with account recovery. The individual had provided Apple with identity and other documentation, which they believed were sufficient to verify their entitlement to access the data on the account. However, Apple stated it did not require copies of an ID card or other official documentation during the registration process for an account in order to verify that the name or date of birth had been provided truthfully, or that the person resided at the address provided by them. This was due to the fact that Apple, in this context, was not seeking to verify the identity of a customer but solely to associate certain data to a specific customer using a registered username. Apple's position was that the account had most likely been locked out as a result of the inputting of incorrect security credentials. Asserting that without being confident that a person was the account owner, they could not proceed with an access request or to facilitate other data protection rights.

Apple stated that its security process would be weakened if any person could access an account without having access to the email address associated with it or having the ability to answer basic security questions. Apple maintained that allowing access in such circumstances would mean providing access to the personal data on an account based on a claim of one person, without a clear means of verifying that the request was not malicious.

Apple considered that, in the specific circumstances, adopting a cautious approach to providing access to an account was fully warranted and, in fact, expected under the GDPR.

Based on the information provided during the inquiry, the DPC was satisfied that Apple complied with Article 12(4) of the GDPR in relation to their response to the access request. The DPC was also satisfied that Apple had complied with the requirements of Article 15(1) and Article 15(2) in relation to the information provided to the complainant.

In relation to the requirement of Article 15(3) to provide a copy of personal data undergoing processing, the DPC was satisfied that the only means by which Apple could have provided this to the complainant was for the complainant to access it themselves using the security credentials provided when the account was set up. As these credentials remained unavailable to the complainant, the only other means available would have been for Apple to break their own security requirements in order to access data.

The DPC found in its decision in February 2024 that Apple's handling of the access request was compliant with the requirements of Article 12 and Article 15 of the GDPR and with the Data Protection Act 2018. The DPC's Draft Decision had been submitted to the other Supervisory Authorities as part of the Article 60 process and no relevant and reasoned objections were received.

The case illustrates an example that in certain cases, where an individual is unable to provide the required security credentials in order to demonstrate their entitlement to access data stored in a cloud service, that the controller is not under an obligation to infringe other requirements of the GDPR, such as the security provisions, in order to allow access to an account under an access request pursuant to Article 15 of the GDPR.

## Summary of DPC Decision Concerning Groupon Ireland Operations Limited (Groupon).

The DPC received a complaint via the Baden-Württemberg German Supervisory Authority in which the complainant alleged they had unsuccessfully tried to submit a subject access and erasure request with Groupon using the advertised processes on the Groupon website. Having made contact with the company, the complainant was directed to a portal where they could submit their request. In response to the request, Groupon requested the complainant to provide a copy of an ID document in order to verify their identity, which the complainant objected to. Groupon later changed their ID requirements in October 2018 and invited the complainant to submit a new request to enable Groupon to process the request with their new procedures. However, the complainant remained dissatisfied that all of their personal data had subsequently been fully deleted in accordance with their erasure request.

The DPC examined the complaint in order to determine if (i) Groupon's request for ID in order to verify the identity of the complainant for the purposes of their original access and erasure requests was compliant with Groupon's relevant obligations under the GDPR; and (ii) whether Groupon had appropriately demonstrated that the complainant's personal data had been fully deleted in response to their erasure request.

The DPC carried out an examination of Groupon's databases to further test Groupon's evidence as to the full erasure of the Complainant's personal data. During this exercise, the DPC verified that the Complainant's personal data were not returned in relation to a number of queries entered into Groupon's databases.

The DPC submitted its draft decision to fellow concerned supervisory authorities through the co-operation mechanism provided by Article 60 of the GDPR. Having received no relevant and reasoned objections to the draft decision, all EU/EEA regulators were therefore deemed to be in agreement with the decision of the DPC.

In relation to Article 5(1)(c) for the personal data gathered to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation) the DPC found that Groupon had infringed Article 5(1)(c) by having initially required the complainant to provide a copy of their ID in order to verify their identity for the purposes of their access and erasure requests, in circumstances where no such verification appeared to have been obtained or required in order to initially open an account and a less data-driven means of verification (namely, by way of the email address associated with the account) was available to Groupon.

The DPC found that Groupon infringed Article 12(2) of the GDPR by initially requesting additional information as to the complainant's identity at the time they made their access and erasure requests, in circumstances where it has not demonstrated that reasonable doubts existed concerning the complainant's identity that would have necessitated that application of Article 12(6) of the GDPR.

In addition, the DPC found that Groupon infringed Articles 15(1), 15(3) and 17(1) of the GDPR by having failed to comply with the complainant's initial access and erasure requests at the time they were made without a lawful basis for not complying, in circumstances where Groupon's request (as a prerequisite to responding to the initial access and erasure requests) for photographic ID has been found to be an infringement of Article 5(1)(c) of the GDPR.

Articles 6(1) of the GDPR relates to the lawfulness of processing. The DPC found that Groupon infringed Article 6(1) of the GDPR by continuing to process the complainant's personal data after they received the data subject's request for erasure of their personal data.

The DPC's decision found no infringement in relation to whether Groupon had appropriately demonstrated that the complainant's personal data had been fully deleted in response to the erasure request.

The final decision was adopted on 8 March 2024. That final decision noted that Groupon no longer requires photographic ID in order to verify a data subject's identity for the purposes of exercising their data subject rights under GDPR, but also issued a reprimand to Groupon in light of the infringements found under point (i).

---

## Enforcement of Corrective Powers exercised by the DPC

---

### An Garda Síochána

A December 2022 decision under the Law Enforcement Directive transposition in the Data Protection Act 2018 required An Garda Síochána to implement appropriate technical and organisational measures with regard to the security of physical Intelligence Bulletin Boards throughout the network of Garda stations. The decision arose on foot of an inquiry that was commenced after a data breach in which an electrical contractor had been given unsupervised access to a Garda station and had posted images of the Intelligence Bulletin Board onto social media. The personal data disclosed

in that data breach included information about criminal convictions, suspicions of criminality and relationships between persons of interest to An Garda Síochána.

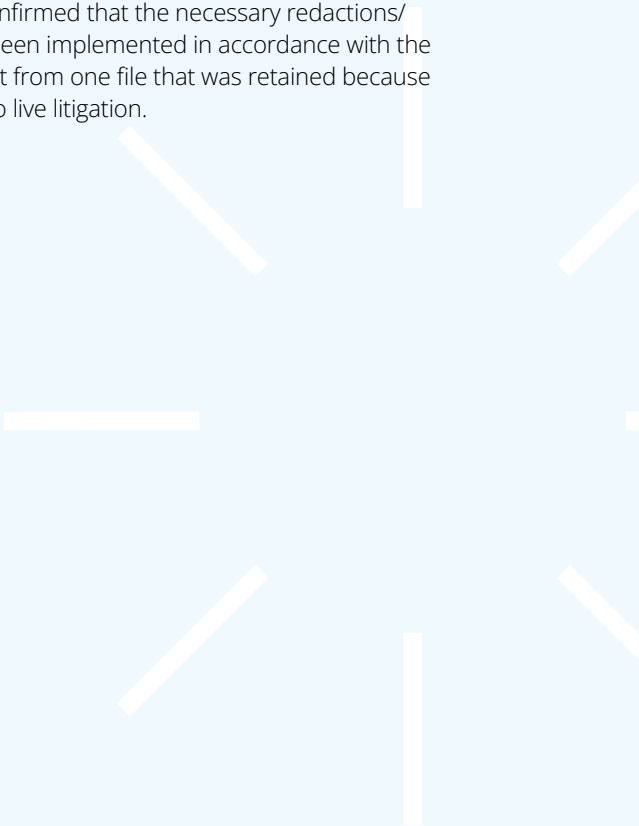
In response to the decision, AGS revised its access policies and all physical Intelligence Bulletin Boards were fully decommissioned by May 2024.

---

### Department of Health

The DPC issued a Final Decision to the Department of Health in June 2023 following an inquiry into the Department's processing of personal data in 29 litigation files related to claims from data subjects with special educational needs. It made findings of infringement of Article 5(1)(c) (data minimisation), 6(1), 6(4) and 9(2) of the GDPR (lawful basis and conditions for processing special category data), 14 (transparency), and 5(1)(f) and 32(1) of the GDPR (security of data processing). The corrective measures included a ban on processing certain categories of records, a fine of €22,500, and a reprimand.

The administrative fine was confirmed by the court and the fine was paid in August 2024. In December 2024 the Department confirmed that the necessary redactions/removals had been implemented in accordance with the Decision – apart from one file that was retained because it was subject to live litigation.





## Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited) (Meta): processing of children's data via the Instagram service operated by Facebook

In September 2022, the DPC adopted a Final Decision regarding processing of children's personal data on the Instagram service, finding that Meta infringed Articles 6(1), 5(1)(a), 5(1)(c), 12(1), 24, 25(1), 25(2) and 35(1) of the GDPR. The Final Decision imposed administrative fines totalling €405 million on Meta and also imposed a reprimand and an order requiring Meta to bring its processing into compliance by taking a range of specified remedial actions. Meta brought legal proceedings to appeal the DPC Decision.

Meta provided the DPC with a Compliance Report in December 2022, setting out relevant changes to its processing. The DPC circulated this Compliance Report to the other Supervisory Authorities concerned, for their consideration.

Having examined the actions outlined in Meta's Compliance Report, the DPC was not satisfied with the nature and extent of the measures adopted in relation to existing users:

- The DPC highlighted that although Meta had now introduced an option to select a "public" or "private" audience setting when registering for Instagram, this improvement only applied to new users, and not to people who had registered previously; and
- The DPC also highlighted that persons under the age of 18 years using "Business Accounts" on Instagram were given the option to publish their phone and/or email contact information as part of their profile. The DPC was not satisfied that Meta had demonstrated measures to reduce the risk resulting from this feature.

As a result of further engagement with the DPC, Meta implemented further changes in December 2023:

- Meta required all users under 18 years of age to choose either a "public" or "private" account setting; and
- Meta removed the option for users under 18 years of age to publish their off-Instagram contact information.

Having consulted the other Supervisory Authorities concerned on the DPC's assessment of the measures adopted by Meta to comply with the order, the DPC concluded the enforcement of the Decision in December 2024.

## TikTok Technology Limited (TikTok): processing of children's data via the TikTok service

In September 2023, the DPC adopted a Final Decision regarding processing of children's personal data on the TikTok service, finding that TikTok infringed Articles 5(1)(a), 5(1)(c), 5(1)(f), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) of the GDPR. The Final Decision imposed administrative fines totalling €345 million on TikTok and also imposed a reprimand and an order requiring TikTok to bring its processing into compliance by taking a range of specified remedial actions. TikTok brought legal proceedings to appeal the DPC Decision.

TikTok provided the DPC with a Compliance Report in December 2023, setting out relevant changes to its processing. The DPC circulated this Compliance Report

to the other Supervisory Authorities concerned, for their consideration.

Having examined TikTok's Compliance Report, the DPC was not satisfied with the nature and extent of the measures adopted. The DPC highlighted to TikTok that the service improvements did not apply to users aged 16 and 17 years who registered before changes were implemented.

As a result of this further engagement with the DPC, TikTok implemented additional improvements in January 2024, requiring all child users aged 16 or 17 years to choose either a "public" or "private" account setting.

## Meta Platforms Ireland Limited (Meta): Behavioural Advertising on the Instagram and Facebook services

Throughout 2023 and 2024, the DPC supervised compliance with two orders made in December 2022 regarding the Facebook and Instagram services. Those orders related to findings made by the DPC that Meta could not rely on Article 6(1)(b) of the GDPR to process personal data for the purposes of behavioural advertising. The DPC's supervision of this compliance has involved assessing Meta's subsequent reliance on the legitimate interests lawful basis under Article 6(1)(f) of the GDPR, and more recently, its reliance on the consent lawful basis under Article 6(1)(a) of the GDPR. In November 2023, Meta launched a new consent model in

which users were offered a choice between subscribing to receive Facebook and Instagram services without ads, or alternatively, agreeing to receive personalised and non-personalised ads to use the services without paying a fee.

In November 2024, Meta announced that it will offer people in the EU an additional new choice to use Facebook and Instagram for free with fewer personalised ads. At year's end, the DPC continued to assess this matter in light of the updated model.

## Galway County Council: surveillance technologies deployed by local authority

The DPC adopted a final decision in this inquiry in August 2023. The decision followed a data protection audit, which examined a range of issues including CCTV systems, APRN technology, and body worn cameras. The decision found infringements in relation to sections 70, 71, 72, 75, 78, 82 and 84 of the Data Protection Act 2018 and Articles 5(1)(a), 24(1) and 35(1) of the GDPR. The DPC ordered the Council to bring its processing into compliance by ceasing unlawful processing via CCTV, erecting properly worded signage and implementing appropriate technical and organisational measures to bring processing into compliance. The DPC subsequently received a

report from the Council outlining the actions that it had taken to comply with the corrective measures.

In order to ensure that the orders contained in the final decision had been fully complied with, the DPC conducted an on-site inspection in February 2024. The DPC was able to verify that the Council had implemented the measures outlined in its compliance report, such as removing unlawful CCTV and erecting appropriate signage. Accordingly, the DPC was satisfied that the Council had brought its processing operations into compliance with the final decision.

---

# 5

---

## Litigation



# Litigation

## Judgments Delivered and Final Orders made in 2024

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
1	High Court Record No. 2023/88 MCA	Julian de Spáinn v An Coimisiún Um Chosaint Sonraí	Statutory Appeal High Court	Judgment of the High Court delivered on 31 January 2024  Order of the High Court 11 March 2024 (as amended on 11 September 2024)	Proceedings concluded

### Outcome:

In response to a Motion brought by the DPC, the High Court made an order annulling two decisions of the DPC and remitting the underlying complaints to the DPC for fresh consideration on their merits.

The proceedings arose from complaints made by Mr de Spáinn against Bank of Ireland and Aer Lingus alleging that, by refusing to apply diacritical marks (specifically the síneadh fada) to his name and address as it appeared in the data controllers’ IT systems, the controllers had breached Mr de Spáinn’s right to rectification under Article 16 of the GDPR.

The complaints were resolved in favour of the data controller, following which an appeal was brought by Mr de Spáinn.

The DPC indicated its willingness to re-examine the complaints afresh and on application from the DPC, the Court acceded to that proposal.



No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
2	High Court Record No. 2022 1823P	Gray, Meegan, Mullan, Mullins, Geary & Scanlan v Data Protection Commission, Ireland & The Attorney General, Grant Thornton (A Firm) and Grant Thornton Corporate Finance Limited	Plenary Proceedings  High Court	Judgment of the High Court delivered on 21 March 2024  Order of the High Court dated 21 March 2024	Proceedings concluded

**Outcome:**

For the reasons set out in a judgment delivered on 21 March 2024 (Stack J), the High Court struck out the proceedings on the basis that they were frivolous and vexatious, had no reasonable prospect of success, and were bound to fail.

The proceedings had their origin in a data breach in which the personal data of a number of individuals was released by Grant Thornton to a third party. That data breach gave rise to a multiplicity of proceedings.

The High Court found that the issues raised in these proceedings had already been decided in earlier

proceedings, or was the subject of further proceedings that had not yet been decided. For that reason, the Court ruled that these proceedings were at least in part an abuse of process.

The proceedings were therefore struck out [and the Court ordered that certain of the plaintiffs who had been involved in the hearing, namely the first, second, third and fifth defendants, should pay the DPC’s costs]. The plaintiffs applied for leave to appeal against the High Court’s judgment directly to the Supreme Court. That application was refused by a determination of that Court made on 3 September 2024.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
3	High Court Record No. 2022/283JR	Peter Nowak v Courts Service & Data Protection Commission (Notice Party)	Judicial Review  High Court	Judgment of the High Court delivered on 20 March 2024	Proceedings concluded

Outcome:

By Orders made on 23 November 2021, the Circuit Court dismissed four separate appeals brought by Mr Nowak against decisions of the DPC. Subsequently, Mr Nowak sought to appeal the Circuit Court Orders. To that end, Notices of Appeal were delivered to the High Court Central Office. In the event, the Central Office declined to accept the Notices of Appeal on the grounds that they were out of time. In response, Mr Nowak brought Judicial Review proceedings against the Courts Service (naming the DPC as a Notice Party), contesting the Central Office's refusal to accept his Notices of Appeal.

By written Judgment delivered on 20 March 2024, the High Court (O'Donnell J) refused to extend time for the filing of the appeals (noting that Mr Nowak had failed/refused to ask the Court to extend time, and there being no other evidential basis on which to do so).

Costs were ordered against Mr Nowak.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
4	Court of Appeal Record No. 2024/113	Peter Nowak v Courts Service & Data Protection Commission (Notice Party)	Appeal of High Court Judgment (in relation to the JR listed at Entry #3 above)  Court of Appeal	Judgment, 8 November 2024	Proceedings concluded

Outcome:

By written judgement delivered on 8 November 2024, the Court of Appeal dismissed the appeal by Mr Nowak and a Judgment and Order of the High Court in which that Court had refused to extend the time for the filing of appeals by Mr Nowak against a series of decisions made by the DPC in response to complaints it had received from Mr Nowak. (See Entry #3 above).

The Court awarded costs against Mr Nowak.



No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
5	Court of Appeal Record No. 2023/280	David Fox v Data Protection Commission	Appeal from the High Court  Court of Appeal	Judgment of the Court of Appeal delivered on 25 April 2024	Proceedings concluded

**Outcome:**

On 14 November 2019, the DPC delivered a decision in relation to a complaint made by Mr Fox against the National Gallery of Ireland. Of the 7 points raised by Mr Fox in his complaint, 4 were upheld by the DPC and 3 were rejected.

Mr Fox subsequently brought an appeal against the DPC’s decision to reject 3 of the points canvassed in his complaint.

In a written Judgment delivered on 25 April 2022, the Circuit Court rejected the appeal, finding that, taking the adjudicative process as a whole, the DPC had fully and fairly considered all elements of the complaint and had come to a determination that was logical and appropriate bearing in mind the law in this area.

Mr Fox next brought an appeal (on a point of law) against the Judgment and Order of the Circuit Court. In its judgment of 25 September 2023, the High Court dismissed that appeal, noting that Mr Fox had failed to identify any point of law and so the High Court had no jurisdiction. The High Court separately found that the points Mr Fox had sought to raise on appeal amounted to (i) an attempt to re-run the process that had taken place before the DPC, and (ii) an invitation to the court to reach a different decision based on bare assertions which were unsupported by any evidence.

By written judgment delivered on 25 April 2024, the Court of Appeal dismissed Mr Fox’s further appeal from the Judgment of the High Court. The Court held that as the appellant’s notice of appeal made no reference to the first, and fundamental, determination of the High Court that it had no jurisdiction to entertain the appellant’s appeal (because the notice of motion identified no point of law), this appeal must also fail. However, the Court went on to consider the points raised by the Appellant, having noted that this was not a case in which defects in the Notice of Appeal could have been saved by an amendment to that document. This was because it would have been difficult, if not impossible, to reframe any of the grounds pleaded by the appellant, or even those raised in submissions, as points of law. The Court held that, at its simplest, the Appellant simply disagreed with the DPC’s decision and wanted the Court to put itself in the position of the DPC and to consider the DPC’s afresh and on its merits. Such an appeal was not open to the Appellant.

Costs were awarded to the DPC.

The Appellant next applied for leave to appeal to the Supreme Court. This was refused by way of a Supreme Court determination dated 19 July 2024.



No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
6	High Court Record No. 2022 339/ MCA	Meta Platforms Ireland Ltd v Data Protection Commission	Application for a stay  High Court	Judgment dated 10 May 2024  Order dated 30 May 2024	The DPC appealed the High Court's judgment to the Court of Appeal.  The appeal was heard on 10 February 2025. Judgment is awaited.

Outcome:

By way of written judgment delivered on 10 May 2024, the High Court acceded to an application by Meta Platforms Ireland Limited (Meta) for an order adjourning the entirety of Meta’s appeal (and related judicial review proceedings) against a decision made by the DPC on 25 November 2022, pending the outcome of separate proceedings before the General Court of the European Union.

Background to the proceedings

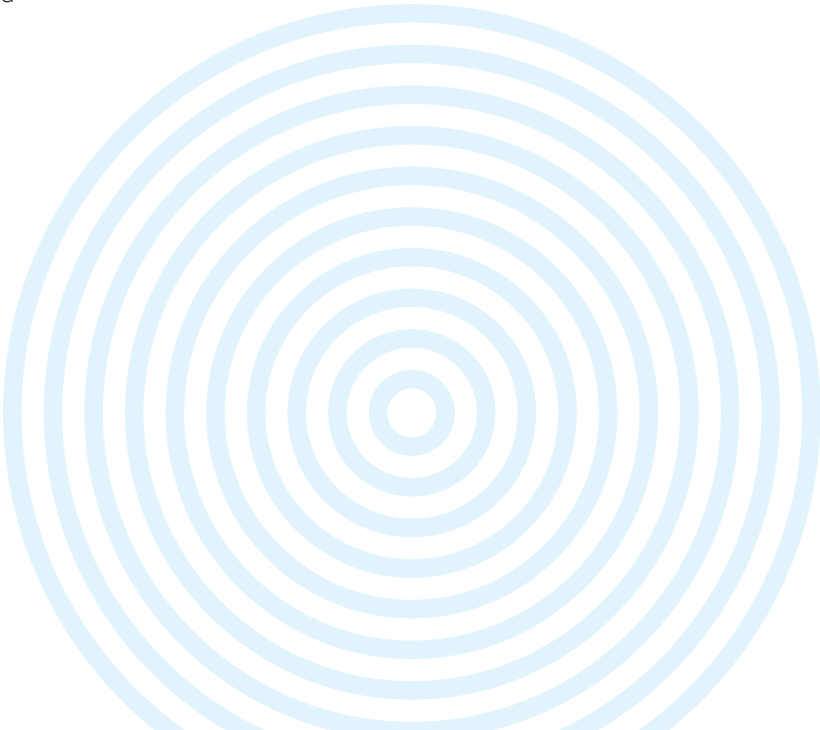
By decision dated 25 November 2022, the DPC made certain findings against Meta arising from a data breach in which the personal data of approximately 500m users was “scraped” from the Facebook platform and published on the internet.

- The DPC made the following orders in the exercise of its corrective powers:
- 1. An order directing Meta to bring its processing into compliance within a period of 3 months, by taking specified steps to secure users’ data and mitigate against the risk of such data being “scraped” by third parties;
  - 2. A Reprimand in respect of the infringements identified in the Decision; and
  - 3. Administrative fines in the amounts of €150 million and €115 million, respectively.

Meta appealed the DPC decision and also issued parallel judicial review proceedings. Meta then brought a motion seeking an order adjourning the domestic proceedings pending the final determination of separate proceedings before the CJEU. The DPC opposed that application, contending that with the exception of one discrete element, the appeal should be progressed without delay.

Following a contested hearing, the High Court held that the appeal (and related judicial review proceedings) should be adjourned in their entirety to await the outcome of the proceedings pending before the CJEU.

On 30 May 2024, the Court awarded Meta its costs of the adjournment application. The Judgment was subsequently appealed by the DPC. A hearing date in the Court of Appeal was awaited at year’s end.



No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
7	Court of Appeal Record No. 2023/282	Johnny Ryan -v- Data Protection Commission & Google Ireland Ltd (as Notice Party)	Appeal from the High Court  Court of Appeal	24th of June 2024	Proceedings concluded

**Outcome:**

By way of written judgment delivered on 24 June 2024 the Court of Appeal dismissed Mr Ryan’s appeal from an earlier Judgment and Order of the High Court in which the High Court upheld a (procedural) decision of the DPC to complete its “own-volition” inquiry into Google’s “real-time bidding” online advertising systems before separately considering a complaint in which an additional issue was raised by Mr Ryan in relation to those systems.

**Background to the appeal**

After it had commenced an own-volition inquiry into Google’s Real Time Bidding (RTB) systems, the DPC was called on by Mr Ryan to separately investigate a complaint in which Mr Ryan called into question the lawfulness of certain other aspects of the same systems. The DPC declined to do so, taking the view that it would be more efficient (and more effective) to complete its own-volition inquiry before considering whether or not to go on to deal with the particular objection raised by Mr Ryan.

Mr Ryan brought judicial review proceedings seeking orders compelling the DPC to investigate his complaint.

In a written Judgment delivered on 28 August 2023, the High Court (Simons J) dismissed the judicial review proceedings, noting that the GDPR affords discretion to supervisory authorities in terms of their approach to the sequencing of investigations. The Court further held that it was reasonable and proportionate for the DPC to have decided to complete its own-volition inquiry first, before turning to the Applicant’s complaint.

In a written Judgment delivered on 24 June 2024, the Court of Appeal upheld the Judgment of the High Court. The Court found no error in the conclusion of the High Court that the decision of the DPC to prioritise the own-volition inquiry and defer the handling of Mr Ryan’s complaint was proportionate and well within the margin of appreciation allowed to supervisory authorities. Costs were awarded to the DPC.

Mr Ryan subsequently sought leave to appeal to the Supreme Court. That application was refused by a determination made on 21 October 2024.



No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
8	High Court Record No. 2023/179 CA	Peter Nowak v Data Protection Commission	Appeal on a point of law  High Court	Judgment dated 2 July 2024  Order of 8 October 2024	The Appellant has brought a further appeal to the Court of Appeal. That appeal is listed for hearing on 18 March 2025.

Outcome:

By way of written judgment delivered on 2 July 2024, the High Court dismissed Mr Nowak’s appeal on a point of law from an earlier decision of the Circuit Court.

These proceedings have their original in a complaint made by Mr Nowak in 2010, which ultimately led to a Judgment of the CJEU in which that Court held that, in the exercise of his right of access to personal data, Mr Nowak was entitled to access to his examination scripts in respect of certain professional accountancy examinations Mr Nowak had sat some years previously. Sometime after Mr Nowak secured access to his examination scripts in 2018, he contended that certain other aspects of his 2010 complaint had not been addressed by the DPC. The aspects in question were

identified by Mr Nowak in 2020. By decision dated 21 April 2022, the DPC ruled against Mr Nowak on each of those other aspects.

Mr Nowak appealed that decision to the Circuit Court. His appeal was rejected by the Circuit Court for the reasons set out in a written judgment dated 9 October 2023 (O’Connor J).

Mr Nowak next brought a further appeal (on a point of law) to the High Court.

By written judgment dated 2 July 2024, the High Court (Bradley J) dismissed Mr Nowak’s further appeal and awarded costs against Mr Nowak

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
9	High Court Record No. 2024/81 JR	Google Ireland Limited v Data Protection Commission	Judicial Review  High Court	Judgment of the High Court delivered on 11 October 2024.  Order dated 5 November 2024	Proceedings concluded

Outcome:

On 23 October 2023, the DPC commenced an inquiry into a series of 6 complaints against Google Ireland Limited, from data subjects in several European countries, alleging that Google’s account opening processes involved the unlawful processing of users’ personal data.

Google brought Judicial Review proceedings in which it alleged that the DPC’s decision to commence its inquiry was unlawful because, as at the date of commencement of the inquiry, it had failed to examine and conclusively determine a series of questions relating to the admissibility of the complaints.

Whilst the Court found that the DPC did not have all relevant and necessary information to hand at the point at which it commenced its inquiry, it found that the DPC was entitled to rely on information it obtained from the complainants after the date of commencement of the inquiry in circumstances where that information would have been available to the DPC if it sought access to it at the appropriate time. On that basis, the Court exercised its discretion to allow the inquiry to continue (save in respect of one of the six complaints).

The Court ordered the DPC to pay 70% of Google’s costs.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
10	Dublin Circuit Court Record No. 2024/1054	Owen V. McGinty v The Data Protection Commissioner	Statutory Appeal  Circuit Court	Judgment of the Circuit Court delivered on 15 October 2024  Circuit Court Order dated 15 October 2024	Proceedings concluded

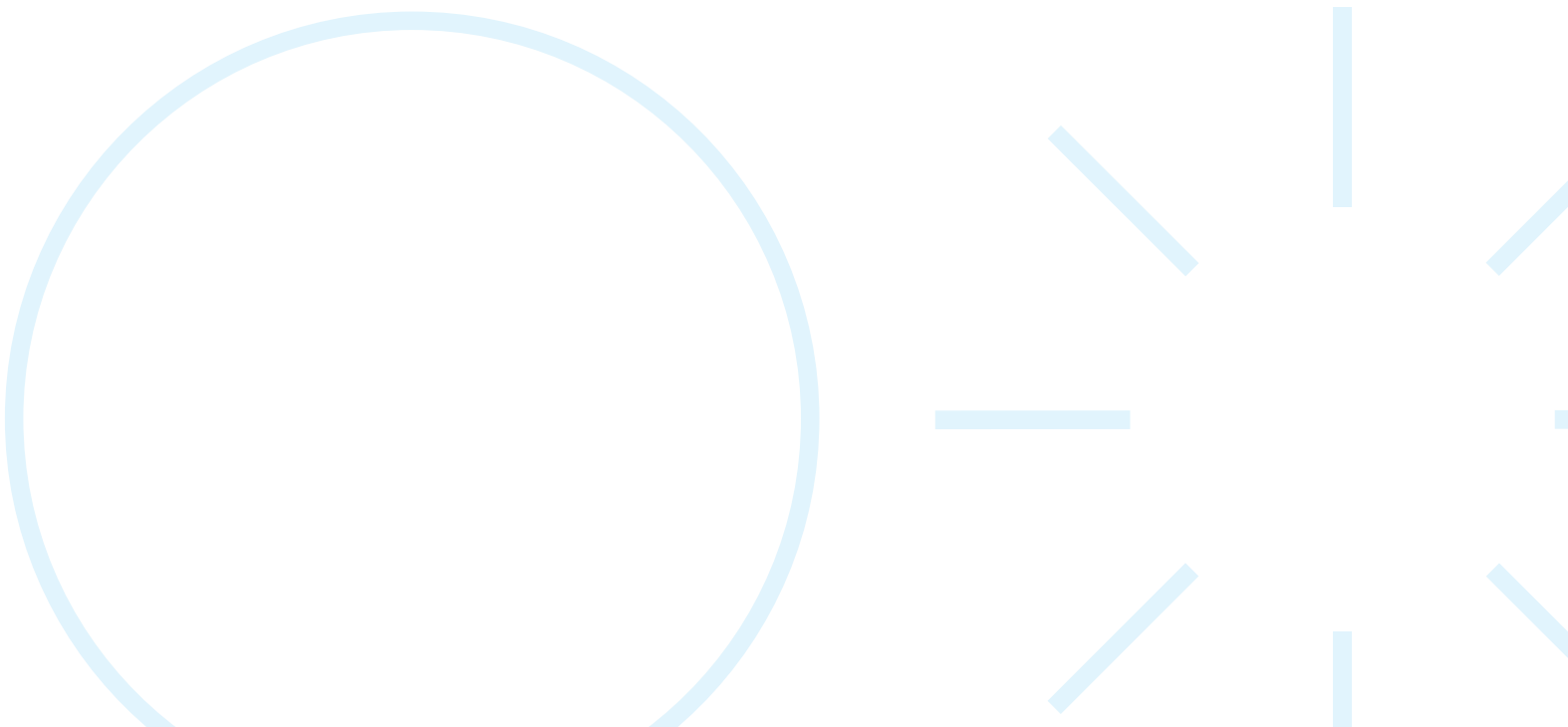
**Outcome:**

By way of written Judgment delivered on 15 October 2024, the Circuit Court found that an appeal brought by Mr McGinty against an earlier decision of the DPC could not be pursued because it was time-barred.

The DPC decision in question was issued on 6 February 2024. In it, the DPC declined to uphold a complaint made by Mr McGinty against the Workplace Relations Commission in which, relying on Article 16 of the GDPR, Mr McGinty demanded amendments to a statutory decision made by an

Equality Officer in 2012 in response to a separate and much earlier complaint brought under equality legislation. (Such amendments were sought on grounds that the Equality Office’s decision contained inaccurate personal data relating to Mr McGinty).

Mr McGinty appealed the DPC’s decision to the Circuit Court but the appeal was filed late. The appeal was duly struck out by the Circuit Court.



No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
11	High Court Record No. 2024/411 MCA	Data Protection Commission v Twitter International Ltd.	Section 134, Data Protection Act 2018 application.  High Court	6 <sup>th</sup> of August 2024	Proceedings concluded

Outcome:

On 8 August 2024, the DPC brought an urgent application before Judge Leonie Reynolds in the High Court under Section 134 of the Data Protection Act 2018 in which it requested the Court to prohibit the processing by X of personal data contained in the public posts of X’s EU/EEA users for the purpose of training its AI tool, “Grok”.

This was the first time that the DPC had brought proceedings under Section 134, being a provision of the Data Protection Act 2018 which allows the Commission, where it considers that there is an urgent need to act to protect the rights and freedoms of data subjects, to make an application to the High Court for an order requiring the data controller to suspend, restrict or prohibit the processing of personal data.

The Court was satisfied that there was an urgency to the DPC’s application in this case.

In answer to the application, X agreed to give certain undertakings to the Court to suspend its processing of an identified body of personal data.

The Court was satisfied that the undertakings in question met the situation in terms of protecting the data in question until such time as the proceedings were the subject of a determination by the Court.

On 4 September 2024, when the matter came back before the Court, the proceedings were struck-out on the basis of X’s agreement to continue to adhere to the terms of the undertakings given on 8 August 2024 on a permanent basis.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
12	Court of Appeal Record. No. 2024/17	Martin Meany v Data Protection Commission	Court of Appeal (Appeal of High Court Costs Order)	Order dated 1 August 2024	Proceedings concluded

Outcome:

On 3 October 2022, Mr Meany brought Judicial Review proceedings against the DPC, alleging that it had failed to issue a decision in respect of a complaint Mr Meany had filed with the DPC in relation to certain Church authorities.

The proceedings were rendered moot when the DPC delivered its decision in relation to Mr Meany’s complaint on 23 June 2023. (The complaint was not upheld). In advance of that date, the DPC had alerted Mr Meany to the fact that it would not decide his complaint until it had first completed an own-volition inquiry into the handling of Church records more generally within certain dioceses in the State.

In an ex tempore judgment delivered on 20 December 2023, the High Court ordered that the proceedings be struck out as they were moot. It directed that there should be no order as to costs.

Mr Meany in turn appealed the costs element of that Order to the Court of Appeal. On consent, the Court of Appeal agreed (on 1 August 2024) to make an order directing that:

- the appeal be struck out; and
- the DPC pay the Appellant’s costs in the High Court proceedings (bearing Record No. 2022/820JR) up to the date of the ex tempore judgment delivered on 20 December 2023.
- No Order as to costs in respect of the Court of Appeal proceedings.



No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Current Status
13	Circuit Court Record No. 2023 /05049	Sonzic Francis v Data Protection Commissioners & Dyson Ireland Ltd, Briscoes Electrical Arnotts and Arnotts Brown Thomas as Notice Parties	Statutory Appeal  Circuit Court	Circuit Court Order dated 14 May 2024	Proceedings concluded

**Outcome:**

Ms Francis brought a statutory appeal, purporting to challenge a “decision” of the DPC.

On 14 May 2024, the Circuit Court made an order dismissing Ms Francis’ appeal in circumstances where the Court found that Ms Francis’ underlying complaint had not been decided but was still being actively investigated by the DPC.

The Circuit Court found that it had no jurisdiction to deal with the appeal in circumstances where no decision had yet been made by the DPC.

No order was made on costs.



---

# 6

---

## Supervision



# Supervision

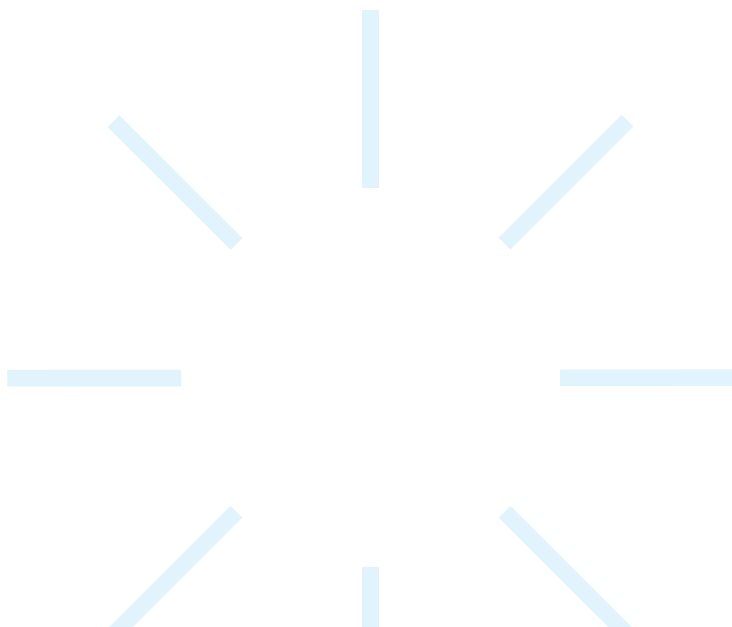
The fifth goal of the DPC's Regulatory Strategy is to support organisations and drive compliance. Supervisory engagement with organisations in all sectors allows the DPC to understand how they process personal data, and how they meet their compliance requirements as data controllers. This aligns with the DPC's task as a supervisory authority under GDPR to promote the awareness of organisations of their data protection obligations. By engaging in this manner the DPC can support organisations in identifying potential data protection issues in the development of new products or services, and advise on implementing best practice compliance solutions at the earliest opportunity, in line with the principle of data protection by design. This work takes on a particular focus where the DPC is the Lead Supervisory Authority and can discuss and engage with companies planning to launch of new products or services in the EU/ EEA market.

The DPC adopts an open and communicative approach with the organisations that it regulates, in addition to sectoral representative bodies, DPO networks and legislators, as a key method to drive compliance, accountability and a wider culture of data protection awareness.

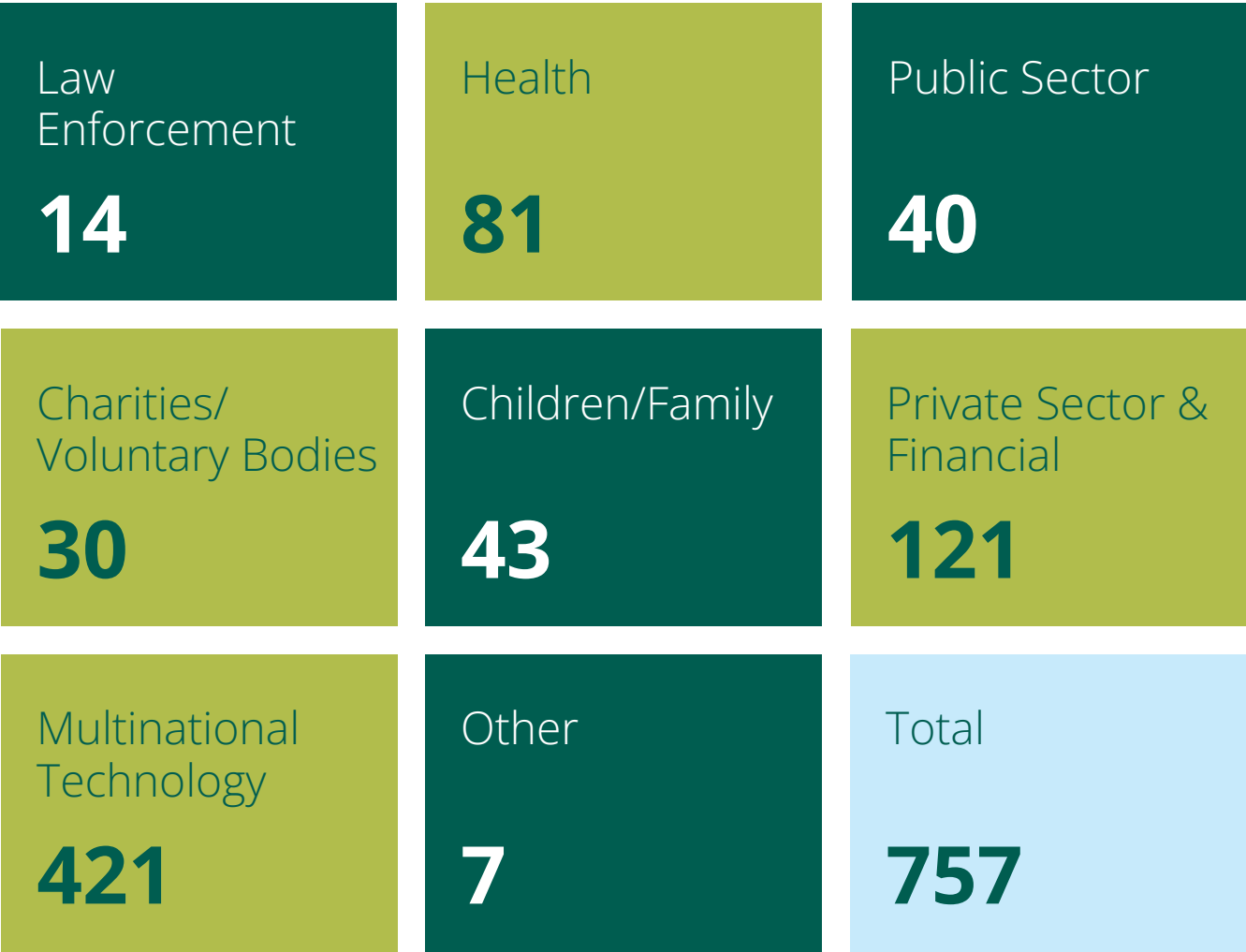
Proactive engagement with organisations in the development of new data processing operations or projects allows the DPC to advocate strongly for the upholding of the data protection rights of individuals by mitigating against potential infringements before they occur. Although resource intensive,

supporting organisations and driving compliance ultimately leads to better outcomes for individuals as customers, service users and citizens.

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



The DPC had **757** supervision engagements during 2024. The sectoral breakdown is as follows:



In addition, across all sectors the DPC engaged in **291** supervision meetings with organisations in 2024. It can be observed from the above that a significant amount of DPC engagement is with the multi-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.



## Legislative Consultation

A key statutory function of the DPC is prior consultation on legislative measures that relate to data processing. Both the GDPR and Data Protection Act 2018 require Government Departments to consult the DPC on any legislative or regulatory measures that will involve data processing. This is of particular importance where legislation is creating a new legal basis for the processing of personal data by public bodies or agencies.

In this consultation process, the DPC works with those drafting legislation to ensure that legislation requiring the processing of personal data is clear, precise, and foreseeable in its effect. Additionally, the DPC seeks to ensure that where legislation underpins the processing of personal data it is clear that this will be necessary to meet a clear objective of public interest, and is proportionate to the aim that it pursues.

Where necessary to meet the requirements of GDPR, in particular where special categories of personal data are concerned, the DPC provides advice on how legislative measures can implement safeguards to protect the rights

and freedoms of affected individuals. Additionally, the DPC helps to ensure that any proposed restriction of data subjects in new legislation meets the requirements of Article 23 of the GDPR. Any such restriction must be necessary and proportionate in safeguarding a clear public interest and respect the essence of the fundamental rights and freedoms in question.

### **The DPC provided guidance and observations on 56 proposed legislative measures in 2024 including:**

1. The Child Care (Amendment) Bill 2024;
2. The Automatic Enrolment Retirement Savings System Act 2024;
3. The Health Information Bill 2024;
4. The Mental Health Bill 2024;
5. Garda Síochána (Recording Devices)(Amendment) Bill;
6. S.I. No. 216/2024 - Garda Síochána (Recording Devices) Act 2023 (Code of Practice); and
7. Seanad Electoral University Members Amendment Bill 2024.



---

## Regulatory engagement

---

### Local authorities and CCTV

Over the course of 2024, the DPC continued to offer guidance and support to local authorities on their use of CCTV and other recording devices for combatting certain waste and litter pollution offences, following the implementation of statutory codes of practice for these activities in 2023. In addition, the DPC continued to conduct inquiries during the year into the usage of CCTV by certain local authorities (see Annual Report 2023).

---

### CCTV and Data Protection Impact Assessments (DPIAs)

In July 2024, the DPC received a consultation request from a Local Authority (Council) for a proposed community CCTV scheme. In line with their obligations under the Law Enforcement Directive, the Council carried out a Data Protection Impact Assessment (DPIA), which they shared with the DPC for review. The Law Enforcement Directive regulates the processing of personal data for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. It is the relevant part of the data protection legislative framework for data processing by Councils for law enforcement purposes, rather than the GDPR.

In their DPIA, the council had correctly identified two potential risks resulting from the CCTV scheme. These risks involved

the excessive surveillance of members of the public and the possible monitoring of individuals within private dwellings. However, in terms of mitigations, the Council's DPIA stated that the CCTV scheme was very popular locally and proposed "consideration of public feedback" as a possible solution to these identified risks.

The DPC replied that this proposed mitigation did not appear adequate as it suggested that risks to data subject rights would be automatically mitigated if the processing were supported by the local community.

The DPC's recommendations to the Council were to implement measures that would tangibly address the identified risks. These included the repositioning of cameras to avoid excessive surveillance of publicly accessible areas, and the reduction of the number of cameras to cover areas that are considered strictly necessary to address public order and safety issues identified in the scheme.

This example illustrates that while canvassing the views of stakeholders, including the public, can be a valuable part of the DPIA process, risks to the rights and freedoms of individuals cannot be collectively waived through public consultation alone. The fact that a CCTV scheme is popular locally does not relieve the obligation on local authorities to consider potential risks to affected individuals in a clear-eyed manner and to put in place effective safeguards to prevent excessive surveillance/ monitoring of individuals.







### CCTV and Transparency

In September 2024, the DPC received a query from a Council on the extent of its obligations to erect signs informing members of the public of the operation of a CCTV scheme in their county town. While the codes of practice developed by the Local Government Management Agency (LGMA) state that signs should be “at or in close proximity to each camera”, the council expressed concern that this would not be appropriate and could interfere with the purpose of the scheme.

The council proposed an alternative approach whereby large signs would be placed on roads leading into the town warning that CCTV was in operation at unspecified locations in the town centre. The DPC replied that this alternative approach appeared to contradict the plain meaning of the codes, which reflect the Council's transparency obligations under the Law Enforcement Directive. The DPC advised the Council that they should place appropriate signs at each location where CCTV is deployed, in line with the right of affected individuals to be properly informed about the processing of their data. This example illustrates the importance of providing adequate transparency information to the public on use of CCTV.

**Failure to put in place appropriate signage for CCTV risks inadvertently engaging in covert surveillance.**

Covert surveillance is generally unlawful and should only be used in very exceptional circumstances, reflecting the much more significant level of interference with the rights of affected individuals that is involved. The Council's proposals in this case were not compliant because they sought to blur this distinction by not providing a reasonable level of information to the public about the location of the CCTV.

### CCTV and Littering

In September 2024, the DPC also became aware of media reporting which claimed that local authorities were prohibited from using CCTV to investigate littering and waste management offences on data protection grounds, except where a motor vehicle was used in the commission of the offence. This claim originated from an interview with a council official in which the Council's implementation of the recently finalised LGMA codes of practice was discussed.

Suspecting that this claim stemmed from a misapprehension of some kind, the DPC contacted the council to seek further clarification. It transpired that, rather than the council considering that they were legally prohibited from using CCTV footage to investigate such offences, the issue was that CCTV footage is generally of limited investigative value where there is no information (such as a vehicle licence plate) that can be directly linked to an identifiable individual. Nothing in data protection law prevents a local authority from using CCTV footage to investigate illegal dumping based on whether or not the suspect is operating a motor vehicle. However, this case illustrates why CCTV should not be regarded as a “silver bullet” solution to the challenge of combatting waste management and litter pollution offences. Local authorities can and should use CCTV to the extent that it is objectively effective in the circumstances and as part of a broader range of measures.

As the above case studies illustrate, the DPC is committed to assisting local authorities in their use of CCTV in a data protection-compliant manner and welcomes the fact that they now enjoy a clear legal framework to use these tools under the Garda Síochána Act, 2005 and the Circular Economy and Miscellaneous Provisions Act, 2022 which were introduced specifically to remedy issues highlighted in DPC decisions.

## Law Enforcement and Body-Worn Cameras– Inland Fisheries Ireland

A key theme for the DPC in 2024 was engagement with several public bodies on their adoption and deployment of recording devices, such as body-worn cameras and drone technology, in support of their law enforcement activities. As the following examples illustrate, the DPC's objective through this engagement is to ensure that these public bodies have an appropriate legal basis in place beforehand so that the conditions around the use of these devices are clear, precise and foreseeable to affected individuals.

In February 2024, the DPC received a consultation request from Inland Fisheries Ireland (IFI) regarding a pilot project on the deployment of body-worn cameras on staff. The IFI had identified a business need to deploy body-worn cameras in order to discourage harassment and intimidation of its staff in the context of inspections, but also to use the footage to investigate and prosecute offences under fisheries legislation. The DPC noted that the pilot project was at an advanced stage: The IFI had already procured the devices and organised staff training. The DPC reviewed the materials provided and noted that, although the IFI had put in place a range of policies and safeguards for the use of the cameras, it did not appear to have an appropriate legal basis for the underlying processing of personal data under current fisheries legislation.

The DPC advised that in order to meet the requirements of data protection law, the IFI would need to identify a legal basis that explicitly empowered it to operate mobile recording devices in pursuit of its law enforcement functions. Examples of such legal bases used by other law enforcement authorities in Ireland are the codes of practice being prepared by An Garda Síochána under the Garda Síochána (Recording Devices) Act 2023, or those prepared by the Local Government Management Agency under the Circular Economy and Miscellaneous Provisions Act 2022.

The DPC concluded that unless and until the IFI could put in place such a legal basis, it would likely only be able use these devices in a limited manner to protect the safety and welfare of its employees, but that any resulting footage could not be retained and used to investigate fisheries offences.

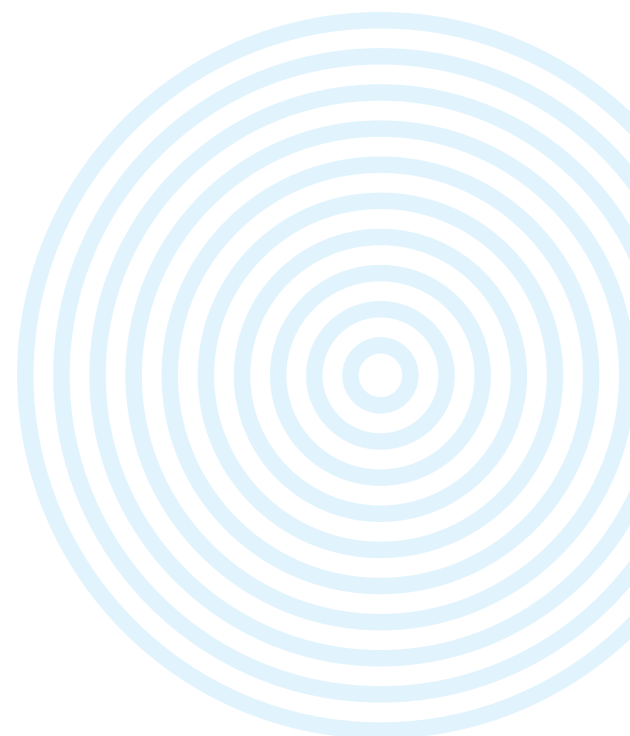
In 2025, the DPC planned to continue to engage with IFI on the establishment of a clear legal basis for the lawful use of Body Worn Cameras by its authorised officers.

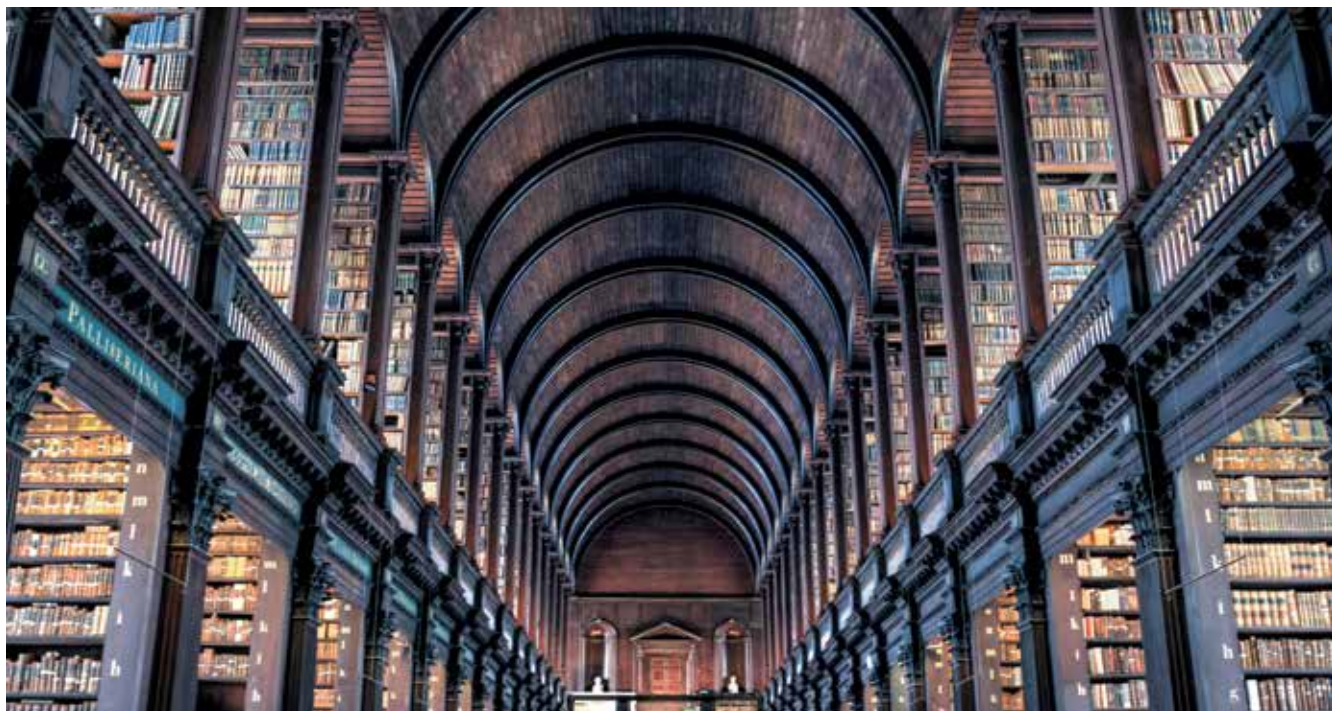
## Law Enforcement and body worn cameras – An Garda Síochána

In March 2024, An Garda Síochána formally consulted with the DPC on its draft code of practice for the deployment of body worn cameras under the Garda Síochána (Recording Devices) Act 2023.

The DPC conducted a thorough review of the draft code, including a site visit to Garda Headquarters to view the technology in operation and to assess the appropriateness of the technical and organisational safeguards in place. In its opinion on the code, the DPC emphasised the importance of the code providing sufficient detail on the circumstances in which Garda members will use body-worn cameras.

This is necessary in order for the code to provide a valid legal basis for processing personal data that meets the requirements of the Law Enforcement Directive. If the finalised code were to contain language that is too imprecise, reflecting mere guidance or statements of best practice, then there is a risk that the code itself as well any convictions based on camera footage, may be open to legal challenge. This consultation process with An Garda Síochána was ongoing at year's end to ensure that the final code allows Garda members to use these tools in a data protection-compliant manner.





### Law Enforcement - Drone Technology Revenue Commissioners

In August 2024, the DPC became aware through media reporting that the Revenue Commissioners was planning a pilot project on the use of drone technology in support of its customs enforcement functions. The DPC began an informal consultation process with the Revenue Commissioners in order to learn more about this pilot project and the lawful basis for processing. While this process remained ongoing at year's end, the DPC advised the Revenue Commissioners of the importance of ensuring a sufficiently robust legal basis for the use of these technologies if they are to be used in a sustainable manner in the long term.

The DPC recognises the value of the use of mobile and portable recording devices by law enforcement authorities and is committed to supporting these authorities in rolling out these tools in a data protection compliant manner.

**As the above examples illustrate, it is particularly important that any public authority considering the adoption of these tools ensures that they have an appropriate legal basis in place prior to the commencement of processing.**

Failure to do so not only presents a serious risk to the fundamental rights of affected persons, but also risks the safety of any criminal convictions based upon evidence gathered with such tools. The use of such tools for law enforcement purposes is permissible under the LED once the requirements of data protection law are met.

### Facial Recognition Technology

In June 2024, the DPC participated in a roundtable event coordinated by the Irish Council for Civil Liberties on the use of Facial Recognition Technology in law enforcement. Other stakeholders attended this event from Ireland and abroad, including representatives of the American Civil Liberties Union. The event provided an opportunity to discuss situations of wrongful arrest and detention if errors in Facial Recognition Technology (FRT) products result in the misidentification by police forces of an individual as a suspect in a crime they did not commit.

This discussion proved valuable to the DPC as part of the wider consideration of the use of FRT in policing, in the context of the DPC's statutory consultation on the Garda Síochána (Recording Devices) (Amendment) Bill 2023, which is intended to provide An Garda Síochána with access to this technology. During 2024, the DPC advised An Garda Síochána of the importance of ensuring that any implementation of FRT in Ireland takes into consideration the significant implications that it can have for individuals and groups of people, including minorities, and that consequently sufficient safeguards are put in place to mitigate any risk arising from the deployment of this technology and the processing of personal data in this context.

## Irish Association for Counselling and Psychotherapy webinars

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 in the health and social care sector during 2024. These sessions built upon the DPC's 2023 engagement and directly addressed the data protection challenges faced by the not-for-profit sector. This included two webinars for members of the Irish Association for Counselling and Psychotherapy (IACP).

The webinars covered crucial topics such as data breaches, requests from law enforcement bodies such as An Garda Síochána for information on patients, and data subject access requests from clients. Each session was designed to be interactive, allowing participants to ask questions and share experiences, to voice their concerns and receive real-time insights which allowed peer-to-peer learning. The engagement levels were high, with an average of **400 attendees per session**, representing a variety of charities, voluntary organisations, and independent practitioners across the country.

To further support the practitioners, the DPC compiled a comprehensive Frequently Asked Questions (FAQ) document based on the issues raised during the webinars. This document serves as an ongoing resource, addressing common concerns and providing practical guidance on data protection compliance. Feedback from participants has been overwhelmingly positive, with **90% reporting that the webinars significantly improved their understanding of their data protection responsibilities**. Many attendees expressed appreciation for the tailored content and the opportunity to discuss sector-specific challenges. This initiative has not only enhanced compliance awareness but has also strengthened the DPC's relationship with the charity sector, paving the way for more targeted support in the future.

The DPC will continue working with representative bodies in the charity and voluntary sector during 2025 to identify opportunities for proactive engagement, and improved compliance.

# 90%

reported that the webinars significantly improved their understanding of data protection

## Sports survey

Following its comprehensive examination of data protection issues in sports initiated in 2023, the DPC has made significant progress in understanding the complex landscape of data processing in both professional and amateur sports in Ireland. In line with Goal 3 of the Regulatory Strategy, the DPC has focused on the handling of children's data and the increasing use of technology for performance monitoring and other purposes.

In order to establish an understanding of the data protection awareness of key actors in this area, in February 2024, the DPC issued a questionnaire to 110 sports clubs across Ireland from major participation sports, including the Gaelic Athletic Association, Ladies Gaelic Football Association, Irish Rugby Federation Union, and Football Association of Ireland. This survey was designed to assess the current state of data protection compliance and to gain deeper insights into the relationships between various parties involved in sports and their data sharing arrangements. The questionnaire covered critical areas such as the use of technology in collecting and analysing player performance data, the purposes of data processing, and the transparency of data handling practices, with a particular emphasis on how children and young people are informed about the processing of their personal data.

The survey findings revealed several concerns: **over 40% of respondents reported not having any formal data protection policies in place**. Half of the organisations surveyed did not have procedures to enable data subjects to exercise their rights. Additionally, 39% indicated they collect performance data, but did not understand that this is classified as special category data. Other recurring issues included the absence of retention schedules, limited understanding of special category (particularly health) data, and insufficient training on data protection responsibilities.

The DPC's next steps will include outreach to governing and bodies and sports organisations to assist with the development of tailored guidance for both clubs and members of the public. As part of this process, we will be conducting a wider stakeholder engagement taking in the sports' governing bodies, representative associations, and government agencies to work collaboratively to develop useful tools for data protection compliance in the sector.

# Over 40%

of respondents reported not having any formal data protection policies in place



---

## Medical Centre Patient Records

In 2024, the DPC engaged with two general practitioner (GP) clinics to assist in resolving a dispute over the management of patient records. The issue arose when a GP departed their original practice to start a new clinic and requested the transfer of their patients' records. However, the original practice was reluctant to release these records in the absence of the consent of the patients in question. The confusion arose from a misunderstanding about who was considered to be a data controller of the patient data, complicating the decision on how to manage patient records when a GP departs from a practice.

To address this situation, the DPC organised a meeting with the GP practice to provide guidance and clarity. The DPC explained the different roles involved in managing patient data, including the roles of data controllers, joint controllers, and data processors. The DPC also stressed the importance of having clear agreements in place when multiple parties are responsible for the same data. The DPC recommended establishing formal joint controller agreements that clearly defined each GP's roles, responsibilities, and liability regarding patient data management. For GP departures, the DPC advised implementing a structured departure protocol where both practices would document which patient records would be transferred, establish secure transfer methods, and maintain comprehensive audit trails. The original practice subsequently created standardised procedures requiring departing GPs to provide advance notice, complete handover documentation, and participate in a transition meeting where record access arrangements would be formalized in writing before any transfer occurred. The DPC further advised implementing a transparent communication protocol requiring practices to promptly notify patients when their GP was departing. This included sending practice letters detailing the GP's new location, timeline for transition, and how continuity of care would be maintained.

The DPC's advice helped the GPs understand their responsibilities under data protection law and highlighted the need for well-defined policies to handle situations like this in the future.

**This case highlights the importance of having robust data governance structures in healthcare settings.** By engaging with the practice and offering the DPC's expertise, the DPC was able to resolve the confusion and ensure that patient data was handled appropriately. It was important for the DPC to assist in facilitating a timely solution to avoid any adverse patient outcomes due to a lack of access to data. This engagement not only solved the immediate problem but also reinforced the broader need for clear guidelines and procedures in medical practices to manage patient data effectively and in compliance with legal requirements. The DPC planned to engage with stakeholders including representative bodies of healthcare practitioners and the Department of Health on these matters in 2025.

---

## Adult Safeguarding Guidance

The DPC has identified as a strategic goal the prioritisation of the protection of children and other vulnerable groups, in the DPC's Regulatory Strategy 2022-2027. As part of this commitment, the DPC has engaged with stakeholders groups in this sector in identifying data protection concerns arising in the context of adult safeguarding.

In 2024, the DPC developed a guidance document on the issues arising in data sharing in adult safeguarding, illustrating the practical day-to-day issues experienced by practitioners for publication in 2025. This guidance seeks to provide clarity around the considerations and analyses that must be born in mind when processing data in the adult safeguarding context. The guidance is part of a planned range of actions including the publication of FAQs for both practitioners and members of the public on specific issues, such as the interaction between GDPR and the Assisted Decision-Making (Capacity) Act 2015.

The DPC also contributed to the Law Reform Commission's report on a Regulatory Framework for Adult Safeguarding, and participated in the launch of this valuable document in April 2024, along with other regulatory colleagues and stakeholders. The DPC welcomes the Law Reform Commission's recommendation of the introduction of a statutory and regulatory framework for adult safeguarding, which would entail comprehensive, cross-sectoral legislation. In the existing regulatory landscape, the DPC remains committed to assisting those working in the complex field of adult safeguarding in understanding and meeting their data protection compliance obligations.

As part of this wider stakeholder engagement, the DPC also delivered a presentation to Designated Officers of the HSE's National Safeguarding Office responsible for adult safeguarding, focusing on data sharing and data protection best practices. The presentation provided a valuable opportunity to support Designated Officers in their daily operations and offer reassurance on best practices in data protection, particularly in the context of data sharing. The DPC planned to deliver more presentations and webinars to similar groups in 2025, which will assist in providing clarity and certainty regarding their data protection obligations, in particular when dealing with sensitive situations.

## English Language College Biometric Processing

In January 2024, the DPC responded to a concern raised by the Irish Council for Civil Liberties in relation to the alleged processing of personal data by way of fingerprint and/or facial recognition data for the operation of a biometric system clock-in system and mobile app by an adult education college. The purpose of the clock-in system was to scan students' fingerprints and faces for the purpose of tracking their attendance at classes. The DPC further noted that this app was allegedly used to record sick leave and students were required to submit medical certificates on it.

The DPC engaged with the college to understand the mechanics of the data processing, and to query the legal basis and terms and conditions of its use. While the DPC established that the college was lawfully relying on explicit consent from students for biometric processing, the consent form and the Terms and Conditions were not fully transparent in ensuring that the withdrawal of consent would be possible, nor that there were alternative methods for clocking in.

Arising from this positive engagement, the data controller implemented the changes highlighted by the DPC and issued an email to all students informing them of the alternative methods of clocking in and how to withdraw consent for the use of their biometric data. This engagement also highlights the need for data controllers to fully interrogate the data protection implications of introducing biometric processing solutions, which may appear to be simple and cost-effective but can represent a highly intrusive form of processing of special category personal data.

## Innovation and Public Service Transformation Strategy

During the course of 2024, the DPC has been consulted by and engaged with several Government Departments and public bodies on the data protection implications of the digitalisation of their services. These projects include the Digital Wallet & Life Events Programme, Online SAFE Registration, the HSE App, and the CSO Digital First Census pilot.

Each of these projects aims to make public services more accessible and available to citizens, delivering greater effectiveness and efficiency. The DPC welcomes the opportunity to engage on these initiatives in order to assist in the implementation of data protection by design, along with the full consideration of the safeguards that are necessary to protect people's personal data when they choose to engage with public services online.

In 2025, the DPC will continue to work with public bodies to ensure that data protection and privacy considerations are at the heart of Ireland's Public Service ICT strategy.

## Compliance Sweep of Supermarket and Convenience Store Sector

In accordance Articles 57 and 58 of the GDPR, which focuses on raising awareness among controllers and processors about their data protection obligations, the DPC carried out a GDPR compliance questionnaire on the Irish Retail Sector in 2024.

The project entailed conducting a fact-finding exercise with the largest retailers in the sector in Ireland with the objective of generating deeper insights into the data processing and compliance levels of data protection among Ireland's largest supermarket and convenience store retailers, which have a considerable footprint on data processing in Ireland<sup>5</sup>. Areas of focus included Article 30 of the GDPR, Records of Processing Activities (RoPAs), Article 12 of the GDPR transparency obligations as well as identifying any emerging or problematic data processing issues. The DPC is currently reviewing the responses to the questionnaires and it intended on engaging one to one with Controllers and following up on the issues identified from this sweep in 2025.

<sup>5</sup> The targeted organisations combined had over 90% market share in the sector





## Road Collision Data

The DPC concluded its consultation with the Department of Transport (DoT) regarding a review of the legislative basis for the receipt from An Garda Síochána (AGS) and the onward sharing of road traffic collision data by the Road Safety Authority (RSA) to local authorities and the National Transport Authority (NTA). This culminated with a new Ministerial Direction, pursuant to section 8(1) of the Road Safety Authority Act 2006, permitting the sharing of collision data to the RSA from AGS and an agreed approach to ensure the onward sharing of data to entities such as local authorities.

Throughout the consultation process, the DPC emphasised that the GDPR should not prevent the proportionate publication of crash location details, particularly where any personal data element is largely anonymised and /or limited to the data necessary to achieve the desired policy objective.

The DoT led the engagement between all stakeholders on examining the specific data fields involved resulting in the identification of a set of data points which met necessity and proportionality requirements. A Data Protection Impact Assessment (DPIA) was also conducted ensuring all risks associated with data sharing were identified and appropriately mitigated.

It is acknowledged that data sharing amongst a number of stakeholders can be a complex task. However, the GDPR provides a clear framework for all stakeholders to consider their data protection obligations. Consideration of the GDPR and implementation of a privacy design approach at the beginning of a project facilitates robust and sustainable data sharing arrangements. It requires organisations to carefully think through its objectives and what is required to achieve those objectives in a manner which involves the least impact upon the data protection rights of individuals. This is the important principle of data protection by design and by default set out in Article 25 GDPR.

Data protection by design and by default provides two critical concepts for future project planning. Data protection by design entails embedding data privacy features and data privacy enhancing technologies directly into the design of a system, product, service or process and then throughout the lifecycle. Data protection by default means that user service settings must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all.

Whilst the DPC has published specific guidelines for *data sharing in the public sector* **QR 1**, it is important that **stakeholders engage with the DPC at an early stage** and that appropriate timelines in respect of the delivery of a project are implemented. Holding workshops and having a project lead, as in this case, were important steps in ensuring a full and detailed assessment could be conducted which ultimately helped facilitate a satisfactory outcome for all stakeholders.

## Data Sharing in the Public Sector



QR 1

## Radio Teilifís Éireann (RTÉ)

RTÉ voluntarily consulted with the DPC regarding a Data Protection Impact Assessment (DPIA) it had conducted in relation to the creation of an internal register of interests and an external register of activities for its staff and contractors. Certain RTÉ staff and external contractors under contract with RTÉ have a duty to declare any conflicts of interests regarding external activities. However, the proposal, whilst improving governance around such declarations and approvals, also entailed the publication of a register of external activities on RTÉ's website. It was proposed that this online register would include name, description of external activity and remuneration (set out in bands) to be published online on a quarterly basis.

During the consultation, the DPC raised a number of issues with RTÉ, particularly in relation to the necessity and proportionality of creating an online register of external activities and the identification of an appropriate legal basis to underpin the processing proposed i.e. online publication of personal information on a quarterly basis relating to external activities carried out by RTÉ personnel in their private capacity.

Whilst RTÉ initially sought to rely upon the legitimate interest lawful ground under Article 6(1)(f) GDPR to publish such details, RTÉ agreed that it would underpin the processing via legislation. However, RTÉ were initially of the view that existing legislation could permit the processing of personal data for an internal register of interests and for an online external register of activities.

Whilst the DPC did not at this time have an issue with RTÉ's position regarding the processing of personal data for an internal register, it disagreed with its view regarding an external register of activities. In noting the generic nature of the legislation being proposed to underpin the proposal (i.e. the Broadcasting Act 2009), the lack of clarity, precision and foreseeability in its application to persons subject to it and the serious interference entailed, in line with recent jurisprudence of the Court of Justice, the DPC strongly recommended RTE to consider seeking an additional legislative mechanism to underpin the processing to publish an external register.

RTÉ responded positively to the DPC's recommendation and agreed not to publish the personal information as proposed in the absence of such a mechanism. Rather, RTÉ paired back its proposal regarding online publication and currently publishes quarterly reports in an anonymised format.

**If bodies intend to publish personal details of individuals online it is important to understand that processing of this nature entails a significant and serious interference with the fundamental rights to privacy and protection of personal data.** As such, the bar to be met is very high, requiring a controller to demonstrate that the processing is justified and that an adequate and robust legal basis exists which is clear, precise and foreseeable to the persons who are subject to it.

## Use of CCTV in restrooms

Throughout 2023, the DPC received numerous queries and complaints from individuals about organisations' use of CCTV in restrooms or areas where a high expectation of privacy exists (see Annual Report 2023).

The DPC engaged with these organisations on a one-to-one basis and also updated its guidance on the use of CCTV by data controllers to include a specific section on *"The use of CCTV in areas of an increased expectation of privacy"*. **QR 2** This was aimed at clarifying the position of the use of CCTV in areas where individuals have a heightened expectation of privacy. In addition, the DPC contacted the relevant industry bodies to inform them of the update with the DPC's guidelines.

As a consequence of this guidance, in 2024 the DPC noted a considerable reduction in concerns raised by the public about CCTV in restrooms or areas where a high expectation of privacy exists.

The DPC intended to engage with small and medium sized enterprises throughout 2025 on similar issues to deliver clear and practical guidelines to assist these organisations in meeting their compliance responsibilities in a proportionate and balanced manner.



**QR 2**



### Technology companies sharing personal data with law enforcement agencies.

In 2023, the DPC contacted several technology organisations in relation to how they share personal data with law enforcement and requested detail on the processes and policies that they have in place when doing so (see Annual Report 2023).

The DPC examined issues such as the process which controllers use to authenticate requests for user data from law enforcement agencies, how they determine the validity of emergency requests for user data so as to respect the principle of data minimisation when responding to requests for user data. Also examined was the internal guidance and/or workflows that is available to the controller's staff who process such requests from law enforcement agencies.

For those controllers whose policies were not considered to be sufficiently developed, recommendations were provided on further action that could be taken in this regard including detail on useful practices that would assist with eliminating any gaps in terms of data protection<sup>6</sup>.

Whilst this project has now concluded, for those organisations where the DPC identified room for improvement, they were expected to revert to the DPC during 2024 with detailed feedback on how they addressed the recommendations. Some responses are listed below:

**Controller A** – Has advised that they have updated policies consistent with the DPC's guidance. They further stated that the DPC's "good practice" observations on the importance of detailed documented guidance for staff handling non-emergency law enforcement requests was accepted, and they have consolidated and updated such guidance accordingly and will continue to ensure that their staff have access to appropriate resources tailored to address the types of requests the company receives.

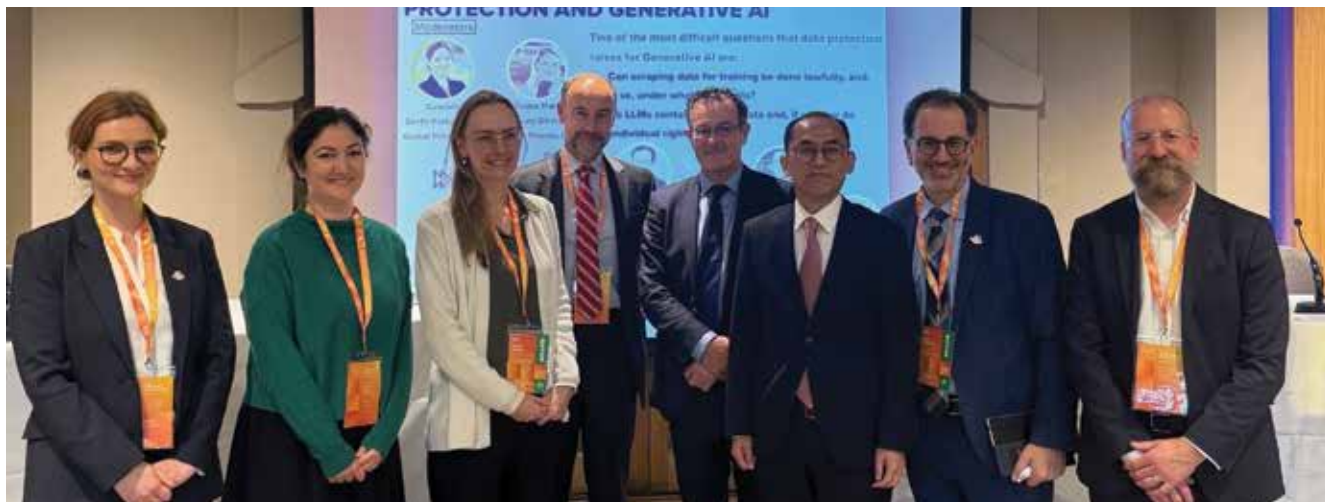
**Controller B** – Has stated that they have implemented enhancements in line with the recommendations from the DPC to these four categories: (1) Authentication of Law Enforcement Requests (2) Emergency Requests (3) Voluntary (Non-Emergency) Disclosures (4) Audits.

**Controller C** – Has stated that they have initiated a variety of substantive changes to their lawful access policies and procedures, including to areas such as Emergency Disclosure Requests, Internal Staff Guidance and Workflows, Authentication of Law Enforcement Portal Accounts, Human Review and the Scope of Data Requests.

<sup>6</sup> Recommendations were provided on a number of matters such as:

- Determining the validity of emergency requests - to provide controller personnel with clearer guidance on how to verify the authenticity of an emergency request;
- Improving workflows and personnel guidance; and
- Processes for authenticating requests for data from law enforcement.





Commissioner for Data Protection and Chairperson of the DPC, Dr Des Hogan participated in the Future of Privacy Forum panel “Two (too?) Hard Questions for Data Protection and Generative AI” in October. Left to Right: **Bianca-Ioana M.** (Deputy Director for Global Privacy at the Future of Privacy Forum), **Dr. Gabriela Zanfir-Fortuna** (Vice President for Global Privacy at the Future of Privacy Forum), **Dr. Miriam Wimmer** (Director at the Brazilian Data Protection Authority, ANPD), **Judge Bertrand du Marais** (Commissioner for Commission Nationale de l'Informatique et des Libertés, CNIL), **Dr Des Hogan** (Commissioner for Data Protection and Chairperson of the DPC), **Haksoo Ko** (Chair of the Personal Information Protection Commission Korea, PIPC), **Jules Polonetsky** (CEO of the Future of Privacy Forum), and **David Weinkauff**, PhD (Senior IT Research Analyst at the Office of the Privacy Commissioner of Canada, OPC).

## Riot Games – Riot Voice Evaluation

In June 2024, Riot Games - an Article 27 GDPR controller - (a controller not established in the European Union) informed the DPC of its intent to launch Riot Voice Evaluation (RVE) for the game VALORANT in the EU/ EEA. Riot Games already offered live voice communication features for VALORANT in the EEA, and RVE would add recording capabilities to allow Riot to evaluate voice communications to identify harmful online behaviours by players and allow Riot to address violations of their Terms of Service. Initially, RVE would be triggered where a player was reported for bad behaviour on voice communication channels. Riot Games intended to progress to using an AI to assess the voice communications to identify and address infringements and would use the snippets of voice communications to improve the AI model. The DPC wrote to Riot with recommendations to increase the transparency to players on RVE and on Riot's proposed use of AI. The DPC recommended that Riot create a transparent, easy-to-use way for players to object to the processing prior to the rollout of RVE.

On retention periods, the documentation outlined various timelines from 24 hours to 2 years of retention for various aspects of the RVE collection and processing that was not reflected in the Privacy Notice. The DPC considered that it was not possible for players to identify such periods with any certainty from the information provided in the Privacy Notice. The DPC therefore recommended that clear retention periods or criteria to determine such periods be developed and communicated to players clearly prior to launch.

In response, Riot made significant changes to their rollout plans, enhancing transparency information to be provided to players, as well as the development of an opt out process. Riot stated that there will be no LLM (Large Language Model) training based on EU/ EEA user data in the initial launch.

## Meta Parental Supervision

The DPC engaged with Meta Platforms Ireland Limited (Meta) on a new parental supervision facility on Meta platforms such as Instagram, Facebook and Quest. The Supervision feature is an optional tool for parents and children, the purpose of which Meta states is to enhance online safety by affording parents with greater control and oversight of their pre-teen's activity in order to provide them with a safe and age appropriate experience across various Meta platforms.

The DPC recognises the need to find a balance between providing children with reasonable autonomy and ensuring effective parental supervision online. On assessing the tool the DPC made several recommendations to Meta, including considerations for inclusion of a notice on the child user information page outlining possible abuses of the parental supervision facility by non-parents and supporting a link to related support services for the child user to access. In order to provide adequate transparency to all users, the DPC recommended Meta re-evaluate the information it provided to users to ensure clear indications of what personal data of third parties is shared in order that both the child and third parties clearly understand who has access to that personal data.

In November 2024, Meta advised that it had considered the DPC's views and had implemented various changes as a result, including updating its Help Centre articles and the language in its Privacy Policy.

## Data Protection Assessment of 3rd Party Developer Access to Personal Data

The DPC completed a data protection assessment of third-party developer access to personal data. The assessment was primarily concerned with access to personal data held by Meta that is provided to third-parties as part of App developing for various Meta platforms. The Assessment reviewed the extent to which Meta had implemented appropriate technical and organisational measures under Article 25 GDPR to be able to demonstrate that processing is performed in accordance with the GDPR.

In February 2024, the DPC issued recommendations that focused on:

- the initial assessment of developers and developer's apps to include developer identification, developer verification, vetting and app review;<sup>7</sup>
- user access, permissions and end of access;
- monitoring data access and data use;
- oversight by Meta of the data access framework; and
- security.

At year's end Meta had informed that DPC that it was assessing the recommendations.

## X Grok

In July 2023, the DPC was informed that Twitter International Unlimited Company (Twitter) was working with x.AI Corp to develop a generative AI-powered tool to enhance search on the X platform. This developed into the generative AI application known as "Grok". In December 2023, Twitter provided the DPC with a Data Protection Impact Assessment and a Legitimate Impact Assessment to support its proposal to build future versions of Grok that would be trained on X user data.

Through a lengthy engagement, the DPC highlighted issues with the Twitter documentation and implementation of Grok, including:

- Transparency to users;
- Potential use of special category data

As part of the engagement and the documents the DPC reviewed, Twitter had established certain mitigations that should be in place prior to processing, particularly around transparency and providing users with the ability to opt out of their data being utilised to train Grok and other AI.

In July 2024, the DPC became aware that the mitigations Twitter had identified had not been completed prior to Twitter beginning to process X user data for training Grok. The DPC immediately asked Twitter to cease the processing, however Twitter declined.

The DPC formed the view that without the mitigations in place, and without a voluntary pause of the processing by the controller, there existed a real risk to the rights and freedoms of data subjects in the EU/ EEA and that there was an urgent need for the DPC, as Lead Supervisory Authority, to act to protect data subjects. To prevent such risks materialising, the DPC made an application to Judge Leonie Reynolds in the High Court under section 134 of the Data Protection Act 2018 on 8 August 2024, the first time such an application had been made<sup>8</sup>.

During the High Court proceedings, Twitter undertook to cease processing any EU/EEA X user data that had been collected during the period when the mitigations were not in place. Further, Twitter subsequently deleted the datasets that included that data so no further use could be made of them. In early September 2024, based on Twitter deleting the dataset and agreeing to make the undertaking permanent, the parties agreed to withdraw the proceedings from the Court.

During the relevant period, the DPC continued to receive complaints from EU/ EEA data subjects relating to the data processing at issue which fell to be considered under standard complaint handling procedures.

<sup>7</sup> For example, the DPC recommended Meta to carry out a re-evaluation of its current processes to identify Developers in order to ensure all Developers who are provided access to its platform have been adequately risk assessed.

<sup>8</sup> Section 134 of the Data Protection Act 2018 allows the DPC, where it considers there is an urgent need to act to protect the rights and freedoms of data subjects, to make an application to the High Court for an order requiring the data controller to suspend, restrict or prohibit the processing of personal data.



## Meta AI

In March 2024, Meta Platforms Ireland Limited (Meta) informed the DPC that it would be relying on legitimate interest under Article 6(1)(f) of the GDPR for training AI models with user personal data. After the DPC highlighted several concerns, Meta made changes to its roll out including:

- Users would be directly notified by Meta of the proposed change;
- Additional transparency measures would be added, including dedicated generative AI resources;
- Information on user's rights to object and a practical way for users to do so;
- Users would be provided at least 4 weeks before the training would begin to allow them to object.

In May 2024, Meta announced an update to its Privacy Policy with changes that would give effect to this. Almost immediately, the DPC began receiving reports of technical issues with the notification and objection form outlining, amongst other things, that:

- Users in some jurisdictions could not access the objection form;
- Users were unable to object in the mobile application; and
- Users who were able to successfully complete the objection form were not always told the status of their objection or were provided an error message after completing the process.

The combination of these issues led to intensive engagement between the DPC and Meta, and in June 2024, the DPC requested that Meta pause the training of AI using EU/EEA user personal data to provide time for the DPC and the DPC's peers, the European Supervisory Authorities, to evaluate the use of legitimate interest as a correct legal basis for the proposed AI training<sup>9</sup>. Meta agreed to voluntarily pause the processing, resulting in no EU/EEA user data being used for AI training<sup>9</sup>. The DPC welcomed the decision by Meta to pause its plans to train its large language model using public content shared by adults on Facebook and Instagram across the EU/EEA. The engagement with Meta was ongoing at year's end.



<sup>9</sup> During this period the DPC collaborated extensively with its EU counterparts, initiating several rapid response meetings in order to keep all authorities apprised of the latest information and the actions that the DPC was undertaking.



## AI OPINION

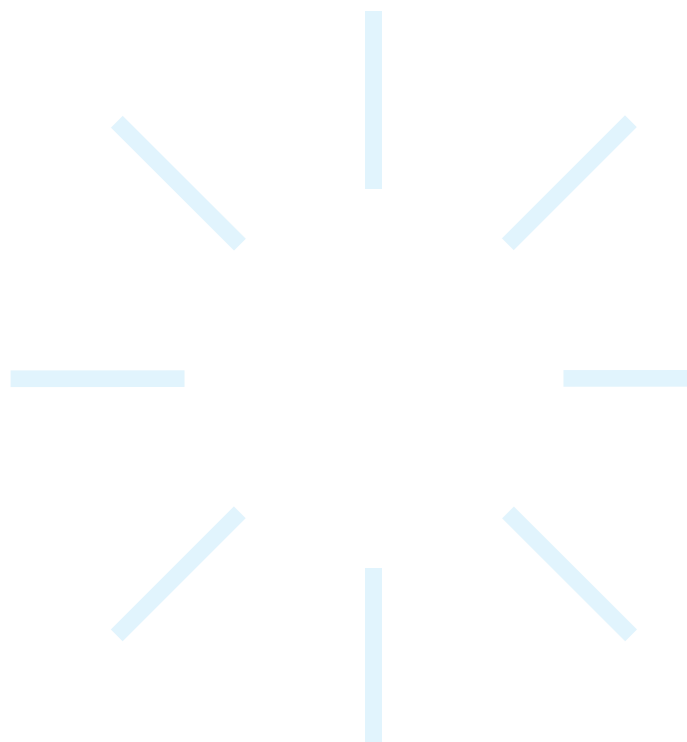
As part of its ongoing review of various proposed AI models being developed by organisations during 2024, the DPC considered that the underlying fundamental issues relating to the personal data processing that takes place in the training and operation of AI models were issues similarly faced by Supervisory Authorities across all Member States of the EU/EEA.

In early 2024, there was no established consensus on matters central to the training and operation of AI Models specifically. Fundamental questions included whether personal data used to train AI models remained personal data in the AI model or in future iterations of the model, along with questions as to how GDPR rights could be exercised by data subjects. The DPC, with its peer regulators, wished to achieve regulatory harmonisation across the EU/ EEA. Given the strategic importance of reaching regulatory consensus in this area, the DPC considered it both necessary and appropriate to refer a set of questions to the EDPB, under the statutory scheme set out under Article 64(2) of the GDPR in September 2024. The aim of the formal referral, the first undertaken by the DPC, was to achieve DPA harmonisation within a number of weeks.

The questions referred to the EDPB related largely to the determination of whether, and under what circumstances, data processed in the context of AI Models would be considered personal data. Other questions related to the suitability of Art 6(1)(f) (legitimate interests) as a legal basis for the processing. The formulation of the request and associated contributions to the development of the Opinion was a cross-functional effort within both the DPC and all Supervisory Authorities, with staff of various technical, legal and administrative roles involved through the EDPB's Technology and Key Provisions subgroups, as well as the Strategic Advisory subgroup of the EDPB engaged. The entire process, including a public consultation with industry and stakeholders was project managed by the EDPB Secretariat. A formal Opinion was adopted by the EDPB with the statutory 14 week period, in late December 2024.

The DPC expressed its gratitude to its peer Supervisory Authorities across the EU/ EEA for assigning significant resources to the deliberative processes and to the EDPB Chair and Secretariat for their stewardship of the Opinion. The clarity provided by the Opinion allowed the DPC to write to several controllers for whom it is the Lead Supervisory Authority in December 2024, drawing the opinion to their attention. This communication also reiterated certain GDPR requirements not covered by the Opinion, which must equally be addressed in the assessments required to ensure the lawful processing of personal data in an AI context, including Special Category Data and purpose processing under Article 6(4) of the GDPR.

The DPC indicated its willingness to meet with controllers to discuss the opinion and the development of AI Models, as well as their data protection assessments and implementation plans prior to launch in early 2025. The Opinion would be of assistance in providing direction on the information, assessments and documentation data controllers need to demonstrate compliance and accountability when developing AI models and bringing them to market.



## Inter-Regulatory Affairs

The European Union's new digital legislative package (including the Data Governance Act, Digital Services Act, Digital Markets Act, Data Act, and the Artificial Intelligence Act) has led to the implementation of a broad range of new regulatory obligations and structures at national and EU level. Personal data is central to the digital economy and EU data protection law is often considered to be a cornerstone of digital regulation. The continued reliance on personal data in today's economy also represents the need to protect fundamental rights, especially with the advancement and increased use of AI.

In addition to the provisions that explicitly reference data protection authorities each new Act in what is termed "the EU digital rulebook" is stated to be without prejudice to the GDPR, meaning that when the relevant competent authorities under those Acts are addressing matters pertaining to personal data, cooperation with the DPC will be necessary, whether at European Commission, EU or national regulator level.

While the DPC may not be the competent supervisory authority across all Acts, it will nonetheless have a very prominent role in providing data protection expertise and guidance to other regulators at national and EU level in the performance of their functions. As such, inter-regulatory cooperation will be essential to ensuring coherence among separate but interacting areas of regulation.

In response to these challenges, the DPC established a new function in 2024 with the creation of a "Head of Inter-Regulatory Affairs" post at Deputy Commissioner level. This new function will serve as the main operational linkage with outside agencies and will be the dedicated point of contact for other authorities to coordinate cooperation tasks.

An important part of this new function involves engagement with Ireland's Digital Regulators Group (comprising of the DPC, the Competition and Consumer Protection Commission, the Commission for Communications Regulation and An Coimisiún na Meán) in order to identify those inter-regulatory touch points across the DPC's respective remits and functions, and areas in which cooperation mechanisms may need to be established.

Inter-regulatory engagement will be a priority area for the DPC in 2025, during which time we will seek to establish new, and strengthen existing, relationships with co-regulators in Ireland and beyond.



In September 2024, Commissioner for Data Protection Des Hogan spoke on a panel for "Ethical considerations in AI development – Privacy and consumer protection implications" at the Forum for EU-US Legal-Economics Affairs, Paris. **Back** (L-R) CNIL Commissioner & Conseiller d'Etat Bertrand Du Marais, EDPS Dr. Wojciech Wiewiorowski, and ARCOM Supervision of Online Platforms Working Group President Benoit Loutrel **Front** (L-R) Commissioner Des Hogan, CJEU Justice Lucia Serena Rossi, Recent European Court of Human Rights President Robert Ragnar Spano.

---

# 7

---

## Children's Data Protection Rights





# Children's Data Protection Rights

## Children's Policy

### Data Protection Toolkit for Schools

In the course of its supervision and engagement activities in 2023 (see Annual Report 2023), the DPC identified a number of areas, which schools, as a sector, appeared to find challenging from a data protection compliance perspective. Subsequently, the DPC commenced a process of stakeholder engagement to discuss data protection concerns arising in the context of schools. The DPC met with a number of bodies and organisations in the education sector, including the Joint Managerial Board (JMB), the Professional Development Services for Teachers (Formerly PDST now OIDE) and the Limerick and Clare Education and Training Board (LCETB), in order to gain a clear picture of the specific areas, which the sector considers merit particular attention in terms of guidance. Issues such as managing subject access requests (SARs) under Article 15 of the GDPR, the exercise of children's rights and the role of parents, and data sharing with other bodies were among the topics of concern raised by stakeholders.

On foot of this engagement, in **December 2024** the DPC published a new "*Data Protection Toolkit for Schools*" resource, *Toolkit for Schools QR 1* which includes a detailed guidance document, a sample Data Protection Impact Assessment (DPIA) template, a checklist for responding to SARs, tips on what to include in a privacy policy, and a "*Frequently Asked Questions*" section, all of which are tailored

to the needs of schools as data controllers. The DPC hopes this resource will further assist schools and the wider education sector in meeting their data protection obligations.



QR 1



## Guidance

Safer Internet Day 2024 –  
*"Managing my digital footprint"*

Protecting children's personal data is one of the five strategic goals of the *DPC's 2022-2027 Regulatory Strategy* [QR 2](#). To celebrate and raise awareness for Safer Internet Day 2024, the DPC produced a *blogpost* [QR 3](#) and collaborated with WebWise (Ireland's Safer Internet Centre) to produce an *infographic* [QR 4](#) to educate young people on how to manage their "digital footprint" online. The aim of this initiative was to highlight to teens that, as we navigate the online world, we all leave traces of information behind us which, when pieced together, form an overall jigsaw or profile of our online activity.

Through this blog and infographic, young people were encouraged to pause and reflect on the amount of information they are sharing online, and to consider some of the ways they can reduce their digital footprint by following the DPC's five top tips.

[QR 2](#)[QR 3](#)[QR 4](#)

## Data Protection Webinar for Irish Play Therapy Community Association

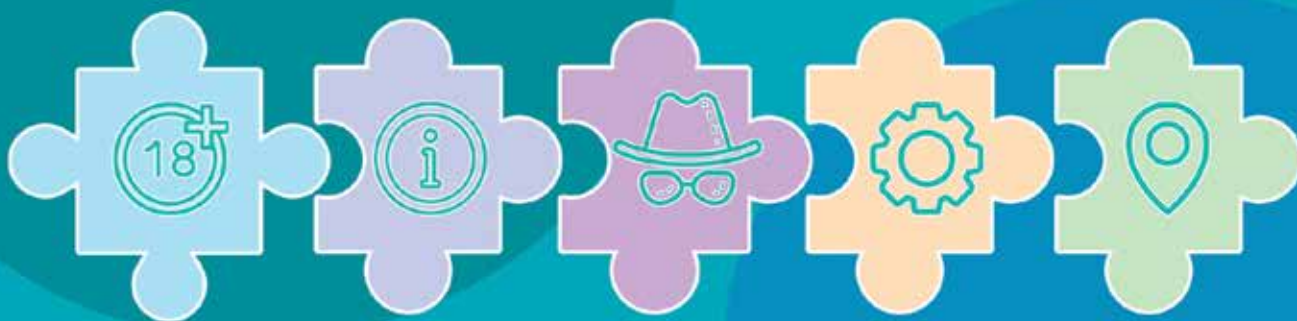
In June 2024, the DPC met with the Irish Play Therapy Community Association (IPTCA), a non-profit association for Play Therapists based in Ireland, who were seeking guidance on a number of data protection challenges that their members are experiencing. Issues such as managing subject access requests (SARs), the exercise of children's rights and the role of parents, data retention, and data sharing with other bodies were among the topics of concern raised by stakeholders.

On foot of this engagement, in October the DPC delivered a two-hour webinar which specifically addressed these issues to approximately 100 registered attendees. The webinar was structured thematically with a dedicated Q&A session after each topic, allowing participants to ask questions and share experiences, and receive answers to their queries in real time.

In order to provide further support, the DPC compiled a comprehensive document based on the questions raised during the webinar, which was circulated amongst all attendees afterwards. The feedback received was very positive, with requests for further sessions to be delivered in 2025.

# Safer Internet Day 2024

## Managing your digital footprint





## External engagements

*A spotlight on the protection of children online and age assurance*

In order to keep abreast with the latest developments and trends in the field of children's data protection, the DPC spoke at numerous external events over the course of 2024. This included panel discussions on safeguarding children and teens online (Google's "Growing Up in the Digital Age Summit"), how to strike the right balance privacy and safety for children (hosted by RAID (Regulation of AI, Internet and Data)), and age assurance in an inter-regulatory landscape hosted by the Law Society of Ireland.

The DPC also attended and participated in the Global Age Assurance Standards Summit in Manchester, a 5-day conference dedicated to the issue of age assurance. This first-of-its-kind event was attended by over 700 stakeholders, from regulators, international organisations, civil society, academia, industry, age assurance service providers, standards developers and technical experts. The DPC participated in a panel discussion entitled "Accessible Age Assurance: Building

*Transparency Into Age Assurance Solutions*", and separately delivered a workshop on how the DPC has approached its "Fundamentals for a Child-Oriented Approach to Data Processing" guidance and the impact and implications that this has for age assurance.

The DPC also recorded an episode for the "Fighting dark patterns – Regain your free will online" podcast series led by Fair Patterns, where the conversation focused on the current legal landscape for children's data protection rights in the EU, the particular dangers that "dark patterns" pose to children and the importance of transparency and education to empower children online.

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 ICO's International Age Assurance Working Group. In addition, as an active member of the Global Privacy Assembly's Digital Education Working Group, the DPC contributed to various surveys and initiatives carried out by the group on topics such as digital literacy for parents during the year.





## Engagement with statutory bodies

Throughout the course of 2024, the DPC met with several statutory bodies to discuss developments in the area of children's data protection issues, including the Office of the Australian Information Commissioner and Ireland's Coimisiún na Meán. The DPC also held meetings with its UK and French counterparts, the Commission nationale de l'informatique et des libertés (CNIL) and the Information Commissioner's Office (ICO), throughout 2024 to exchange views and discuss the latest developments in both DPAs' work on children's data protection rights. In late 2024, the DPC paid a visit to its colleagues at the CNIL in their offices in Paris to concretise plans for a joint initiative between both DPAs in 2025 on the topic of "*sharenting*", the habitual sharing by parents of information online relating to their children such as photos, videos, information and private moments.

## Codes of Conduct

The DPC continued to engage with Technology Ireland throughout 2024 on their "European Youth Online Data Protection Code of Conduct". This Code was motivated by the publication of the DPC's "Fundamentals for a Child-Oriented Approach to Data Processing", and is intended to focus on certain topics of the GDPR that are deemed particularly important to drive higher standards of protection for children's personal data online.

## Work on children's issues within the European Data Protection Board

### *Statement on Age Assurance*

The DPC's focus and dedication to the complex issue of age assurance in the digital environment also continued at an EU level throughout 2024. In March 2024, the DPC joined the drafting team for a statement being prepared by the EDPB on general data protection principles and criteria for age assurance systems. The statement, expected to be adopted in early 2025, would list ten principles for the compliant processing of personal data when determining the age or age range of an individual. The DPC is proud to have been involved in driving a consistent approach to age assurance across Europe, one which protects children's wellbeing, while also complying with data protection principles.

### *Guidelines on children's issues*

The DPC has been continuing its role as co-rapporteur in the preparation at EDPB level of guidance on children's data protection issues alongside a team of co-rapporteurs from Germany, France, Greece and Denmark. The purpose of these guidelines is to seek to achieve a harmonised approach at EU level in relation to the critical area of the processing of children's data.

---

# 8

---

## Data Protection Officers

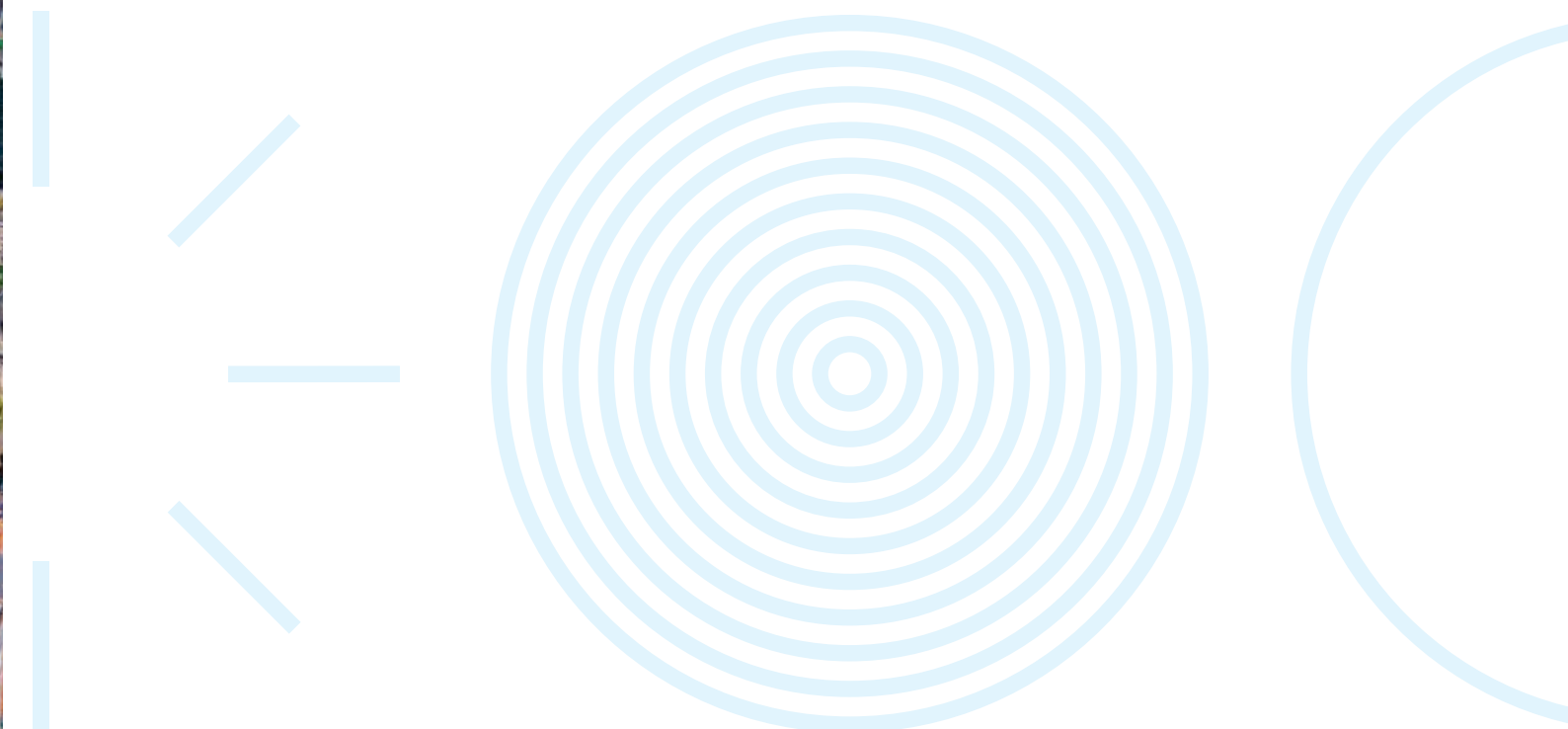


# Data Protection Officers

The role played by organisational Data Protection Officers (DPOs) is critical for the successful application of data protection law. Under Articles 37-39 GDPR, DPOs play an important role in assisting their organisations in meeting their data protection compliance obligations by advising and informing colleagues and management, and monitoring adherence to policies and procedures. In order to carry out their tasks in an effective manner, DPOs must be fully supported by their employer and allowed to act independently within the organisation, as legislation requires.

Active support of the DPO by management includes providing sufficient financial resources, infrastructure, and staff as may be required. DPOs must also be given sufficient time to carry out their tasks, in particular where the DPO may be required to carry out duties additional to their Data Protection responsibilities. A well-resourced DPO team has been demonstrated to be of great benefit to organisations in all sectors in building a culture of data protection awareness, which in turn drives compliance and reduces the risk of data breaches or other incidents occurring.

It is important to note that where a DPO has been appointed, the organisation as a data controller is obliged to support them in performing their tasks, and that failure to do so infringes the GDPR (Article 39.2). As the main point of contact within their organisation for the DPC, DPOs are an important stakeholder for the DPC and during 2024, the DPC continued to support DPOs and assist them in being more impactful in carrying out their roles.







The DPC participated in the 2023 Coordinated Enforcement Framework (CEF) Topic *“The Designation and Position of Data Protection Officers”* with the aims of:

- Helping to identify emerging issues;
- assessing the knowledge, expertise and impact of the DPOs; and
- generating deeper insights into the role at an EU level.

The DPC found three substantive issues:

- The Resources of the Data Protection Officer - 33% of respondents felt they did not have sufficient resources to fulfil the role of a DPO)
- Conflicts of Interests - 36% of respondents indicating that had additional tasks to those relating to Data protection with a substantial number pointing to tasks which did not complement the role of DPO.
- Experience - 80% of DPOs replied they have at least 3+ years of experience working on the application and the interpretation of data protection requirements.

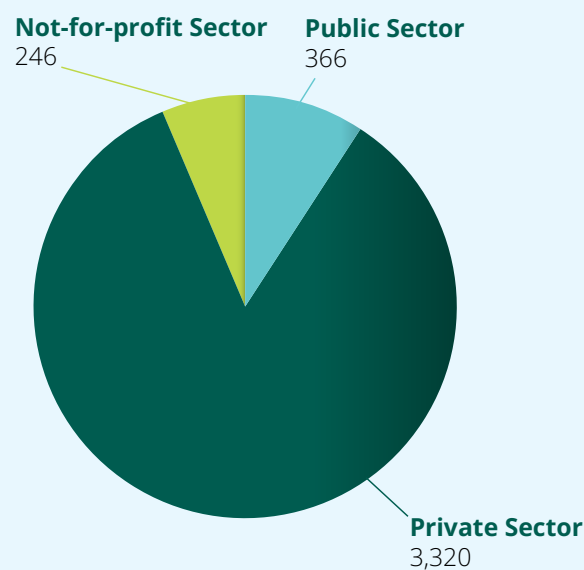
Further details on this report can be found on the EDPB website: [Coordinated Enforcement Framework QR 1](#)



QR 1

be notified of the formal designation of a DPO by an organisation. As of the end of the 2024 the DPC has been notified of the **designation of 3,932 DPO's** broken down by sector as follows:

### Notification of Data Protection Officers



As part of the requirements of GDPR, the DPC must



From left to right – Online Safety Commissioner Niamh Hodnett and Deputy Commissioner Jenny Dolan at the DPO Conference, November 2024

## DPO Supports

The development of sector-based DPO networks has been a positive feature of the implementation of GDPR in Ireland since 2018, and engagement with these groups has proven to be a valuable resource for the DPC in terms of stakeholder engagement. DPO networks provide an opportunity for colleagues to share information and practical solutions to issues arising in data protection compliance. They also connect DPOs to a wider professional network and contribute to building up the data protection and privacy community. In 2024, the DPC continued to engage with established DPO networks, and made connections with new and developing networks, across different sectors which included the following:

- The DPC participated in a conference organised by the Health Research Data Protection Network, on issues arising in the application of GDPR to health research and clinical trials.
- The DPC contributed to a training course for DPOs in the public sector, developed by the Institute for Public Administration in collaboration with the Civil Service DPO Network for the second year running.
- The DPC engaged with the International Pharmaceutical & Medical Device Privacy Consortium, discussing issues arising in the application of GDPR by the Med Tech sector in Ireland and internationally.
- The DPC participated in the annual conference of the Association of Data Protection Officers (ADPO).

In 2025, the DPC aims to expand its engagement with DPO networks, and any formal or informal groups of DPOs or privacy professionals are invited to get in touch.



From left to right – Commissioner Dale Sunderland, Professor Joyce O'Connor, Deputy Commissioner MB Donnelly, Professor Martin Curley and Commissioner Dr. Des Hogan

## DPO Conference

On 29 November 2024, the DPC hosted its DPO Network conference “Supporting DPO Success” in the Cusack Suite of Croke Park in Dublin. This conference was organised in accordance with the DPC’s commitment to championing, supporting and promoting the development of DPOs and Privacy Professionals, reinforcing a sense of community and empowerment among those working in the Data Protection sector. The day provided a networking opportunity for DPOs and Privacy Professionals, while also delivering helpful and insightful presentations on a range of topics relevant to DPOs and Privacy Professionals.

The event consisted of seven information sessions delivered by industry experts, addressing and discussing key areas of interest for DPOs and Privacy Professionals. The day’s opening session with the Commissioners focused on the power of cooperation and the DPC’s belief in the importance of supporting DPOs, setting the tone for a day centred on championing DPO success. Sessions also focused on GDPR

and Innovation, the skills required to be a DPO, examining the protection of children’s data in online spaces and offering tips on how to engage with the DPC. The event was a day of learning and successful collaboration within the DPO community.

Overall, feedback on the conference has been very positive and has highlighted a keen interest in similar events hosted by the DPC for DPOs and Privacy Professionals. The DPC DPO Network Team have made these recordings available on the [DPC website QR 2](#), as part of the resources rolling out for DPOs for 2025, alongside a planned series of informational webinars catering to the needs of DPOs and Privacy Professionals.



QR 2



---

# 9

---

## International Activities



# International Activities

## European Data Protection Board and Supervisory Bodies

Each EU Member State and EEA country<sup>10</sup> 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 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 2024, the DPC attended and actively participated at all monthly EDPB plenary meetings, as well as expert subgroup meetings (over **180** meetings in total).

<sup>10</sup> European Economic Area. The EEA includes Iceland, Liechtenstein and Norway..



In March 2024, Commissioners, Des Hogan and Dale Sunderland met with European Commissioner for Justice Didier Reynders in Brussels.

## Enhanced cooperation with other EDPB Supervisory Authorities 2024

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 in day-to day operations under the One Stop Shop (OSS) in the performance of its role as a Lead Supervisory Authority. This included responding to routine requests for information, follow up communications and actions on OSS complaints, providing updates on OSS inquiries and supervision cases.

In recognition of the importance of its international engagement work, the DPC created a “Head of EDPB/ International Affairs” post at Deputy Commissioner level in October 2024.

As part of the on-going co-operation and communication between the DPC and the other EU/EEA Supervisory Authorities in 2024, the DPC received **1,175** voluntary and formal mutual assistance requests from other European Regulators.

In 2024, the DPC submitted the following to the GDPR Article 60 cooperation process:

- **Draft Decisions 7**
- **Final Decisions 11**

Of the seven (7) Draft Article 60 Decisions, **four (4) were large scale inquiries which received no objections.** Enhanced cooperation the DPC engaged in at all levels across all functions during 2024 contributed to this outcome, 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.

In addition, the DPC submitted, through the Article 60 cooperation mechanism, **115 notifications** of amicable resolutions achieved in cross-border complaints.

As a Concerned Supervisory Authority, the DPC reviewed 112 Article 60 **Draft Decisions/ Revised Draft Decisions** and 31 Informal Consultations sent to it by peer DPAs during the year.





## European Case Handling Workshop in Tallinn, Estonia

The DPC also facilitated numerous bilateral engagement meetings with members of EDPB 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 in April and France in June;
- Participated in the European Conference of Data Protection Authorities in Riga, Latvia;
- Participated in the European Case Handling Workshop in Tallinn, Estonia;
- 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 Serbian Data Protection Authority for a study visit to the DPC;
- Welcomed a secondee from the European Data Protection Board Secretariat; and
- The DPC sent a secondee to the Dutch DPA and a secondee to the EDPB;

The DPC aimed to continue participating in the secondee programme in 2025. In addition, the DPC had one official on secondment in Brussels since October under the NEPT Secondment programme.

DPC participation in the European Case Handling Workshop in Tallinn, Estonia,

On the 5th and 6th of December 2024, four delegates from the DPC's national and cross-border complaint handling teams participated in the European Case Handling Workshop (ECHW) 2024, which took place in Tallinn, Estonia. The workshop, which was attended by EDPB members, provided a platform for DPAs to discuss case handling in their organisations and share practical knowledge and experience of cases.

During the two-day session, workshops were held on a range of topics, including the AI act and the role of DPAs, data breaches, video surveillance, Data Protection Impact Assessments, and the relationship between controllers and processors.

Representatives from the DPC hosted a workshop titled "Dealing with complex cases: social media, definition of 'personal data', special categories of personal data." The DPC gave a presentation outlining the life-cycle of a cross-border complaint handled by the DPC, which covered each stage of the process, from the initial receipt of the complaint to its resolution. The DPC highlighted in particular the key steps and coordination with other supervisory authorities involved in dealing with cross-border complaints. Articles 15 (Right of access) and 17 (Right to erasure) of the GDPR were explored in depth with the other DPAs, using detailed DPC case studies of complex cases.

The DPC presentation contributed to a beneficial discussion with other DPAs on the topic as well as an exchange of knowledge and experience of dealing with complex cases.

## Cooperation with International Supervisory Authorities 2024

Further to engagement at a European level, the DPC engaged with international supervisory authorities, including:

- Bilateral engagement with: the UK Information Commissioner's Office; Australian Privacy Commissioner; Office of the Privacy Commissioner for Bermuda; US Federal Trade Commission and the Office of the Privacy Commissioner of Canada.
- Participation at the Global Privacy Assembly in Jersey, United Kingdom.
- Participation in the British, Irish and Islands Data Protection Authorities (BIIDPA) Forum.
- Welcomed a secondee from the Office of the Privacy Commissioner for Bermuda.

In 2025 the DPC hopes to continue to expand its international engagement efforts at both European and International levels.

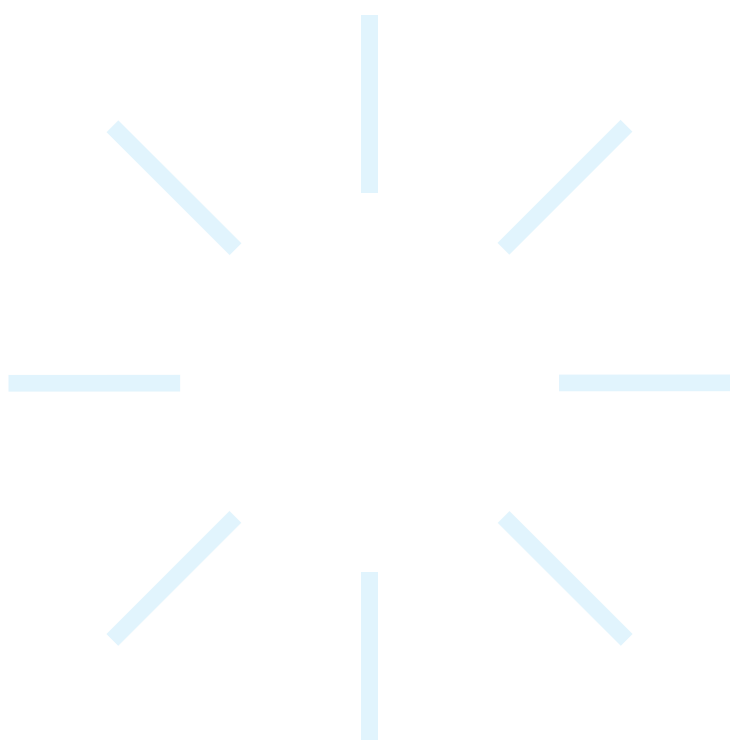
## Attaché Position – Brussels

The DPC undertook a pilot project to establish a full time Attaché in Brussels for an initial 12-month period from May 2023 to May 2024. The Attaché met regularly with key DPC stakeholders based in Brussels, including the European Commission, the European Data Protection Board and its subgroups, Members of the European Parliament, Civil Society Organisations and Data Controllers with representatives based in Brussels.

Throughout 2024, negotiations were ongoing in the European Parliament and European Council in relation to the Proposal for a Regulation to Harmonize GDPR Procedural Rules, which meant that a large amount of the engagement with the Attaché focused on this topic. Other topics of interest to Brussels based stakeholders included the DPC's Regulatory Strategy and the numerous large scale inquiries which had been completed by the DPC in 2023 and 2024. Brussels based stakeholders provided feedback to the DPC that they appreciated having a DPC presence available to them and recommended that the position be continued beyond its pilot phase. In addition to Brussels based stakeholders, the central location of Brussels facilitated DPC engagements with fellow European Data Protection Regulators on the margins of meetings or data protection related events in Brussels. The Attaché also arranged for high-level meetings between the Commissioners and prominent stakeholders during a visit to Brussels, including:

- European Commissioner for Justice;
- Head of Data Protection Unit, Directorate General Justice, European Commission;
- Chair of the European Data Protection Board;
- European Data Protection Supervisor;
- The European Consumer Organisation (BEUC); and
- European Digital Rights Network.

Following on from this successful pilot phase, the DPC decided to continue the position and will continue to develop the DPC's presence in Brussels.





Staff from Serbian Commission visits DPC

### **Study Visit - Commissioner for Information of Public Importance and Personal Data Protection in Serbia**

In September 2024, the DPC welcomed a delegation from the Commissioner for Information of Public Importance and Personal Data Protection in Serbia. This visit was part of an EU-funded project to support the Serbian Ministry of Justice in preparing for accession to the EU, managed by the German Ministry for Development.

The Commissioners welcomed the delegation and introduced the DPC staff from Legal, International Affairs and Supervision a number of units who presented on the work of the DPC.

### **Study Visit: Students of “New Media”, Copenhagen, Denmark**

In 2024, the DPC twice hosted students of “New Media” from Copenhagen, Denmark; first in April and then again in October. The DPC shared insights with the students into its remit as a regulatory body under the GDPR, as well the work the DPC undertakes in order to meet that brief. The importance of the GDPR and data protection in the context of Social Media was also discussed, which was of particular relevance to their studies.





Commissioners, Des Hogan and Dale Sunderland met with European Data Protection Board (EDPB) Chair Anu Talus in March 2024 when in Brussels.

## Certification

Certification has been a growing area for supervisory authorities across the EU in 2024.

In Ireland, the DPC is the supervisory authority responsible for approval of data protection criteria or mechanisms 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 worked closely with its EU colleagues at the European Data Protection Board (EDPB) during 2024 on the assessment of a number of national and EU certification schemes in addition to improving internal procedures and developing further guidelines for stakeholders.

There are currently two approved European Certification Schemes. A register of approved Schemes can be found on the EDPB's website: [www.edpb.europa.eu](http://www.edpb.europa.eu). Whilst no certification body 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.

Work also continued on finalising an inter-agency agreement between the DPC and Irish National Accreditation Board on accreditation of certification schemes under GDPR Articles 42 and 43 and we have held a number of productive meetings to progress matters. Following workshops held in Spain and Luxembourg in 2023, the DPC, along with its EU colleagues, formally set up channels of communication with Europe Accreditation (EA) in 2024 with the aim of understanding our respective roles under GDPR Certification and ensuring consistency and coherence in the application process throughout the EU. It is anticipated that future engagements with EA will lead to a standardised approach to certification assessments throughout Europe which can be reflected in agreements at a national level such as between the DPC and Irish National Accreditation Board.

The DPC is currently reviewing two EU Certification Schemes. It is anticipated that the DPC will be in a position to submit a Scheme to the EDPB for review in 2025.



Commissioner Des Hogan speaking at EDPS conference

## EDPB Coordinated Enforcement (CEF) 2024

The DPC participated in the 2024 Coordinated Enforcement Framework (CEF) Topic “The Implementation of the Right of Access”. EDPB members including the DPC decided to prioritise this topic as it is at the heart of data protection and one of the most frequently exercised data protection rights. 30 supervisory authorities across the EEA launched coordinated actions into the compliance of certain data controllers with the right of access under the GDPR. The DPC participated in this action as a fact-finding exercise with data controllers mainly established in Ireland. This action aligned with the DPC Regulatory Strategy 2022-27 to cooperate and communicate with peer data protection authorities on emerging issues.

The DPC contacted 30 data controllers with a view to:

- Ensuring that the right of access can be effectively exercised by data subjects and assess how controllers comply with the right of access in practice; and
- Raising awareness of the requirements applicable to the right of access. The EDPB has adopted extensive guidance on this topic, through its Guidelines 01/2022.

Following the collation of the completed questionnaires, the DPC produced an aggregated national report, which was fed into the broader EDPB report. The completed EDPB report including the DPC national report is available on the [European Data Protection Board QR 1](#).

The DPC identified three substantive issues during this exercise:

1. The responses clearly show that subject access requests account for the majority of data protection requests they received in 2023, mostly 90% of requests and upwards.
2. Some excellent examples were provided of managing SARs particularly when engaging with customers who may need assistance due to a vulnerability or difficulty. For example, controllers would treat SARs on a case-by-case basis and engage with vulnerable customer support teams were necessary, as well as seeking the assistance of appropriate external support agencies.
3. The report found mainly a high level of awareness and understanding of the EDPB Guidelines 01/2022 on the right of access. However, this was not across the board, and some respondents' level of awareness and understanding could have been better. Respondents who identified that they had proper data protection and governance units and teams across all organisation showed a better understanding of the Guidelines 01/2022.

In a consultative capacity, the DPC will engage with some respondents in this action based on the replies received. The DPC does not intend to carry out any formal investigations.



QR 1

## 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 policies 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 SA's during the co-review phase and the views of all SA's during the co-operation phase and co-ordinating and collating these responses and discussing them with the applicant to come to a draft that all SA's are satisfied with. Once this stage is reached an Opinion of the EDPB is sought under Article 64 (2) and DPC can formally approve the application once received.

### 2024 BCR

The DPC was BCR lead in relation to **16** BCR applications from **11** different companies. **Two** of those applications were submitted to the EDPB seeking an Article 64 Opinion and subsequently approved by DPC in 2024 –Processor BCR application for Accenture Global Holdings Limited (AGHL) and Controller and Processor BCR applications for Aptiv Global Operations Limited.

The DPC also assisted other European Data Protection authorities by acting as co-reviewer for another SA on **9** BCR applications.

BCR lead in relation to **16** BCR applications from **11** different companies

## 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 2024 the DPC was lead SA on **29** approved BCR for **19** different BCR holders.

## Implementation of new recommendations for controller

The EPDB updated the WP256 Referential for Controller BCR applications. It is now called "*Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR)*". Each BCR Holder using an approved Controller BCR was required make the related changes as part of their 2024 Annual Update. In 2024 this affected 17 of the already approved BCR files. The DPC issued detailed information and material to assist these BCR holders to bring their BCRs in line what was required. This was a significantly increased body of work above a normal review of an annual update. DPC has commenced its review on all of these files and completed the review of 11. The list of these approved BCR files is published on the DPC's website.

## BCR Workshop 2024

In April 2024 approximately 50 representatives from Data Protection Authorities all over the EEA met in Vilnius, Lithuania for the biennial BCR Workshop. The purpose of this workshop is the training of new colleagues starting to deal with BCR applications by more experienced colleagues sharing their knowledge. There is also a hugely important brainstorming and experience sharing element where the SA's attempt to solve case studies and address the questions that have been raised the most during assessment of BCR applications. This aids the consistency of approach but also improves the knowledge of all SA's. DPC delivered a presentation at the workshop entitled "BCR procedure: from A to Z" which was very well received.







BCR Workshop April 2024 Vilnius Lithuania

## BCR application in focus

### Aptiv Global Operations Limited

Aptiv Global Operations Limited (Aptiv) is a global technology company that designs, develops and manufactures software and hardware solutions operating in approximately 50 different countries around the world. Aptiv workforce, customer and vendor data may be dealt with by its operations based in third countries, therefore, they need to ensure they have met the conditions 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 they needed to transfer data within the group for scenarios where they acted as both a Controller and a Processor.

As Aptiv's EEA data protection compliance programme is centred in Ireland, Aptiv approached the DPC to act as BCR Lead to seek approval for their BCR. DPC assessed the application material provided to ensure the criteria required to act as Lead BCR under WP263 was being met. Once satisfied the information provided during the initial application process 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 Aptiv we could act as their BCR lead and requested the full suite of documentation.

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. 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, 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 a positive Opinion 23/2024 in November 2024 on this BCR file and DPC confirmed its approval by way of a National Decision issued to the applicant in November 2024.

---

# 10

---

Human Resources,  
Communications and  
Corporate Governance





Human Resources

Recruitment

In 2024, the Data Protection Commission (DPC) continued to invest in building organisational capability by successfully onboarding 70 new staff members across a range of grades and functions. This was achieved through a strategic and multifaceted recruitment approach that included open and confined competitions, interdepartmental mobility, and the utilisation of Publicjobs open and interdepartmental panels.

Recruitment activity throughout the year focused on ensuring the DPC has the right expertise to meet current and emerging demands. Key DPC specific competitions and appointment processes initiated or concluded in 2024 included the following roles:

- Confined Principal Officer Competition
- Higher Executive Officer (HEO) Legal Analyst
- Private Secretary to the Commissioners
- DPC Attaché to Brussels (Assistant Principal)
- Director of Legal
- Confined Executive Officer (EO) Competition

These appointments reflect the DPC’s ongoing commitment to ensuring a high-performing workforce that supports the effective delivery of its regulatory mandate.

	2024	2023	2022
New Joiners	70	44	45
Leavers	27	24	45
Internal Promotions	21	15	33

DPC total Headcount Information	2024
Date	No.
1st January 2023	196
1st January 2024	213
1st January 2025	251

Two new functional areas were created within the organisation in response to the increased remit of the DPC – with Deputy Commissioners appointed to lead in the areas of EDPB/International Affairs & AI Act and Inter-Regulatory Affairs.

Employee Engagement

During 2024, building on the DPC’s Regulatory Strategy 2022-27, the DPC’s Employee Engagement Forum commenced work on developing a DPC statement of values, which will articulate the core beliefs and principles guiding the organisation. This statement aims to establish clear expectations for employee behaviour and decision-making while fostering a sense of belonging and purpose among staff. By enhancing employees’ understanding of how their roles contribute to the broader mission of the DPC, the forum seeks to strengthen engagement.

Industrial and Employee Relations

Ongoing engagement with representative unions/ associations continued through the Departmental Council, with three meetings held throughout the year. Employee Relations support was provided to line managers and staff on a variety of issues.

Equality, Diversity & Inclusion (EDI) Committee

The EDI Committee, was established in June 2024. It is dedicated to creating an environment at work that values and capitalises on each person’s distinct viewpoints and experiences inside the DPC.

The EDI Committee will form an important part of an overall DPC People Strategy and will contribute to the DPC’s implementation of the “Workforce of the Future” pillar of the Public Service Transformation 2030 Strategy. Bespoke training for all the members of the Committee in partnership with the Irish Centre for Diversity was undertaken. During 2024, the Committee held three meetings and it will bring forward a range of initiatives throughout 2025 in line with its Terms of Reference.

## Communications

Throughout 2024, the DPC has promoted data protection awareness through effective outreach, stakeholder engagement and transparent communication. The DPC is committed to raising the public's awareness of their data protection rights and how they can control the use of their personal data.

The DPC actively engages with the media, members of the public and other stakeholders through a range of channels including; press releases, media interviews, social media campaigns, podcasts and the DPC's website, all to ensure they are kept up to date with the DPC's activities and decisions. Over the course of 2024, the DPC published a total of **26 press releases** leading to significant coverage on international and national level media. The Commissioners and members of staff contributed to over **80 speaking events** in 2024.

The DPC's social media platforms continued to play an important role in the communications of the DPC in 2024. The growth of the DPC's social media presence across X (Formerly Twitter) and LinkedIn, was integral to the support of its awareness-raising and communications activities. The combined followers across both platforms increased by over 3,700 during 2024, to over 51,800, an **increase of 7.7%** on last year's figures. There was exceptionally strong engagement of nearly 57,000 interactions, with an average engagement rate per impression of **5.65%**.

Additionally in 2024, following the completion of a project aimed at increasing website accessibility for users, the DPC received an honourable mention in the executive summary of the EU Web Accessibility Directive (EUWAD) Report 2024 published by National Disability Authority (NDA). **The accessibility score for [www.dataprotection.ie](http://www.dataprotection.ie) increased from 35.5% to 94.0% in 2024.**

**26**  
press  
releases

**80**  
speaking  
events



social media  
presence increase  
of **7.7%**

average  
engagement  
rate of **5.65%**



accessibility score for  
[www.dataprotection.ie](http://www.dataprotection.ie)  
increased from  
**35.5% to 94.0%**

### New Guidance produced by the DPC in 2024

Managing your  
Digital Footprint  
(Blog)

AI, Large Language  
Models and Data  
Protection (Blog)

Data Protection  
Toolkit for  
Schools

### DPC New Premises

The DPC received sanction from the Department of Public Expenditure, NDP Delivery and Reform for the leasing of office space at 6 Pembroke Row, Dublin 2 in 2021.

Work continued throughout 2024 to complete the build and fit-out of the DPC's new headquarters. A contract for the fit-out of the building was awarded by the OPW, with the contractor arriving on-site at the end of March 2024 and these works were to be completed by January 2025, at which point the building was to be handed over to the DPC for the final stages of fit-out.

The DPC appointed a Project Board in 2024 to oversee the transition. The Board included Senior Management from the People and Learning, Enterprise & Operations ICT, Governance Finance & Risk and Complaints Handling business units. The Project Board is supported by members of the Corporate Services and Information & Communication Technologies teams.

## Corporate Governance

### DPC Audit and Risk Committee

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 January 1 2023 and runs for three years. The members of the Committee are:

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

Four meetings of the Audit and Risk Committee were held in 2024.

### 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'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. The DPC continues to provide, and improve Irish language services with enhancements of services, as per the existing Scheme.

### 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 under this Act, as noted on the DPC website.

Interactions between lobbying bodies and Designated Public Officials must be reported by the lobbyists. The Standards in Public Office Commission (SIPO) has established an online register of lobbying at [www.Lobbying.ie](http://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

Public Sector Equality and Human Rights Duty

The DPC seeks to meet 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 below:

Postal address:  
Accessibility Officer Data Protection Commission  
6 Pembroke Row  
Dublin 2  
D02 X963  
Ireland

Email: [DPCAaccessibilityOfficer@dataprotection.ie](mailto:DPCAaccessibilityOfficer@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.

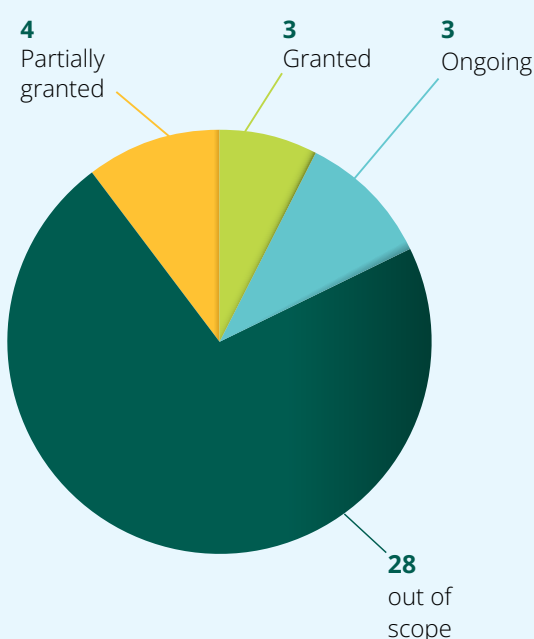
There is a designated customer service comments mailbox for customers to engage with the DPC. Any and all comments received are taken into consideration as part of the on-going review of delivering quality customer service.

### Freedom of Information (FOI)

In 2024, the DPC received a total of **39 FOI requests**.

Three were granted, four were partially granted and 28 were deemed out of scope, with four ongoing as of 31 December 2024. 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.

#### 39 FOI requests



### Parliamentary Questions (PQs)

The DPC received 28 PQs in 2024 and provided observations in response to 13 of these questions.

### Elected Representative Correspondence

The DPC received 9 pieces of correspondence from elected representatives in 2024, across all business areas.

### Access to Information on the Environment

The DPC received no requests in 2024 under the AIE Regulations.

---

## **Appendix 1:** Report on Protected Disclosures received by the Data Protection Commission in 2024

---





The policy operated by the Data Protection Commission (DPC) under the terms of the Protected Disclosures Acts 2014 and 2022 is designed to facilitate and encourage all workers to raise genuine concerns about possible internal wrongdoing in the workplace, 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.

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 1 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 2024:**

Fifty-two (52) potential protected disclosures (set out in the table 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 364/2020). Nineteen of the disclosures were accepted as valid protected disclosures.



Reference Number	Type	Date Received	Status	Outcome
01/2024	Section 7 (external, to “prescribed person”)	3 January 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
02/2024	Section 7 (external, to “prescribed person”)	12 January 2024	Closed	Not accepted as a valid protected disclosure, referred as a potential complaint.
03/2024	Section 7 (external, to “prescribed person”)	21 January 2024	Closed	Submission was not a protected disclosure. DPC not the intended authority.
04/2024	Section 7 (external, to “prescribed person”)	2 February 2024	Closed	Accepted and referred for potential investigation. Ongoing at year-end.
05/2024	Section 7 (external, to “prescribed person”)	8 February 2024	Closed	Not accepted as a valid protected disclosure, redirect to the Info Unit.

Reference Number	Type	Date Received	Status	Outcome
06/2024	Section 7 (external, to "prescribed person")	7 February 2024	Folded into pre-existing case.	The report was incorporated as a part of an existing protected disclosure case.
07/2024	Section 7 (external, to "prescribed person")	21 February 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
08/2024	Section 7 (external, to "prescribed person")	1 March 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
09/2024	Section 7 (external, to "prescribed person")	5 March 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
10/2024	Section 7 (external, to "prescribed person")	5 March 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
11/2024	Section 7 (external, to "prescribed person")	19 March 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
12/2024	Section 7 (external, to "prescribed person")	28 March 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
13/2024	Section 7 (external, to "prescribed person")	10 April 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
14/2024	Section 7 (external, to "prescribed person")	19 April 2024	Closed	Not accepted as a valid protected disclosure, redirect to the Info Unit.
15/2024	Section 7 (external, to "prescribed person")	30 April 2024	Closed	Reporting person requested that their case be closed.
16/2024	Section 7 (external, to "prescribed person")	9 May 2024	Closed	Accepted. DPC engaged with the organisation and were satisfied with their policies. Case was concluded.

Reference Number	Type	Date Received	Status	Outcome
17/2024	Section 7 (external, to "prescribed person")	27 May 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
18/2024	Section 7 (external, to "prescribed person")	24 May 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
19/2024	Section 7 (external, to "prescribed person")	10 June 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
20/2024	Section 7 (external, to "prescribed person")	6 June 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
21/2024	Section 7 (external, to "prescribed person")	26 June 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
22/2024	Section 7 (external, to "prescribed person")	24 June 2024	Closed	Not accepted as a valid protected disclosure, redirect to the Info Unit.
23/2024	Section 7 (external, to "prescribed person")	3 July 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
24/2024	Section 7 (external, to "prescribed person")	4 July 2024	Closed	Accepted. DPC engaged with the organisation and were satisfied with their policies. Case was concluded.
25/2024	Section 7 (external, to "prescribed person")	28 June 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
26/2024	Section 7 (external, to "prescribed person")	16 July 2024	Closed	Accepted. DPC engaged with the organisation and were satisfied with their policies. Case was concluded.
27/2024	Section 7 (external, to "prescribed person")	19 July 2024	Closed	Accepted. DPC engaged with the organisation and were satisfied with their policies. Case was concluded.

Reference Number	Type	Date Received	Status	Outcome
28/2024	Section 7 (external, to "prescribed person")	23 July 2024	Closed	Accepted. Case was transferred to another supervisory authority (SA). The DPC concluded the case on its end.
29/2024	Section 7 (external, to "prescribed person")	27 July 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
30/2024	Section 7 (external, to "prescribed person")	29 July 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
31/2024	Section 7 (external, to "prescribed person")	31 July 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
32/2024	Section 7 (external, to "prescribed person")	1 August 2024	Closed	Engaging with complainant at year end.
33/2024	Section 7 (external, to "prescribed person")	2 August 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
34/2024	Section 7 (external, to "prescribed person")	6 August 2024	Closed	Accepted. DPC engaged with the organisation and were satisfied with their policies. Case was concluded.
35/2024	Section 7 (external, to "prescribed person")	9 August 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
36/2024	Section 7 (external, to "prescribed person")	13 August 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
37/2024	Section 7 (external, to "prescribed person")	21 August 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
38/2024	Section 7 (external, to "prescribed person")	22 August 2024	Closed	Not accepted as a valid protected disclosure, redirect to the Info Unit.
39/2024	Section 7 (external, to "prescribed person")	3 September 2024	Closed	Reporting person requested that their case be closed.
40/2024	Section 7 (external, to "prescribed person")	11 September 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.

Reference Number	Type	Date Received	Status	Outcome
41/2024	Section 7 (external, to "prescribed person")	23 September 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
42/2024	Section 7 (external, to "prescribed person")	9 October 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
43/2024	Section 7 (external, to "prescribed person")	14 October 2024	Open	Engaging with complainant at year end.
44/2024	Section 7 (external, to "prescribed person")	4 November 2024	Closed	Not accepted as a valid protected disclosure, redirect to the Info Unit.
45/2024	Section 7 (external, to "prescribed person")	6 November 2024	Closed	Insufficient detail provided, complainant did not follow up when requested.
46/2024	Section 7 (external, to "prescribed person")	13 November 2024	Open	Engaging with complainant at year end.
47/2024	Section 7 (external, to "prescribed person")	21 November 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
48/2024	Section 7 (external, to "prescribed person")	21 November 2024	Open	Engaging with complainant at year end.
49/2024	Section 7 (external, to "prescribed person")	25 November 2024	Open	Accepted and referred for potential investigation. Ongoing at year-end.
50/2024	Section 7 (external, to "prescribed person")	28 November 2024	Open	Engaging with complainant at year end.
51/2024	Section 7 (external, to "prescribed person")	11 December 2024	Open	Engaging with complainant at year end.
52/2024	Section 7 (external, to "prescribed person")	19 December 2024	Open	Engaging with complainant at year end.



---

# Appendix 2: Report on Energy Usage at the Data Protection Commission

---



# Report on Energy Usage at the Data Protection Commission

## 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 and are participating in the “Reduce your Use” campaign for Winter 2024/25.

The DPC will be moving to a new Head Office in 2025 which will significantly improve the DPC’s energy efficiency with the closure of the 2 existing offices in Dublin. The new office has a BER rating of A3.

Over the last number of years, we have made significant progress in meeting the DPC’s energy efficiency and greenhouse gas targets across the organisation.

Office Location	% Reduction in actual consumption from 2019 base line
Fitzwilliam Sq - Electricity	22%
Satellite Office - Electricity	14%
Portarlington - Electricity	30%
Portarlington - Natural Gas	58%



### DUBLIN

#### 21 Fitzwilliam Square

The head office of the DPC was located at 21 Fitzwilliam Square, Dublin 2 during 2024. Energy consumption for the office was solely electricity, which was used for heating, lighting and equipment usage.

21 Fitzwilliam Square is a protected building and is therefore exempt from the energy rating system.

#### Satellite office

In 2024 the DPC maintained additional office space in Dublin to accommodate the increase in its staff numbers. This office was sourced by OPW and the DPC took occupancy in October 2018. This office was to be maintained until a new permanent head office was ready to facilitate the DPC’s Dublin-based staff and operations in 2025. The Office is 828 sq mts in size.

Energy consumption for the building is solely electricity, which is used for heating, lighting and equipment usage. The energy rating for the building is C2.

### PORTARLINGTON

The Portarlington office of the DPC has an area of 444 sq mts 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
<b>Dublin</b>		
Fitzwilliam Sq.	61,653 kWH	
Satellite Office	76,712 kWH	
<b>Portarlington</b>		
Portarlington Office	28,400 kWH	18,589 kWH

**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**

- 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 Satellite office.
- Introduction of Government Energy Conservation plans.
- Sensor lighting introduced in Bathrooms Portarlington Office.

**Reduction of Waste Generated**

- DPC use 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 provide General Waste and Recycling bins at stations throughout the offices.
- 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.

---

## Appendix 3: Statement of Internal Controls

---



# Appendix 3:

## Statement of Internal Controls

DPC Statement of Internal Controls The Financial Statement of the Data Protection Commission for the year 1 January 2024 to 31 December 2024 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 2024 by the Comptroller and Auditor General.



# Index

## A

**Access:** 18, 20, 21, 22, 23, 24, 29, 54, 85, 106, 113

**Access Request:** 23, 24, 54

**AI:** 2, 8, 9, 13, 18, 51, 68, 84, 85, 86, 87, 88, 92, 102, 110, 111

**Article 60:** 28, 43, 46, 48, 49, 52, 53, 54, 55, 101

**Artificial Intelligence:** 2, 9, 12, 88

## B

**Breach:** 11, 21, 22, 27, 32, 33, 37, 40, 41, 42, 43, 44, 45, 46, 48, 49, 56, 61, 64

**Breach Complaints:** 33

## C

**CCTV:** 20, 21, 29, 30, 36, 37, 39, 58, 74, 75, 82

**Cross-border:** 6, 12, 18, 28, 43, 52, 100, 101, 102

## D

**Data controller:** 24, 30, 37, 40, 41, 50, 53, 60, 68, 79, 80, 85, 95

**Decision:** 23, 28, 37, 39, 41, 43, 44, 45, 46, 47, 48, 49, 53, 54, 55, 56, 58, 63, 64, 65, 66, 67, 68, 69, 79, 86, 110

**Disclosure:** 20, 33, 115, 116, 117, 118, 119

**DPO:** 2, 9, 20, 32, 71, 95, 96, 97, 98

## E

**Electronic direct marketing:** 17, 22, 26

**Employee:** 110

**Erasure:** 22, 24

**Erasure request:** 25, 52, 53, 55

**European Union:** 38, 64, 72, 84, 88

## F

**Financial:** 32, 40, 95

## G

**Governance:** 18, 88, 109, 112

## L

**Law Enforcement Directive:** 2, 17, 22, 29, 33, 56, 74, 75, 76, 100

**LED:** 2, 17, 18, 22, 29, 33, 77, 122

## N

**Notification:** 21, 48, 86

## P

**Personal data:** 8, 9, 12, 17, 20, 21, 22, 23, 24, 25, 27, 29, 30, 33, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 61, 64, 66, 67, 68, 71, 73, 74, 76, 77, 78, 80, 81, 82, 83, 84, 85, 86, 87, 88, 91, 93, 100, 102, 111

**Processing:** 8, 17, 20, 21, 22, 23, 24, 25, 27, 29, 30, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 47, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 64, 66, 68, 71, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 84, 85, 86, 87, 93

## R

**Request:** 23, 24, 25, 52, 53, 54, 55, 74, 76, 83, 87

**Resolution:** 20, 25, 28, 33, 102

**Right:** 22, 24, 84, 102, 106

**Rights:** 17, 23, 38, 88, 89, 90, 91, 92, 93, 103, 113

## T

**Transparency:** 38, 44, 47, 52, 53, 56, 75, 78, 80, 84, 85, 86, 92, 112

# Notes

# Notes