An Coimisiún um Chosaint Sonraí
Data Protection Commission

Annual Report 2023

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

Contents

Foreword

2023 was a busy year in personal data rights protection. The year saw a significant increase in complaints dealt with by the Data Protection Commission ("DPC") with record fines issued and corrective orders imposed following cross-border and national inquiries. More generally, there were a large number of data protection-related judgments from the Court of Justice of the European Union and continued domestic focus before the Irish courts.

This annual report sets out the breadth of work undertaken by the DPC throughout 2023. Detailed case studies throughout the report set out the range of organisations dealt with. From property and financial companies, to real estate agencies, schools and education providers, health care organisations, public sector agencies, employers and prospective employers, bookmakers, energy providers, insurance companies, restaurants, charities and social media companies, organisations use and process people's personal data every day, often in complex and not easily understood ways. Throughout 2023, the DPC sought to defend the individual's right to the proper protection of their personal data through fair and proportionate regulation, in line with the applicable legal frameworks and continuously evolving case law.

Cross Border Inquiries and Enforcement

In addition to detailing several national inquiries concluded, the report describes how the DPC worked with its peer European Data Protection regulators under the GDPR on large scale inquiries and, more generally, in guidance and standard setting through the work of the European Data Protection Board. The DPC had 89 statutory inquiries on-hand during the year, including 51 cross-border inquiries. Several large-scale inquiries concluded with the DPC delivering **87%**[1] of all GDPR enforcement fines across the EU (as measured by monetary fines).

1) **DLA Piper GDPR Fines and Data Breach Survey 2024 - -** https://www.dlapiper.com/en/insights/publica-tions/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024

The DPC also undertook a number of successful prosecutions under the ePrivacy Regulations, which addressed unsolicited marketing messages.

Of note in 2023 was the conclusion of the DPC's investigation into the lawfulness of Meta's transfers of personal data from the EU to the USA, and the DPC's investigation in relation to TikTok and child users. As the DPC is the EU Lead Supervisory Authority in cases where a company has its sole or main establishment in Ireland the DPC led these investigations, which proceeded in conjunction with fellow EU regulators under the GDPR's cooperation and consistency mechanisms. Final decisions in these cases were adopted in May (Meta) and September (TikTok) 2023, imposing fines of €1.2bn and €345m respectively. A feature of this regulation has seen the companies concerned bring multiple concurrent sets of legal proceedings before the Irish High Court and the European Courts challenging the outcome of DPC inquiries and the process by which they were concluded.

Engagement and supervision

A large focus of the DPC is providing guidance to organisations and companies under its Supervision function. Priority areas of focus in 2023 included protection of children's data rights and the rights of vulnerable persons under the DPC's Regulatory Strategy 2022-27. Safeguarding data protection rights saw the DPC providing support and engagement with various sectors from restaurants to sporting organisations, non-governmental organisations, technology multinationals, law enforcement agencies, schools and public sector bodies.

Under our engagement and supervision functions, the DPC met with representative bodies on a number of occasions to work through how the application of the risk and principled-based approach of GDPR might work in practice. The DPC offers guidance and recommendations to groups and organisations on the best approach and the DPC telephone helpline operates a daily service to assist the public on this and other matters.

Through engagement, the DPC addressed the non-sharing of important information between care agencies where GDPR was cited as a reason for not sharing information. The GDPR permits organisations to lawfully share information (process data) where the life or safety (vital interests) of an individual is concerned - whether in a care or other setting. During the year, the DPC worked to support NGOs providing services to vulnerable individuals and this engagement will continue.

The DPC regularly engages with companies on new products and how to address data protection issues which may arise, including children's data protection rights. In early 2023, the DPC produced four short guides for parents on children's data protection rights under the GDPR. These guides are to help parents understand their children's rights and to answer questions that can arise in typical situations where those rights apply.

Legislation and approvals

The DPC provided input and observations on over 37 pieces of proposed legislation, was the lead regulator in relation to 22 applications for Binding Corporate Rules approval from 14 different companies and worked on a number of draft codes of practice including three codes developed under the Circular Economy and Miscellaneous Provisions Act 2022. This legislation was introduced to provide a clear legal basis for local authorities to use recording devices such as CCTV and body-worn cameras for the prevention, investigation, detection, and prosecution of litter and waste management offences.

CCTV

The report highlights instances where CCTV or other surveillance of individuals occurred in both the public and private spheres. During the year enforcement action was taken against some local authorities and companies where individuals' data was processed by CCTV without a lawful basis. At the heart of GDPR is the principle of do no harm – translated in the principles of proportionality and necessity, data minimisation, purpose limitation and subsequent erasure when personal data is no longer required for the purpose collected. Organisations who collect CCTV footage must have a clear justification and lawful basis to do so. Subsequent sharing of that information/ imagery similarly requires a clear lawful basis. One example highlighted in the report is the periodic use of CCTV in restrooms, whether in restaurants or schools. As restrooms are areas where a high level of privacy is expected by individuals, a strong evidence-based justification will be required for any recording and use of CCTV images or footage.

Data Protection Officers

This report raises the important role of Data Protection Officers in organisations. In all public bodies and many private companies, the Data Protection Officer (DPO) plays a critical role in championing individuals' privacy rights by ensuring the organisation fully considers how the processing of its employees and customers' data meets its legal obligations to vindicate individual rights, acting as a "critical friend" to those organisations by keeping the compliance conversation front and centre. The DPO role is supported by good data governance practices and support staff in organisations. They also play an important role in dealing with minor data breaches and notifying serious data breaches to the DPC. Breach notifications to the DPC increased in 2023. With regular access to senior management, DPOs have an independent role in gatekeeping data protection standards in organisations. In 2023 the DPC worked with DPO networks and facilitated both public sector and a national peer to peer DPO network for private and public bodies alike. This work will deepen in the years to come.

Sad goodbyes

2023 was also a year in which the DPC said goodbye to two people who were integral to the work of the office over the last number of years. In September, the untimely passing of Bride Rosney deprived the DPC's Audit and Risk Committee of a most capable voice and inquiring mind. Bride was an active member of the DPC's ARC since its inception and we were fortunate to have benefitted from her knowledge and guidance. Then in November an esteemed colleague and serving member of staff at the DPC, Kathleen Malone, passed away suddenly to the great shock and dismay of her colleagues. Kathleen's exceptional contribution, work ethic and expertise are missed by all of us at the DPC. We take the opportunity to remember them both and to extend the condolences of the DPC to both Bride and Kathleen's families.

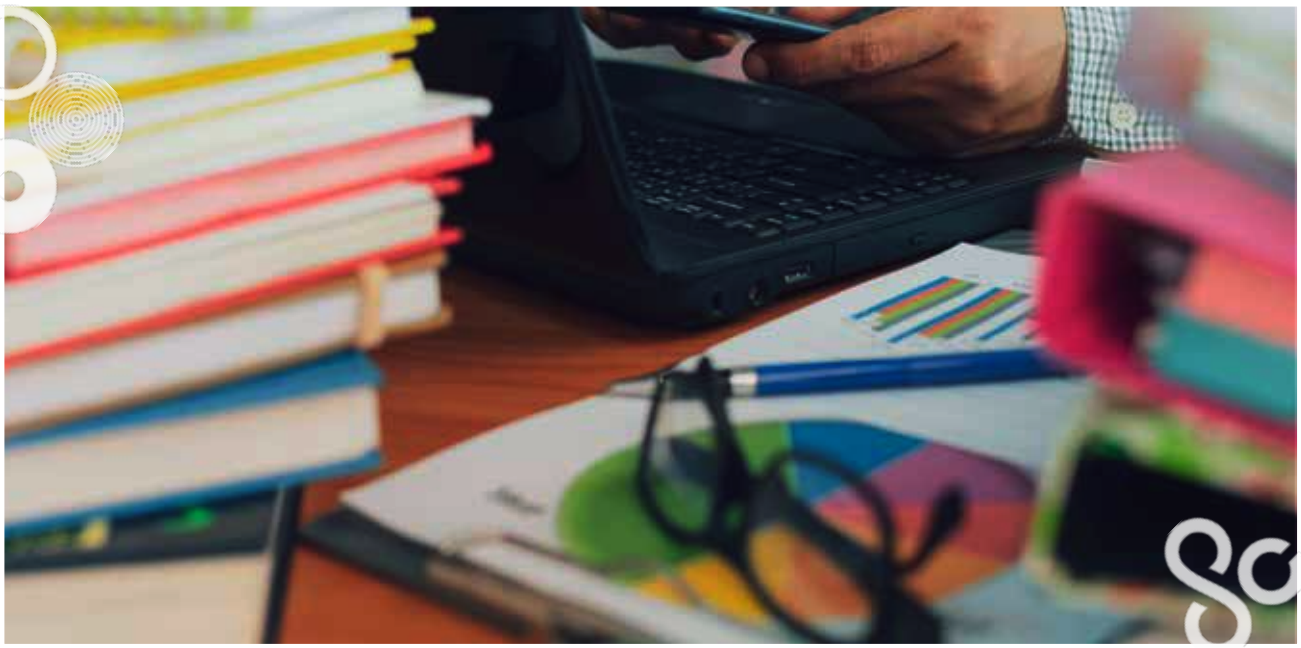
Commissioner Dale Sunderland and Commissioner Chair Dr. Des Hogan.

Changing of the guard

The DPC's activities in 2023 took place under the leadership of Helen Dixon, who was sole Commissioner for Data Protection during the year ahead of the conclusion of her second five-year term in early 2024. The work detailed in this report occurred under Commissioner Dixon's tenure and with my fellow Commissioner, Dale Sunderland, I take the opportunity to acknowledge with deep gratitude the stewardship of the Commission over the past ten years by Commissioner Dixon. In 2023, the Public Appointments Commission, on behalf of the Irish Government, oversaw an independent, open recruitment process to appoint new commissioners to the DPC. That process concluded in early 2024 with the appointment by Government of Dale Sunderland and I to the roles of Commissioners for Data Protection.

We take over a respected and outward looking regulator; one with the values of vindicating the rights of the individual through fair and proportionate regulation in the years to come.

Dr Des Hogan
Chairperson, Commissioner for Data Protection

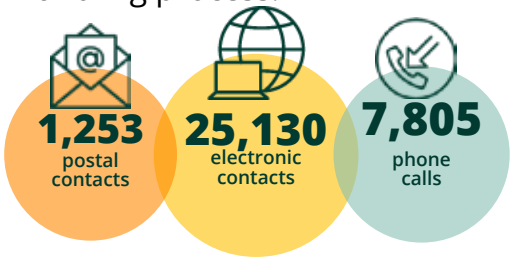


Executive Summary

Supporting Individuals

From 1 January 2023 to 31 December 2023:

- The DPC received **25,130** electronic contacts[2], **7,085** phone calls and **1,253** postal contacts ;
- The DPC processed **11,200** new cases[3] in 2023. This represents a **20%** increase on the 9,370 figure for 2022.
- Of the **11,200** new cases, 8,600 were of a type that could be dealt with relatively expeditiously and 2,600 progressed to the complaint-handling process.



- In addition to receiving 11,200 new cases, the DPC concluded **11,147** cases in 2023, of which **3,218** were resolved through the formal complaint-handling process. This figure includes complaints received prior to 2023.

In 2023, the most frequent GDPR topics for queries and complaints continued to be:

- Access Requests;
- Fair-processing;
- Disclosure;
- Direct Marketing; and
- Right to Erasure.

2) Electronic communications comprise both emails to the DPC's info@ account and webforms submitted through the DPC website.
3) Cases are defined as contacts that require further engagement beyond the initial query. Cases in this instance can therefore include complaints from individuals, but also encompasses requests for advice and guidance which do not have a complaint element. The figure does not include contacts from the media, speaking invitations, breach notifications or prior consultation.

Supporting Industry

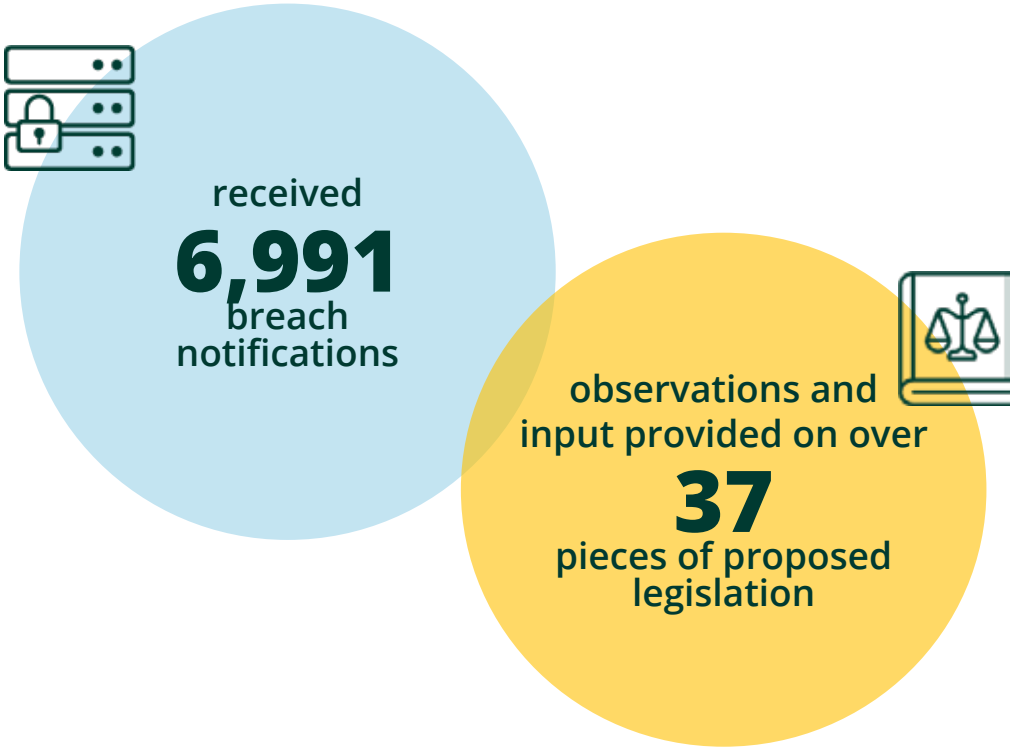
- Total valid breach notifications received in 2023 was **6,991**. This represents a **20% increase** on the 5,828 breaches notified in 2022.
- Of those breach notifications received in 2023, **92%** were concluded by year end.

The most frequent cause of breaches reported to the DPC arose as a result of correspondence inadvertently being misdirected to the wrong recipients, at **52%** of the overall total.

Regulating through Supervision and Investigation

During 2023 the DPC provided input and observations on over **37** pieces of proposed legislation.

Carried out a statutory consultation on the Codes of Practice introduced under the **Circular Economy and Miscellaneous Provisions Act 2022**, which will provide a clear legal basis for Local Authorities to use recording devices such as **CCTV and Body-worn Cameras** for the prevention, investigation, detection, and prosecution of litter and waste management offences. This will ensure that Local Authorities can deploy these technologies in a targeted and proportionate manner, in compliance with data protection law.



Expanded on stakeholder engagement across the fields of **health and social care** to provide assistance and guidance on issues arising in the processing of the personal data of vulnerable persons. As part of this multi-faceted approach, the DPC contributed to a report by the **Law Reform Commission** on the national regulatory framework for adult safeguarding.

The DPC was leading reviewing supervisory authority (SA) in relation to **22 Binding Corporate Rules (BCR) applications** from 14 different companies. **Four of those applications were given approval in 2023**. The DPC assisted other European Data Protection authorities by acting as co-reviewer for another SA on 5 BCR applications and acted as rapporteur on drafting teams for Article 64 Opinions on 3 BCR in 2023.

Multi-Tech Supervision had 100 engagement meetings with various Tech Companies and other Supervisory Authorities in 2023 and brought about the **postponement or revision of four scheduled internet platform projects** with implications for the data protection rights and freedoms of individuals.

2023 saw a significant increase in the number of queries received relating to the use of **CCTV in areas where there is a higher expectation of privacy**. As a result, the DPC published a detailed update of its **CCTV guidance** to address these issues and our expectations on the use of CCTV in such areas and wrote to a number of data controllers and sectoral representative bodies to make them aware of these developments.

As of 31 December 2023, the DPC had **89 Statutory Inquiries on-hand**, including 51 Cross-Border Inquiries.

In May, the DPC announced the conclusion to a GDPR inquiry into **Meta Platforms Ireland Limited concerning Data Transfers**. The Decision was subject to an Article 65 European Data Protection Board Dispute Resolution Process, after which the DPC imposed a fine of **€1.2 billion** on Meta Ireland, in addition to an order to bring its processing operations into compliance.

In September, the DPC issued its final Decision in its inquiry into **TikTok Technology Limited**. The inquiry examined the processing of **personal data relating to children** by TikTok. The Decision was subject to an Article 65 European Data Protection Board Dispute Resolution Process, after which the DPC ordered TikTok to bring its processing into compliance and imposed fines totalling **€345 million**.

By the end of 2023, following adoption of its decisions, the DPC imposed fines totalling **€1.55 billion**.

In 2023, the DPC concluded **13 inquiries**; issued **24 Preliminary Draft Decisions** to complainants and regulated entities in advance of finalisation, sent forward **18 Draft Decisions** to the Article 60 co-decision making process; referred **2 Decisions** to the European Data Protection Board's Article 65 Dispute Resolution Mechanism; **issued 12 Finalised Decisions** in 2023; and sought submissions on statements of issues or inquiry reports from relevant parties in a further **3 inquiries**. In addition the DPC submitted through the Article 60 cooperation mechanism **229 notifications of amicable resolutions** achieved in cross-border complaints.

Inquiries and related Enforcement Action that concluded in 2023

In 2023 the DPC concluded the following inquiries under the GDPR and the Data Protection Act 2018.

Organisations	Decision Issued	Fine Imposed	Corrective Measure Imposed
WhatsApp Ireland Ltd	January 2023	€5.5 million	Order re: Articles 5(1)(a) and 6(1) GDPR.
Kildare County Council	January 2023	€50,000	Temporary ban on CCTV cameras at a number of locations. Order re: Articles 5(1)(a), 6(1), 13, and 32(1) GDPR. Sections 71, 72, 76, 78, and 82 Data Protection Act 2018.
Airbnb Ireland UC	January 2023	N/A	No infringement found.
Centric Health	February 2023	€460,000	Reprimand re: Articles 5(1)(f), 5(2) and 32(1) GDPR.
Bank of Ireland	February 2023	€750,000	Reprimand re: Articles 5(1)(f) and 32(1) GDPR. Order re: Articles 5(1)(f) and 32(1) GDPR.
Archbishop of Dublin	February 2023	N/A	Order re: Article 5(1)(a) GDPR.
Meta (Facebook)	May 2023	€1.2 billion	Suspension of data flows re: Article 46 GPDR. Order re: Article 46 GDPR.
Department of Health	16 June 2023	€22,500	Ban re Articles 5(1)(c), 6(1), 6(4), and 9(1) GDPR. Reprimand re Articles 5(1)(c), 5(1)(f), 6(1), 6(4), and 32(1) GDPR.
Airbnb Ireland UC	June 2023	N/A	No infringement found.
Airbnb Ireland UC	June 2023	N/A	Reprimand re Articles 5(1)(c) and 5(1)(e). Order re Articles 5(1)(c) and 5(1)(e).

Organisations	Decision Issued	Fine Imposed	Corrective Measure Imposed
Airbnb Ireland UC	July 2023	N/A	Reprimand re: Articles 5(1)(c), 6(1)(f), 15(1), 12(1) and 12(3). Order re: Article 12(1).
Galway County Council	August 2023	N/A	Temporary ban on CCTV cameras and ANPR at a number of locations. Temporary ban on use of body worn cameras. Order re: Article 35 GDPR and Sections 71, 72, 76, 78, 82, 90(1) Data Protection Act 2018. Reprimand re: Article 24 GDPR.
TikTok	September 2023	€345 million	Reprimand re: Articles 5(1)(a), 5(1)(c), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) GDPR. Order re: Articles 5(1)(a), 5(1)(c), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) GDPR .
Airbnb Ireland UC	September 2023	N/A	Reprimand re: Article 12(4).
Airbnb Ireland UC	September 2023	N/A	Reprimand re: Articles 6(1)(f), 5(1)(c) and 5(1)(e). Orders re: Articles 5(1)(c) and 5(1)(e).
Airbnb Ireland UC	September 2023	N/A	Reprimand re: Articles 6(1)(f) and 5(1)(c). Order re: Article 6(1)(f) and 5(1)(c).
Apple Distribution International Limited	November 2023	N/A	No infringement found.
Microsoft Operations Ireland Limited	November 2023	N/A	Reprimand re: Articles 12(4) and 17. Order re: Article 12(4) and Article 17.
Meta (Facebook and Instagram)	November 2023	N/A	Ban on processing personal data for behavioural advertising purposes on the basis of Article 6(1)(b) or (f) GDPR.

Confirmation of Administrative Fines

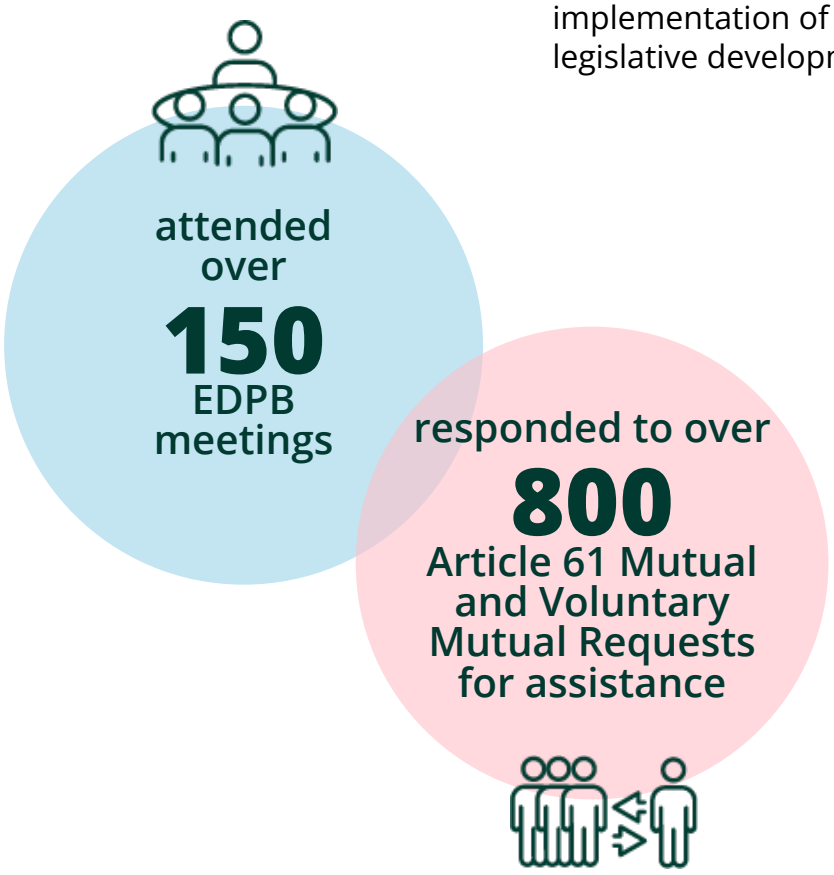
In 2023, the DPC had its Decisions to impose administrative fines on five different organisations confirmed in the Dublin Circuit Court, ranging between €15,000 and €750,000. On collection, fines are transferred to the central exchequer in Ireland.

- VIEC t/a Virtue Eldercare – (€100,000)
- A&G Couriers t/a Fastway Couriers – (€15,000)
- Kildare County Council – (€50,000)
- Centric Health – (€460,000)
- Bank of Ireland – (€750,000)

Engaging with Fellow Regulators

Since 1 January 2023, the DPC:

- Responded to over **800** GDPR Article 61 Mutual and Voluntary Mutual Requests for assistance from other European Regulators;
- Participated in over **150 European Data Protection Board (EDPB) meetings**, which were conducted both virtually and in-person;
- Continued to have representatives on all EDPB subgroups; and
- The DPC continued to be an active member of Ireland's Digital Regulator's Group, along with ComReg, the Competition and Consumer Protection Commission and Coimisiún na Meán (formerly the Broadcasting Authority of Ireland) as part of Ireland's implementation of recent EU digital legislative developments.



Mainstreaming Data Protection

Staff of the DPC presented at **120 speaking events** in 2023 , comprising a combination of both virtual and in-person seminars.

The DPC remains committed to driving awareness of data protection rights and responsibilities.

The DPC's website serves as a central hub for data protection information, providing individuals with comprehensive guidance on a variety of topics, such as understanding data protection laws, exercising data protection rights, and reporting data breaches. In 2023, the DPC, produced **five** pieces of substantial new guidance[4] (including four specifically tailored towards children), two infographics, and **12** new case studies[5] for the DPC website throughout the course of the year.

Other Activity

In 2023 the DPC:

- Concluded **237** electronic direct marketing investigations;
- **Prosecuted four companies** for the sending of unsolicited marketing communications without consent (Regulation 13 of Statutory Instrument 336 of 2011) to individuals. The Court returned convictions on all charges and it imposed fines totalling €2,000;
- **Received 26 and concluded 37 Law Enforcement Directive complaints**;

4) https://www.dataprotection.ie/en/dpc-guidance
5) https://www.dataprotection.ie/en/dpc-guidance/case-studies

Mission

Upholding the consistent application of data protection law through engagement, supervision and enforcement, and driving compliance with data protection legislation.

The Data Protection Commission 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 Data Protection Commission 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 Data Protection Commission 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
- ✓ Results-driven

Regulatory Strategy

In December 2021, the DPC published its Regulatory Strategy for 2022-2027, which is the roadmap for the DPC through a period of transformative change.

The DPC has set out an ambitious vision for what it believes will be five crucial years in the evolution of data protection law, regulation and culture.

The Strategy – and the work agenda that flows from it – has been based around five interconnected pillars of equal priority.

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

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

Roles and Responsibilities

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 core functions of the DPC, under the GDPR and the Data Protection Act 2018 — which gives further effect to the GDPR in Ireland — 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; and**
- **co-operating with data protection authorities in other EU member states on issues, involving cross-border processing.**

The DPC also acts as supervisory authority for personal-data processing under several additional legal frameworks. These include the **Law Enforcement Directive** (Directive 2016/680, as transposed in Ireland under the **Data Protection Act 2018**) which 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 DPC also performs certain supervisory and enforcement functions in relation to the processing of personal data in the context of electronic communications under the **e-Privacy Regulations** (S.I. No. 336 of 2011).

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

In addition to specific data protection legislation, there are in the region of 20 more pieces of legislation, spanning a variety of sectoral areas, concerning the processing of personal data, where the DPC must perform a particular supervisory function assigned to it under that legislation.

DPC's Senior Team

In 2023, the DPC's Senior Management Committee (SMC) comprised the Commissioner for Data Protection, two Directors/Deputy Commissioners and seven other Deputy Commissioners. The Commissioner and members of the SMC oversee the proper management and governance of the organisation, in line with the principles set out in the Corporate Governance Standard for the Civil Service (2015). The SMC has a formal schedule of matters for consideration and decision, as appropriate, to ensure effective oversight and control of the organisation.

During 2023, the SMC comprised of:

- Helen Dixon, Commissioner for Data Protection;
- Ian Chambers, Deputy Commissioner, Head of Regulatory Activity;
- Tony Delaney, Deputy Commissioner, Head of Regulatory Activity;
- MB Donnelly, Deputy Commissioner, Head of Strategy, Governance, Finance, and Risk;
- Graham Doyle, Deputy Commissioner, Head of Corporate Affairs, People and Learning, Media and Communications;
- Cian O'Brien, Director and Deputy Commissioner with responsibility for Large-Scale Inquiries and Investigations;
- Ultan O'Carroll, Deputy Commissioner, Head of Technology, Operational and Performance;
- Fleur O'Shea, Deputy Commissioner, Head of Legal Affairs;

- Sandra Skehan, Deputy Commissioner, Head of Regulatory Activity ; and
- Dale Sunderland, Director and Deputy Commissioner with responsibility for Regulatory Consultation, Supervision, Guidance and International Affairs.

In February 2024, the Minister for Justice, Helen McEntee TD, announced the appointment by Government of two new Data Protection Commissioners, Dr. Des Hogan and Mr. Dale Sunderland following the end of tenure of the outgoing Commissioner, Ms. Helen Dixon, whose term in office came to an end on 19 February 2024.

Funding and Administration – Vote 44

The DPC is funded entirely by the Exchequer. The Commissioner for Data Protection is the Accounting Officer for the Commission's Vote, Vote 44. The Data Protection Commission was voted a budgetary allocation of €26.364M of which €17.100M was allocated for pay related expenditure, and €9.264M of which was allocated to non-pay expenditure. The funding for 2023 represented an increase of €3.1M on the 2022 allocation.

DPC Senior Management Committee, December 2023.
Back row L-R: Ian Chambers, Dale Sunderland, Graham Doyle.
Middle row L-R: Sandra Skehan, Ultan O'Carroll, Fleur O'Shea, Cian O'Brien.
Front row L-R: Tony Delaney, Helen Dixon, MB Donnelly.

Contacts, Queries & Complaints

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

Contacts/Queries

Between 1 January 2023 and 31 December 2023:

The DPC received **25,130** electronic contacts[6], **7,085** phone calls and **1,253** postal contacts, an increase of 18%, 3% and 12% on the respective 2022 figures.

Complaints

During the same period, the DPC received **11,200** new cases[7]. **2,600** of which progressed to the formal complaint-handling process, including 230 electronic direct marketing complaints. The total number of cases received is an increase of **20%** on the 2022 total, and the most cases received by the DPC in any year since the GDPR took effect.

Overall, the DPC concluded **3,218** complaints in 2023, including **1,756** complaints received prior to 2023.

Upon receipt of a concern raised by an individual, it is 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, as it may rest in the jurisdiction of another data protection regulator.

6) Electronic communications comprise both emails to the DPC's info@ account and webforms submitted through the DPC website.
7) 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.

Complaints Received under the GDPR – Top 5 Issues in 2023	No	% of total
Access Request	1014	39
Right to erasure	374	14
Fair Processing	348	13
Direct Marketing	323	12
Disclosure	121	5

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;

d. S.I. 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011.

Article 57(1)(f) of the GDPR mandates the DPC to handle complaints 'to the extent appropriate' depending on 'the subject matter of the complaint'. Under section 109(1) of the 2018 Act, "the Commission shall examine the complaint and shall, in accordance with this section, take such action in respect of it as the Commission, having regard to the nature and circumstances, considers appropriate."

Accordingly, once a concern has been assessed as a complaint and progresses to a complaint handling unit, the examination is conducted in accordance with the legislative requirements.

Amicable Resolution

Fundamental to the DPC's complaint-handing obligations is the vindication of the human rights of data subjects. In the DPC's experience, the majority of individuals are satisfied when the behaviour of the data controller complained about is addressed. This can be achieved through the amicable resolution process.

As part of the complaint handling process, under the Data Protection Act 2018, the DPC must consider whether a complaint can be amicably resolved within a reasonable period. Where the DPC considers there is a reasonable likelihood of the parties to a complaint reaching an amicable resolution within a reasonable timeframe, it will take steps as it considers appropriate to arrange or facilitate the amicable resolution of the complaint.

There are many ways in which a complaint might be amicably resolved. For example, in some cases, this could involve the satisfaction of the data subject right that the complainant might have attempted to "exercise" a change in processing practises or a complaint might also be resolved through the clarification of an issue to the satisfaction of both parties.

In the DPC's experience, a high proportion of complaints it handles are amenable to being amicably resolved in a timely fashion.

The most common complaints concluded via amicable resolution relate to data controllers not responding to access requests, or failure to adequately meet their GDPR obligations in respect of customers.

Access Rights Complaints

Article 15 of the GDPR provides that an individual may obtain from a data controller confirmation of whether or not personal data concerning them are being processed and, where that is the case, access to a copy of their information. This is an important right and one which gives rise to the largest number of complaints to the DPC annually. The right of access is one of the fundamental rights conferred on individuals by the GDPR.

By the end of 2023, the DPC had received **1,014** new access complaints and concluded **1,120**.

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 or any other action the DPC considers appropriate. 2023 saw an addition to this section of the Data Protection Acts allowing the DPC to issue reprimands outside of the inquiry process.

In 2023, the complaint handling units concluded **3,218** cases through the amicable resolution process or by utilising the actions specified in section 109 of the 2018 Act.

Enforcement

As necessary, the DPC utilises its powers of enforcement against an organisation when it becomes apparent that it is failing in its obligations under the data protection legislation. The most common example is where a data controller does not engage at all with either the individual or the DPC, thus frustrating both the individual's right to exercise their data protection rights, and the DPC's legal obligation to examine such allegations of infringements.

In 2023, the DPC issued three enforcement notices to a General Practitioner and organisations associated with a boutique hotel, in line with section 109(5)(d)(i), for the noncompliance with Article 15 (subject access request) and finalised the process in relation to a further notice that issued in Q4 of 2022. Where an organisation does not comply with an enforcement order the DPC will enforce these to the extent possible in order to ensure compliance with data protection legislation.

Complaint case studies can be found in "Appendix 4" of this report.

Assistant Commissioner Jenny Dolan and guest speaker Niamh Hodnett, Online Safety Commissioner, Coimisiún na Meán.
DPC staff day, October 2023.

Electronic Direct Marketing Complaints

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

The DPC received **230 new complaints** in relation to electronic direct marketing in 2023.

A total of **237 electronic direct marketing investigations** were concluded in 2023. This figure comprises:

- 1 complaint from 2021;
- 47 complaints from 2022; and
- 189 complaints from 2023.

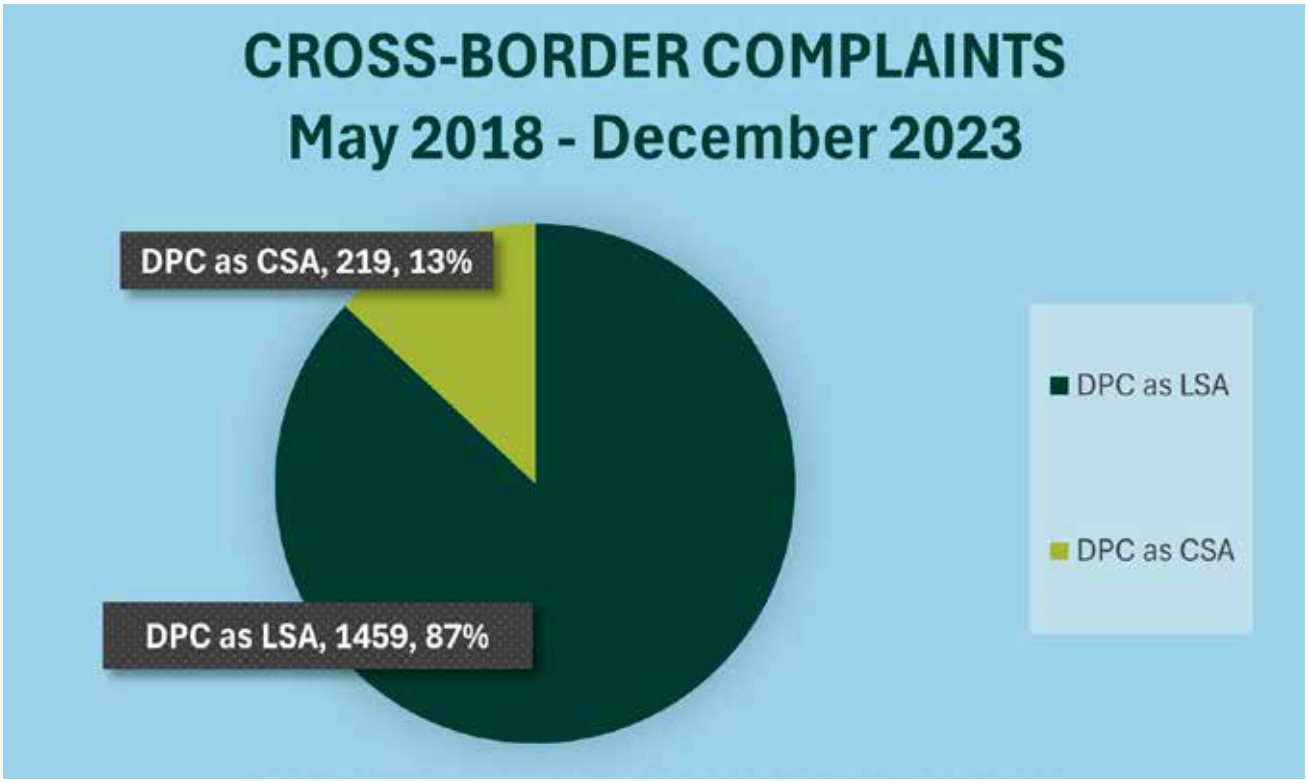
In 2023, the DPC **prosecuted four companies** for the sending of unsolicited marketing communications without consent (Regulation 13 of Statutory Instrument 336 of 2011) to individuals. The Court returned convictions on all charges and it imposed fines totalling €2,000.

Case studies detailing these prosecutions can be found in "Appendix 4" of this report.

One-Stop-Shop Complaints

The One-Stop-Shop mechanism (OSS) was established under the GDPR with the objective of streamlining how organisations that do 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 **1,678 cross border complaints**, for which the DPC has been established as the Lead Supervisory Authority for **1,459 (87%)**.

82.5% of the 1,459 valid cross-border complaints, for which the DPC is the LSA, have now been concluded.

Since May 2018, **61%** 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. **39%** of cross border complaints were lodged with the DPC directly.

In 2023, the DPC received **156** valid cross border complaints, relating to companies for whom the DPC is the LSA[8]. By year end, the DPC had concluded **279 cross-border complaints**. During this period, a further **13** complaints were lodged with the DPC where another Supervisory Authority was identified as the LSA.

In 2023 the DPC submitted through the GDPR Article 60 cooperation mechanism **229** notifications of cases where **an amicable resolution had been achieved**. Details of these cases can be found published on the EDPB website.

Case studies detailing cross border complaints can be found in "Appendix 4" of this report.

Law Enforcement Directive Complaints

The Law Enforcement Directive (EU 2016/680) ('LED') as transposed into Irish law on 25 May 2018 in the Data Protection Act 2018 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 the 'LED' to be applicable, the data controller must also be a 'competent authority' as set out in Section 69 of the Data Protection Act 2018.

In 2023, the DPC received **32 LED complaints and concluded 37 LED complaints** (including complaints received prior to 2023) the majority of which involved An Garda Síochána as the data controller but also included organisations such as the Director of Public Prosecutions, the Department of Social Protection and the Irish Prison Service.

82.5%
cross-border complaints concluded since 2018.

8) These complaints were both received directly by the DPC and transmitted to the DPC by other EU/EEA Supervisory Authorities.

Direct Intervention

The DPC prioritises and directly intervenes in issues that give rise to immediate data protection concerns for large groups of people, in order to ensure a timely response on matters that may potentially have wide repercussions. The DPC engages in a variety of ways with these issues to ensure that processing is brought into compliance with GDPR obligations.

Some of the matters prioritised for direct intervention in 2023 included:

- CCTV in school toilets, public houses, nightclubs, public transport facilities;
- Biometric processing of personal data in the workplace;
- Posting of images of children on-line;
- Disclosure of sensitive personal data in public locations.

In selecting certain matters for direct intervention, the DPC is particularly cognisant of its Regulatory Strategy 2022-2027, which identifies children and vulnerable adults as being in need of specific supports to ensure their data protection rights are upheld.

Complaints under the Data Protection Acts 1988 & 2003

The DPC continues to receive complaints that fall to be handled under the 1988 & 2003 Acts. In 2023, the DPC issued **11** formal Decisions under the Data Protection Acts 1988 & 2003, of which **6** fully upheld the complaint, **4** partially upheld the complaint and **1** rejected the complaint.

Institute of Directors Ireland Chief Executive Officer, Caroline Spillane CDir, with DPC Commissioner Helen Dixon, April 2023.

Breaches

Under the GDPR, Data Protection Officers are recognised as intermediaries between Data Protection Authorities (such as the DPC), individuals and the business units of an organisation. The DPC's Regulatory Strategy 2022-27 recognises the important role DPOs play in championing data protection in their organisations. Organisations are obliged to notify data breaches to the DPC. Such notifications usually come through their DPO who 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.

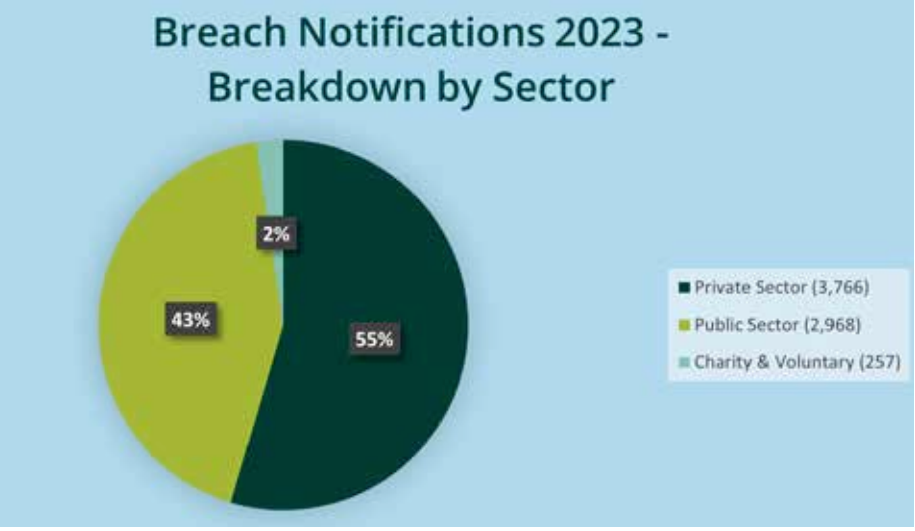
In 2023, the DPC received **6,991 valid GDPR data breaches**. This represented a **20% increase** (1,077) on the GDPR data breach numbers reported in 2022.

Since the introduction of GDPR – and in line with previous years – the highest category of data breaches notified to the DPC in 2023 related to unauthorised disclosures, in cases affecting one or small numbers of individuals, accounting for **52%** of the total notifications.

Of the total 6,991 breach notifications that the DPC received in 2023, 3,766 related to the private sector, 2,968 to the public sector and the remaining 257 came from the voluntary and charity sector. Of those breach notifications received in 2023, **92%** 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, with insurance and telecom companies featuring 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 – continues to feature prominently.

The DPC has engaged with a number of 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 potential inquiries.



Breach Notifications: Nature of Breach for cases received 2023

Nature of Breach	Total	Percentage
Disclosure unauthorised – Postal Material to incorrect recipient	2255	33.69%
Disclosure unauthorised – Email incorrect recipient	1203	17.97%
Integrity – unintentional alteration (Personal Data Disclosed)	602	8.99%
Disclosure unauthorised – Other	571	8.53%
Unauthorised Access – Paper files/Documents/Records	415	6.20%
Availability – accidental (Loss/destruction of Personal Data)	396	5.92%

E-Privacy Breaches

The DPC received a total of **146** valid data-breach notifications (an increase of 42% on the 105 figure for 2022) under the ePrivacy Regulations. The figure of 146 accounts for just **over 2%** of total valid breach cases notified for the year.

Law Enforcement Directive Breaches

The DPC also received **59 valid breach notifications** in relation to the LED, (Directive (EU) 2016/680), which was transposed into Irish law, by the 2018 Act.

Data-Breach Complaints

In 2023, the DPC handled 43 complaints relating to alleged personal data breaches which were not notified to this office in line with Article 33.

Breach Case Studies can be found in "Appendix 4" of this report.

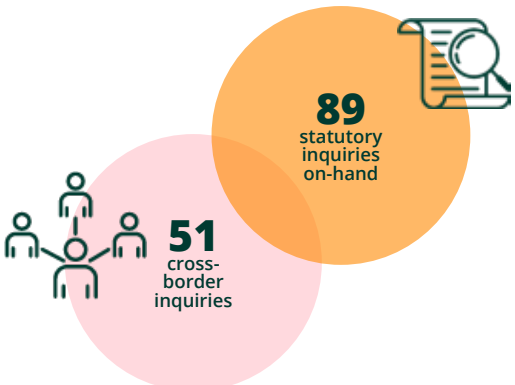
Inquiries

Statutory Inquiries by the DPC

Under the Data Protection Act 2018, the DPC may conduct two different types of statutory inquiry under Section 110 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 2023, the DPC had **89** Statutory Inquiries on-hand, including **51** Cross Border Inquires.



Confirmation of Administrative Fines

In November 2023, the DPC had its decisions to impose administrative fines on five different organisations confirmed in the Dublin Circuit Court, ranging between €15,000 and €750,000. On collection, fines will be transferred to the central exchequer in Ireland.

- VIEC t/a Virtue Eldercare – (€100,000)
- A&G Couriers t/a Fastway Couriers – (€15,000)
- Kildare County Council – (€50,000)
- Centric Health – (€460,000)
- Bank of Ireland – (€750,000)

Inquiries and related Enforcement Action that concluded in 2023

In 2023 the DPC concluded the following inquiries under the GDPR and the Data Protection Act 2018.

Organisations	Decision Issued	Fine Imposed	Corrective Measure Imposed
WhatsApp Ireland Ltd	January 2023	€5.5 million	Order re: Articles 5(1)(a) and 6(1) GDPR.
Kildare County Council	January 2023	€50,000	Temporary ban on CCTV cameras at a number of locations. Order re: Articles 5(1)(a), 6(1), 13, and 32(1) GDPR. Sections 71, 72, 76, 78, and 82 Data Protection Act 2018.
Airbnb Ireland UC	January 2023	N/A	No infringement found.
Centric Health	February 2023	€460,000	Reprimand re: Articles 5(1)(f), 5(2) and 32(1) GDPR.
Bank of Ireland	February 2023	€750,000	Reprimand re: Articles 5(1)(f) and 32(1) GDPR. Order re: Articles 5(1)(f) and 32(1) GDPR.
Archbishop of Dublin	February 2023	N/A	Order re: Article 5(1)(a) GDPR.
Meta (Facebook)	May 2023	€1.2 billion	Suspension of data flows re: Article 46 GPDR. Order re: Article 46 GDPR.
Department of Health	June 2023	€22,500	Ban re Articles 5(1)(c), 6(1), 6(4), and 9(1) GDPR. Reprimand re Articles 5(1)(c), 5(1)(f), 6(1), 6(4), and 32(1) GDPR.
Airbnb Ireland UC	June 2023	N/A	No infringement found.
Airbnb Ireland UC	June 2023	N/A	Reprimand re Articles 5(1)(c) and 5(1)(e). Order re Articles 5(1)(c) and 5(1)(e).

Organisations	Decision Issued	Fine Imposed	Corrective Measure Imposed
Airbnb Ireland UC	July 2023	N/A	Reprimand re: Articles 5(1)(c), 6(1)(f), 15(1), 12(1) and 12(3). Order re: Article 12(1).
Galway County Council	August 2023	N/A	Temporary ban on CCTV cameras and ANPR at a number of locations. Temporary ban on use of body worn cameras. Order re: Article 35 GDPR and Sections 71, 72, 76, 78, 82, 90(1) Data Protection Act 2018. Reprimand re: Article 24 GDPR.
TikTok	September 2023	€345 million	Reprimand re: Articles 5(1)(a), 5(1)(c), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) GDPR. Order re: Articles 5(1)(a), 5(1)(c), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) GDPR .
Airbnb Ireland UC	September 2023	N/A	Reprimand re: Article 12(4).
Airbnb Ireland UC	September 2023	N/A	Reprimand re: Articles 6(1)(f), 5(1)(c) and 5(1)(e). Orders re: Articles 5(1)(c) and 5(1)(e).
Airbnb Ireland UC	September 2023	N/A	Reprimand re: Articles 6(1)(f) and 5(1)(c). Order re: Article 6(1)(f) and 5(1)(c).
Apple Distribution International Limited	November 2023	N/A	No infringement found.
Microsoft Operations Ireland Limited	November 2023	N/A	Reprimand re: Articles 12(4) and 17. Order re: Article 12(4) and Article 17.
Meta (Facebook and Instagram)	November 2023	N/A	Ban on processing personal data for behavioural advertising purposes on the basis of Article 6(1)(b) or (f) GDPR.

Domestic Inquiries 2023

Inquiries that concluded in 2023

Centric Health

The DPC issued its Final Decision in this Inquiry in January 2023. The Inquiry was commenced following a ransomware attack affecting patient data held on Centric's patient administration system. Over 70,000 patients were affected by access to, unauthorised alteration of, and loss of availability of their personal and special category data. Some 2,500 patients were permanently affected as their data was deleted with no backup available. The Decision reprimanded Centric and imposed fines totalling €460,000 in respect of Centric's infringement of Article 5(1)(f) GDPR, Article 5(2) GDPR, and Article 32(1) GDPR.

Kildare County Council

The DPC issued its Final Decision in this inquiry in January 2023. The Decision followed an audit, which examined a range of issues including CCTV systems, ANPR technology, and body worn cameras. The Decision found the Council infringed Articles 5(1)(a), 13, and 32(1) GDPR along with sections 71(1)(c), 71(1)(f), 71(10) 72(1), 76(2), 78, and 82(2) of the Data Protection Act 2018. The corrective measures exercised by the DPC included a temporary ban on processing personal data through CCTV cameras, a temporary ban on processing personal data through CCTV cameras for the purposes of traffic management and an administrative fine in the amount of €50,000.

Church Records by Archbishop of Dublin

The DPC issued its Final Decision in this inquiry in February 2023. This inquiry was an own volition Inquiry into the right to rectification and erasure for data subjects who choose to leave the Catholic Church. The focus of this inquiry was on the entries on the Baptism Register and the extent of their rights pursuant to Articles 16 and 17 of the GDPR. Corrective powers were exercised to direct the Archbishop to make changes to the Privacy Policy for the Archdiocese. Those changes were implemented, in accordance with the Order.

Bank of Ireland – Banking365

The DPC issued its Final Decision in this inquiry in February 2023. This inquiry was in relation to a series of data breaches on the Bank of Ireland 365 app. The inquiry investigated 10 data breaches relating to the unauthorised disclosure of personal data, including financial data, on the BOI365 app.

Bank of Ireland was found to have breached Articles 5(1)(f) and 32(1) GDPR, and the corrective powers exercised included a reprimand, a fine of €750,000 and an order to bring processing into compliance with Articles 5(1)(f) and 32 GDPR.

Department of Health

The DPC issued its 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) GDPR (lawful basis and conditions for processing special category data), 14 (transparency), and 5(1)(f) and 32(1) GDPR (security of data processing). The corrective measures include a ban on processing, a fine of €22,500, and a reprimand. Details of this inquiry can be found on page 36.

Galway County Council

The DPC issued its Final Decision in this inquiry in August 2023. The Decision followed an audit, which examined a range of issues including CCTV systems, ANPR 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) 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.

Inquiries at Draft Decision issued by end 2023

Mediahuis ('MIG') (formerly Irish News and Media plc)

This is a complaint-based inquiry in which the balance between the complainant's personal data rights and the rights of a media organisation to freedom of expression are evaluated, in the circumstances of the case. The DPC issued its Draft Decision in March 2023 to the data controller and the Complainant and is in the progress of preparing a Final Decision at year's end.

Sligo County Council

The DPC issued its Draft Decision in this inquiry in September 2023. The DPC commenced this inquiry and carried out a data protection audit to inquire into the processing of personal data, by or on behalf of the Council, through the use of CCTV and Automated Number Plate Recognition systems and any other technologies that may be used to monitor individuals.

Department of Social Protection re SAFE/PSC Facial Mapping

This inquiry is examining the lawfulness of the personal data processing involved in the facial mapping that is part of the process by which a citizen registers or renews a Public Services Card. The DPC provided the Department of Social Protection with a Draft Decision in November 2023.

Inquiries that reached a key investigative stage in 2023

South Dublin County Council

The DPC commenced this inquiry to inquire into processing of personal data through the use of technologies such as CCTV, body worn cameras, automatic number plate recognition enabled systems, drones and other technologies. The DPC carried out seven on-site inspections during this inquiry. The DPC commenced its decision-making stage in 2023 and was preparing a Draft Decision at year's end.

Department of Social Protection: Child Benefit

This inquiry considers whether certain processing of personal data by the Department in the context of ongoing eligibility assessments/checks for child benefit is compliant with the GDPR and with the Data Protection Act 2018.

The DPC issued a Statement of Issues in 2023 and the Department made submissions in response in June 2023. The inquiry was ongoing at year's end.

An Post GeoDirectory

The DPC commenced this inquiry in July 2023. The inquiry is examining the nature of the information processed by An Post GeoDirectory in the provision of services and products to customer companies that appears to include material that may be deemed to be personal data. The DPC opened an inquiry to assess whether GeoDirectory is acting as a controller and/or has complied with obligations as a controller under the GDPR and/or the Data Protection Act 2018.

Central Bank of Ireland

The DPC opened an own-volition inquiry into the Central Bank of Ireland in October 2023. The inquiry is examining a notified data breach affecting the Central Credit Register and associated processing by the Central Bank of Ireland. The breach notification stated that certain borrower information was retained on the Central Credit Register for up to three months more that allowed by statute, and was available for inclusion in credit reports between 1 June and 7 August 2023. The inquiry is examining organisational and technical measures implemented to ensure the security and accuracy of personal data, particularly in relation to procedures concerning data retention, archiving, reporting errors, ensuring accuracy of personal data, ensuring control and supervision of processors by the controller and communication of personal data breaches to data subjects.

Department of Public Expenditure, NPD Delivery and Reform (DPENDR) re: Single Customer View and MyGovID

This inquiry concerns a complaint to the DPC alleging that the database underpinning the Public Services Card ('the PSC') was unlawfully made available and/ or transferred to DPENDR and was used by DPENDR in a manner inconsistent with data subject's rights. In particular, the complaint alleged that DPENDR had no lawful basis or legitimate purpose to process the data subject's personal data and special category personal data, and that DPENDR was processing their personal data and special category personal data without legal basis and without transparency in relation to the processing activities being undertaken. The DPC is currently preparing a Statement of Issues paper.

Summary of DPC Decision concerning the Department of Health Inquiry

In 2023, the DPC completed an inquiry into certain aspects of the Department of Health's processing of personal data in 29 litigation files. The inquiry was commenced following public allegations in 2021 that the Department had unlawfully collected and processed personal data about plaintiffs and their families in special educational needs litigation.

On the files examined, the DPC found evidence that the Department sought information from the HSE about services that were provided to plaintiffs and their families. The Department also included broadly worded questions asking the HSE to share any other information which the HSE felt was worth mentioning. This broad question resulted in the provision of private information about the lives of plaintiffs and their families.

The Department told the DPC that they processed this personal data for the purposes of determining whether an approach should be made to the plaintiff to seek to settle the case. Under sections 41 and 47 of the Data Protection Act 2018, controllers can process personal data where it is necessary to provide or obtain legal advice or in the context of legal proceedings. In order to determine whether personal data had been lawfully processed by the Department under this provision, the DPC applied the EU law principles of necessity and proportionality.

The DPC issued its Final Decision to the Department of Health in June 2023. In its Decision, the DPC found that the Department did not infringe data protection law by seeking information about the services that were being provided to plaintiffs where there was open litigation. However, the DPC found that the Department did infringe data protection law by asking broad questions that resulted in the provision of sensitive information about the private lives of plaintiffs and their families. This information included details about plaintiffs' jobs and living circumstances, information about their parents' marital difficulties and in one case, information received directly from a doctor about the services that were being provided to the plaintiff.

The DPC found that the processing of this information was excessive and disproportionate to the aims pursued by the Department and not necessary for the purposes of litigation. The DPC found that there was no lawful basis for this processing in the files examined, and that the Department had infringed the principle of data minimisation by processing this personal data.

During the inquiry, the DPC found that the Department retained other information collected from the HSE and received from other government departments on its files. The DPC did not find an infringement of data protection law arising from the Department's storage of this information for the purposes of defending litigation. The files relate to active litigation and the DPC recognised that there are a number of obligations that require defendants to retain documents that relate to open litigation.

Additionally, the DPC found infringements of the GDPR's transparency obligations as the Department did not include details of its practices in its privacy notice. In particular, the privacy notice did not convey the extent of information sharing that took place between the Department and the HSE. The DPC found that the Department could not rely on any exemptions under the Data Protection Act 2018 to avoid providing summary information about those practices in its privacy policy.

The DPC also found that the Department had infringed the requirements to process personal data securely. The inquiry found that the Department ought to have ensured that better internal access restrictions to files were in place.

Having regard to the relevant factors under the GDPR and the fining cap for public authorities under the Data Protection Act 2018, the DPC decided to impose a fine of €22,500 for these infringements. The DPC also imposed a ban on further processing the sensitive data in the files examined for the purposes of determining an appropriate time to settle a case. In addition to the fine and ban on processing outlined above, a reprimand was imposed for all of the infringements.

Cross Border Inquires

Where a particular inquiry 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 GDPR. The Article 60 mechanism outlines a procedure designed to facilitate the conclusion of decisions on the basis of consensus between LSA and Concerned Supervisory Authority ('CSAs'). Through this mechanism, CSAs are enabled to share their views on the matter with the LSA. Where those views take the form of a relevant and reasoned objection, exchanged in response to the LSA's draft decision, 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 Inquiries that concluded in 2023

WhatsApp Ireland Limited (WhatsApp): lawful basis for processing personal data for the purpose of service improvement and security

The DPC issued its Final Decision in this inquiry in January 2023. The inquiry examined the legal basis on which WhatsApp relies to process the personal data of WhatsApp users. It found that WhatApp is not entitled to rely on the 'contract' legal basis for the purpose of service improvement and security in the context of the WhatsApp Terms of Service and that its processing of users' data to date, in purported reliance on the 'contract' legal basis, amounts to a contravention of Article 6 of the GDPR.

The Decision also found that WhatsApp infringed Articles 5(1)(a) GDPR. The Decision ordered Meta to bring its processing operations into compliance with the GDPR within a period of 6 months and an imposed administrative fine of €5.5 million. The Final Decision is under appeal. Details of this inquiry can be found on page 40.

Meta Platforms Ireland Limited (Meta): own volition inquiry concerning the lawfulness of Facebook's data transfers to the United States

In May 2023, the DPC adopted its Final Decision in this inquiry finding that Meta infringed Article 46(1) GDPR by transferring personal data from the EU/EEA to the US without a lawful basis . The Decision ordered Meta to suspend any future transfer of personal data to the US until such time measures become available to make the Data Transfers compliant; it imposed an administrative fine in the amount of €1.2 billion on Meta; and it ordered Meta to bring its processing operations into compliance with Chapter V of the GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EU/EEA users transferred in violation of the GDPR. The Final Decision is under appeal. Details of this inquiry can be found on page 41.

Tiktok Technology Limited (Tiktok): measures in relation to users under age 18

The DPC adopted its Final Decision in this inquiry in September 2023. The inquiry examined the processing of personal data relating to children by TikTok. It focused on public-by-default settings, settings associated with the 'Family Pairing' feature, transparency information provided to child users, and age verification.

The DPC's Decision found infringements of Articles 5(1)(c), 5(1)(f), 24(1), 25(1), 25(2), 12(1), 13(1)(e) and 5(1)(a) GDPR. The Decision exercised corrective powers by reprimanding TikTok, by ordering TikTok to bring its processing into compliance; and by imposing administrative fines totalling €345 million. The Final Decision is under appeal. Details of this inquiry can be found onpage 42.

Commissioner Helen Dixon addressing DPC staff, February 2023.

Summary of DPC Decision concerning WhatsApp Ireland Limited ('WhatsApp'): lawful basis for processing personal data for the purpose of service improvement and security

In January 2023, the DPC adopted its Final Decision finding that WhatsApp infringed Articles 5(1)(a), 6(1), 12 and 13(1)(c) of the GDPR. The inquiry concerned the lawful basis for WhatsApp's processing of personal data for the purpose of service improvement and security.

The DPC had sent a Draft Decision to its peer regulators in the EU/EEA in April 2022 in accordance with Article 60 of the GDPR. Having received relevant and reasoned objections from other Supervisory Authorities and being unable to reach consensus with CSAs, the DPC referred the objections to the EDPB for determination under the Article 65 GDPR dispute resolution mechanism. The EDPB adopted a binding decision on the subject matter of objections from peer Supervisory Authorities on 5 December 2022 and the DPC issued its Final Decision on 12 January 2023.

The Final Decision includes findings that WhatsApp Ireland is not entitled to rely on the contract legal basis for the delivery of service improvement and security (excluding what the EDPB terms as 'IT security') for the WhatsApp service, and that its processing of this data to-date, in purported reliance on the contract legal basis, amounts to a contravention of Article 6(1) of the GDPR.

The Final Decision, in line with the DPC's Draft Decision, also found that WhatsApp infringed its obligations in relation to transparency. This finding of infringement was based on how information in relation to the legal basis relied on by WhatsApp Ireland was not clearly outlined to users, with the result that users had insufficient clarity as to what processing operations were being carried out on their personal data, for what purpose(s), and by reference to lawful basis.

The DPC imposed an administrative fine of €5.5 million on WhatsApp Ireland in respect of its infringement of Article 6(1) GDPR (and taking into account the infringement of the Article 5(1)(a) fairness principle), and ordered that WhatsApp Ireland must bring its processing operations into compliance with the GDPR. The DPC, having already imposed a very substantial fine of €225 million on WhatsApp Ireland for breaches of its transparency obligations over the same period of time, did not propose the imposition of any further fine or corrective measures.

WhatsApp initiated three court challenges against the DPC/ EDPB: a statutory appeal before the Irish High Court, Judicial Review proceedings before the High Court and annulment proceedings against the EDPB before the Court of Justice.

Summary of DPC Decision concerning Meta Platforms Ireland Limited ('Meta): own volition inquiry concerning the lawfulness of Facebook's data transfers to the United States

In May 2023, the DPC made its Final Decision in this inquiry finding that Meta infringed Article 46(1) GDPR by transferring personal data from the EU/EEA to the US. While Meta effected those transfers on the basis of the updated Standard Contractual Clauses ('SCCs') that were adopted by the European Commission in 2021 in conjunction with additional supplementary measures, the DPC found that these arrangements did not address the risks to the fundamental rights and freedoms of data subjects that were identified by the CJEU in its judgment in judgment in Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems.

The DPC's proposed findings in its Draft Decision were submitted to its peer regulators in the EU/EEA in July 2022 in accordance with the process set out in Article 60 GDPR. Peer EU/ EEA Supervisory Authorities endorsed the DPC's proposal to make an order to suspend the data transfers. However, relevant and reasoned objections were received from four Supervisory Authorities that Meta should be subject to an administrative fine for the infringement that was found to have occurred. Two of the Concerned Supervisory Authorities also sought the imposition of an additional order designed to address previous data transfers. The DPC was unable to resolve these objections. The DPC then referred the objections to the European Data Protection Board for determination pursuant to the Article 65 dispute resolution mechanism.

The EDPB adopted its Decision on 13 April 2023 and the DPC adopted its Final Decision on 12 May 2023. The Decision ordered Meta to suspend any future transfer of personal data to the US until such time as measures become available to make the Data Transfers compliant; **it imposed an administrative fine in the amount of €1.2 billion on Meta**; and it ordered Meta to bring its processing operations into compliance with Chapter V of the GDPR, by ceasing the unlawful processing, including storage, in the US of personal data of EU/EEA users transferred in violation of the GDPR.

Meta initiated three court challenges against the DPC/ EDPB: a statutory appeal before the Irish High Court, Judicial Review proceedings before the High Court and annulment proceedings against the EDPB before the Court of Justice.

On 10 July 2023, the European Commission adopted its Adequacy Decision for the EU-U.S. Data Privacy Framework, acknowledging new binding safeguards to address the concerns raised by the CJEU, and concluding that the United States ensures an adequate level of protection for personal data transferred from the EU to US companies under the new framework.

Summary of DPC Decision concerning Tiktok Technology Limited (Tiktok): measures in relation to users under age 18

The DPC commenced this own-volition inquiry in September 2021 concerning TikTok's processing of children's personal data regarding:

1. Processing relating to the platform settings for Child Users', including how children's' accounts were set to public by default and the 'Family Pairing' feature.
2. Processing regarding age verification for children under 13.
3. Transparency of processing for Child Users.

The DPC submitted its Draft Decision to its peer regulators in the EU/EEA in September 2022 in accordance with Article 60 of the GDPR. However, relevant and reasoned objections were received from two Concerned Supervisory Authorities. The DPC was unable to reach consensus with the CSAs and decided to refer the objections to the EDPB for determination under the Article 65 GDPR dispute resolution mechanism, the EDPB adopted a binding decision on the subject matter of objections from peer Supervisory Authorities on 2 August 2023 and the DPC issued its Final Decision on 1 September 2023. The Final Decision records findings of infringement of Articles 5(1)(c), 5(1)(f), 24(1), 25(1), 25(2), 12(1), 13(1)(e) and 5(1)(a) GDPR. The Decision also reprimanded TikTok for the infringements, **imposed administrative fines totalling €345 million,** and ordered TikTok to bring its processing into compliance.

The Final Decision found that TikTok infringed Articles 25(1), 25(2), and 5(1)(c) GDPR by failing to implement appropriate technical and organisational measures to ensure that, by default, only personal data which were necessary for TikTok's purposes of processing were processed; and to ensure, by default, that the social media content of Child Users was not made accessible to an indefinite number of persons without the user's intervention. The Final Decision also found that TikTok infringed Article 24(1) GDPR by failing to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this GDPR in respect of the risk of how children's accounts were set to public by default, and the risk of children under 13 accessing the platform.

The Decision also found that TikTok infringed Article 13(1)(e) GDPR by failing to provide Child Users with information on the categories of recipients of personal data. The Decision also found that TikTok infringed Article 12(1) by failing to provide Child Users with information on the scope and consequences of the public by default processing in a concise, transparent, intelligible manner and in a form that is easily accessible.

The Decision further found that TikTok infringed Articles 5(1)(f) and 25(1) GDPR in respect of its Family Pairing setting, by allowing an intended Parent/Guardian to enable direct messages for a Child User where such messages were not previously enabled by the Child User. This occurred in circumstances where the intended Parent/Guardian was not verified by the platform. The fact that the intended Parent/Guardian could loosen the relevant setting was found to be an infringement of the GDPR. The Decision did not find the existence of the Family Pairing option, or the ability for the intended Parent/Guardian to make privacy settings stricter, to be problematic.

As noted, the Final Decision reprimanded TikTok for the infringements, imposed administrative fines totalling €345 million, and ordered TikTok to bring its processing into compliance. TikTok initiated three court challenges against the DPC/ EDPB: a statutory appeal before the Irish High Court, Judicial Review proceedings before the High Court and annulment proceedings against the EDPB before the Court of Justice.The DPC subsequently engaged with TikTok on the appropriate compliance measures required to comply with the Decision. As a result of the Decision and this process, TikTok implemented changes to its processing of children's personal data between September 2023 and year's end, with additional changes due in 2024. The action to be taken by TikTok to comply with the Decision included: the cessation of certain processing regarding public-by-default processing of children's data, the provision of information to users, and the elimination of deceptive design patterns identified in the Decision.

Inquiries where the Article 60 GDPR Draft Decision cooperation process commenced and remained ongoing in 2023

Google Ireland Limited (Google): Location data inquiry

This Inquiry concerns the lawfulness of Google's processing of location data and whether it meets its obligations as a data controller with regard to transparency. In August 2023, the DPC submitted its Draft Decision to its peer regulators in the EU/EEA in accordance with the process set out in Article 60 GDPR. That process remained ongoing at end of year.

Yahoo! EMEA Limited (Yahoo): Transparency of processing

The inquiry examines Yahoo's compliance with the requirements to provide transparent information to data subjects under the provisions of the GDPR. In October 2022, the DPC submitted its Draft Decision to its peer regulators in the EU/EEA in accordance with the process set out in Article 60 GDPR. That process remained ongoing at year's end.

Meta Platforms Ireland Limited: complaint based inquiry concerning the lawfulness of Facebook's data transfers to the United States

This inquiry concerns a complaint made against Meta Platforms Ireland Limited regarding the transfer of the Complainant's personal data, processed by means of the Facebook service, to the United States. In April 2023, the DPC submitted its Draft Decision to its peer regulators in the EU/EEA in accordance with the process set out in Article 60 GDPR. That process remained ongoing at year's end.

Twitter International Unlimited Company (Twitter): complaint concerning user generated content on the Twitter platform

The DPC commenced four inquiries regarding complaints concerning user generated content posted on the Twitter service which was not removed following data subjects requesting that Twitter do so. The DPC issued Preliminary Draft Decisions and provided Twitter with an opportunity to make submissions prior to the matter being considered by the concerned supervisory authorities across the EU/EEA under the Article 60 process. In line with Article 60 GDPR, the DPC subsequently issued Draft Decisions in the inquiries to concerned supervisory authorities. That process remained ongoing at year's end.

Inquiries where submissions on a Preliminary Draft Decision, Statement of Issues, or Inquiry Report were invited from the relevant parties during 2023

TikTok Technology Limited (TikTok): data transfers from the EU to China

This inquiry concerns transfers by TikTok of the personal data of users of its platform from the EU to China and whether TikTok is complying with requirements under Part V of the GDPR in relation to international transfers of personal data to third countries. The inquiry is also examining whether TikTok is complying with its transparency obligations to users insofar as such data transfers are concerned.

In May 2023, the DPC issued TikTok with a Preliminary Draft Decision for the purpose of enabling TikTok to make submissions prior to the matter being considered by the concerned supervisory authorities across the EU/EEA under the Article 60 process. At year's end, the DPC was considering the submissions of TikTok.

Google Ireland Limited (Google): real time bidding (adtech system)

This inquiry concerns processing carried out by Google in the context of the operation of its 'Authorised Buyers' real time bidding advertising system. It is examining Google's compliance with its obligations as a controller including in relation to the legal basis relied on by Google for the processing undertaken by it, its collection and retention of personal data as well as transparency information provided to data subjects. The DPC issued Google with a Preliminary Draft Decision setting out its provisional views and Google made submissions in response in March 2023.

By year's end the DPC was considering those submissions before submitting its Draft Decision to its peer regulators in the EU/EEA in accordance with the process set out in Article 60 GDPR.

LinkedIn Ireland Unlimited Company ('Linkedin): complaint by La Quadrature du Net

This inquiry concerns a complaint in relation to the lawfulness of the processing of personal data of users of the LinkedIn service carried out by LinkedIn for behavioural analysis and targeted advertising. The complaint in question was lodged by a French digital advocacy organisation, La Quadrature du Net, 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 provided a Preliminary Draft Decision to LinkedIn in April 2023 in order to give it a final opportunity to make submissions. At year's end the DPC was considering LinkedIn's submissions before submitting its Draft Decision to its peer regulators in the EU/EEA in accordance with the process set out in Article 60 GDPR.

Meta Platforms Ireland Limited (Meta): access and portability requests for certain technical information

This inquiry concerns a complaint made by a data subject to the DPC in relation to Meta's handling of an access request and data portability request made by them. The request of the data subject concerns data held in a specific technical database by Meta. The inquiry is examining whether Meta has discharged its obligations in respect of the data subject rights to access and portability under the GDPR, having regard to Article 12 of the GDPR (transparency requirements), including the extent to which a data controller may refuse to act on a data subject request in circumstances where that controller believes that the request is 'manifestly unfounded or excessive', as referred to in Article 12 GDPR. At year's end, the DPC was preparing a Preliminary Draft Decision.

Meta Platforms Ireland Limited (Meta): complaint by La Quadrature du Net

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, 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. Meta was provided with an opportunity to provide submissions following updates to the DPC's draft inquiry report in September 2023. At year's end the DPC was considering those submissions prior to preparing a Draft Decision for review by its peer regulators in the EU/ EEA.

Google Ireland Limited (Google): consent obtained in the Google account creation process

This inquiry concerns Google's processing of personal data as part of the registration process when setting up a Google account and as a result of the consent provided by users, under various personalisation settings, at the point of account creation. The inquiry was commenced in 2023 on foot of a series of coordinated complaints received from European Consumer Organisations acting under the coordination of the European Consumer Organisation (BEUC) under Article 80 of the GDPR. The inquiry is examining the lawfulness of the consent obtained by Google, data protection by design and default, compliance with transparency obligations and the principle of fairness.

Google commenced judicial review proceedings on 18 January 2024 challenging the commencement of the inquiry and the hearing of those proceedings is scheduled for July 2024.

Meta Platforms Ireland Limited (Meta): Personal Data Breaches affecting Facebook User Tokens

This Inquiry concerns an examination of whether Meta has discharged its GDPR obligations to implement organisational and technical measures and data protection by design and default obligations to secure and safeguard the personal data of its users in connection with a data breach which occurred in September 2018 and affected Facebook user tokens. Meta made submissions on the DPC's Preliminary Draft Decision in February 2023. By year's end, the DPC was considering those submissions before submitting its Draft Decision to its peer regulators in the EU/EEA in accordance with the process set out in Article 60 GDPR.

Meta Platforms Ireland Limited ('Meta'): breach notification issues

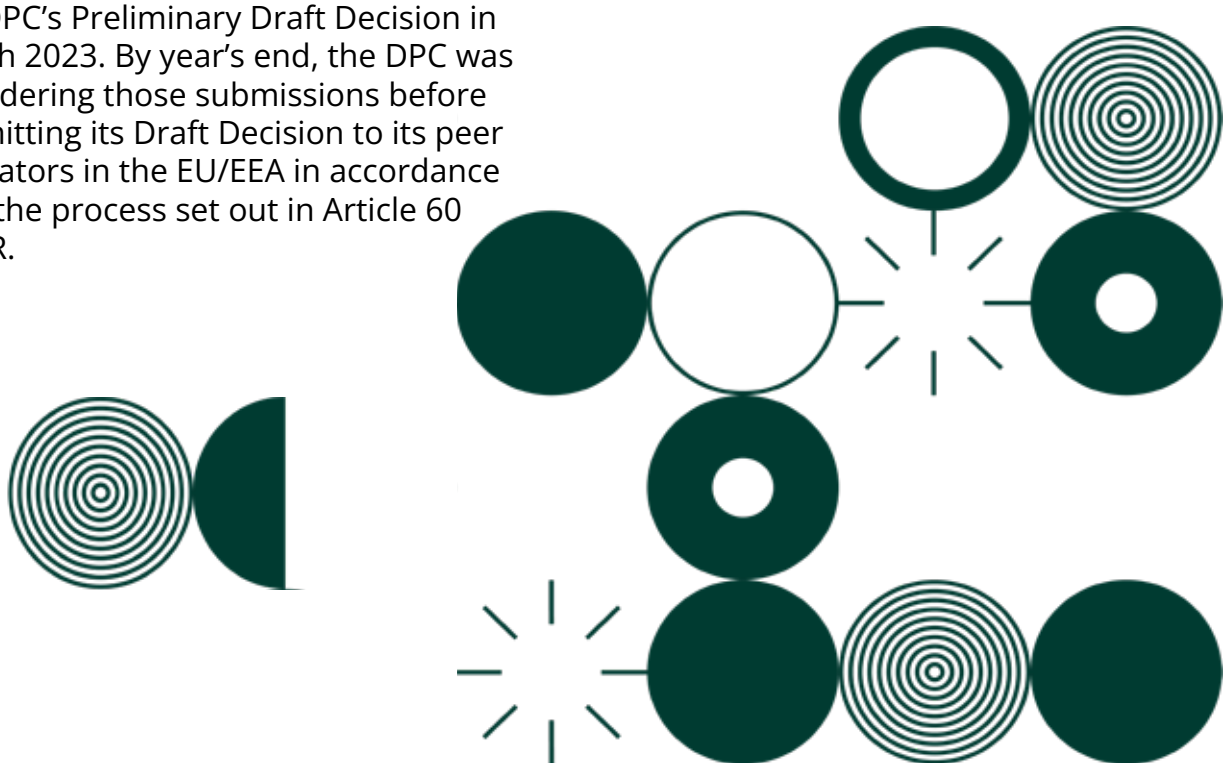
This inquiry concerns Meta's compliance with the breach notification obligations arising under Article 33 GDPR in connection with the notification to the DPC of a data breach which occurred in September 2018 and affected Facebook user tokens. Meta made submissions on the DPC's Preliminary Draft Decision in February 2023. At year's end, the DPC was considering those submissions before submitting its Draft Decision to its peer regulators in the EU/EEA in accordance with the process set out in Article 60 GDPR.

Meta Platforms Ireland Limited ('Meta'): passwords stored in plain text

This inquiry examined whether Meta complied with its obligations under the GDPR, in particular in relation to security of processing. The inquiry was commenced as a result of a security incident which occurred in early 2019 where user passwords were inadvertently stored in plaintext on Facebook's internal systems. Meta made submissions on the DPC's Preliminary Draft Decision in March 2023. By year's end, the DPC was considering those submissions before submitting its Draft Decision to its peer regulators in the EU/EEA in accordance with the process set out in Article 60 GDPR.

MTCH Technology Services Limited (MTCH) and the Tinder service

This own-volition inquiry concerns the extent to which MTCH complied with its obligations under the GDPR with respect to a number of complaints from data subjects located in Ireland and across the EU. It examines MTCH's compliance with the right of data subjects to access their data under Article 15 GDPR and the right to erasure under Article 17 GDPR. Specifically, the inquiry examines whether MTCH is in compliance with the GDPR in regard transparency information and in its response to data subject access requests, and whether MTCH's lawful basis for the ongoing processing of users' personal data following users' erasure requests has a valid lawful basis. By year's end, the DPC had issued the controller with a Preliminary Draft Decision to provide it with an opportunity to make submissions prior to the matter being considered by the concerned supervisory authorities across the EU/EEA under the Article 60 process.



Yelp Ireland Limited ('Yelp')

This inquiry relates to Yelp's compliance with Articles 5, 6, 7 and 17 of GDPR following a number of complaints received by the DPC in relation to the processing of personal data by Yelp on its website. In January 2023, the DPC issued a Statement of Issues for the purposes of inviting submissions from Yelp. The DPC was preparing a Preliminary Draft Decision at year's end.

Twitter International Unlimited Company (Twitter) Scraping/Breach

The DPC launched an own-volition inquiry in December 2022 in relation to multiple international media reports, which highlighted that one or more collated datasets of Twitter user personal data had been made available on the internet. These datasets were reported to contain personal data relating to approximately 5.4 million Twitter users worldwide. The datasets were reported to map Twitter IDs to email addresses and/or telephone numbers of the associated data subjects. The DPC provided Twitter with an Issues Paper and Twitter made submissions on it in November 2023. At year's end, the DPC was preparing its Preliminary Draft Decision.

Cases involving individual complainants concluded by DPC through EU Co-Operation procedure in 2023

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 2023, the DPC **concluded 279 such cases.** Details of these cases can be found published on the EDPB Article 60 case register. In addition, the DPC also concluded 9 inquiries concerning cross-border complaints in 2023. These Inquiries were in relation to complaints related to issues concerning rights to access and erasure; including the lawful basis for requesting ID and/or photographs to verify identity; data minimisation compliance; compliance with conditions for consent; & compliance with transparency and information obligations.

Organisation	Decision Issued	Corrective Measure Imposed
Airbnb Ireland UC	January 2023	No infringement found of Articles 5, 6 and 13.
Airbnb Ireland UC	June 2023	No infringement found of Articles 5, 6, 12 and 17.
Airbnb Ireland UC	June 2023	Reprimand re Articles 5(1)(c) and 5(1)(e). Order re Articles 5(1)(c) and 5(1)(e).
Airbnb Ireland UC	July 2023	Reprimand re: Articles 5(1)(c), 6(1)(f), 15(1), 12(1) and 12(3). Order re: Article 12(1).
Airbnb Ireland UC	September 2023	Reprimand re: Article 12(4).
Airbnb Ireland UC	September 2023	Reprimand re: Articles 6(1)(f), 5(1)(c) and 5(1)(e). Orders re: Articles 5(1)(c) and 5(1)(e).
Airbnb Ireland UC	September 2023	Reprimand re: Articles 6(1)(f) and 5(1)(c). Order re: Article 6(1)(f) and 5(1)(c).
Apple Distribution International Limited	November 2023	No Infringements found of Articles 5, 6, 7 and 13.
Microsoft Ireland Operations Limited	November 2023	Reprimand re: Articles 12(4) and 17. Order re: Article 12(4) and Article 17.

Airbnb Ireland UC – ID Request and Erasure request

This inquiry commenced in September 2022 concerns a complaint in relation to the lawful processing of personal data for the purposes of identity verification, along with infringements in relation to the principal of data minimisation.

A complaint was lodged with the Federal Commissioner for Data Protection and Freedom of Information (BfDI) in Germany against Airbnb and was therefore transferred to the DPC as Lead Supervisory Authority under the One-Stop Shop mechanism. The complaint was that Airbnb had unlawfully requested a copy of the individual's ID in order to verify their identity. The individual expressed concerns of identity theft given the volume of personal data required for submission to complete an accommodation booking. Airbnb would not accept the booking until identity was verified by providing a copy of ID in addition to a newly taken photograph to ensure that the ID related only to the person making the booking. In this instance Airbnb initially misunderstood the complaint as a request to erase the Airbnb account. In addition to the complaint regarding ID verification, the individual also wanted Airbnb to delete their ID.

The DPC Decision in September 2023 found that there were infringements by Airbnb with regards to the legal basis for processing under Article 6(1)(f) as well as infringements with regard to data minimisation in relation to the request for a copy of the individual's photographic ID under Article 5(1)(c).The DPC inquiry also found that the continued retention of the individual's ID following successful identity verification for the lifetime of their account infringed the principle of data minimisation along with the principle of storage limitation under Article 5(1)(e).

The DPC inquiry found no infringement in the time taken by controller in responding to the individual's request, nor in the controller's handling of the individual's erasure request.

This case is an example of how the DPC's intervention reinforced the proportionality of the controller's mechanisms for data verification and minimisation. In previous engagements DPC has found the controller relied on Article 6(1)(f) as the legal basis for processing ID, once all other efforts to verify identity were unsuccessful. The controller in this case did not make other attempts at verification before requesting a copy of the ID and therefore could not rely on legitimate interests for processing.

Microsoft Ireland Operations Limited – Erasure Request; Transparency

This inquiry commenced in June 2023 concerns a complaint in relation to the controller's response to an individual's access requests and their request to exercise their right to erasure.

The complaint was lodged with the Bavarian Lander Office for Data Protection Supervision against Microsoft Ireland Operations Limited ("Microsoft"), and thereafter transferred to the DPC as Lead Supervisory Authority. In this case the complainant had twice requested that Microsoft erase URLs containing their personal data, which had appeared in internet search results for their name on the Bing search engine.

The inquiry established that two distinct erasure requests were submitted by the Complainant – one in March 2021 and one in October 2021. With regard to the March 2021 erasure request, Microsoft erased two of four URLs and rejected the request to erase the remaining URLs. With regard to the October 2021 erasure request, Microsoft initially rejected the request to erase three URLs. It subsequently changed its position and commenced the erasure process in late November 2021, completing the process in March 2022. The inquiry established that as the URLs should have been accepted for delisting in October 2021, Microsoft did not act on the erasure request without undue delay. Also, in each response to the Complainant requests, the controller informed the individual of the steps taken in relation to each URL and their right to lodge a complaint with a supervisory authority, but it failed to inform them of their right to a judicial remedy.

In its Decision adopted in November 2023, the DPC exercised corrective powers with an order, in accordance with Article 58(2)(d) of the GDPR for Microsoft to revise its internal policies and procedures as regards the information to be provided to data subjects. A reprimand to Microsoft Ireland Operations Limited pursuant to Article 58(2)(b) of the GDPR in light of the infringements found was also issued.

This case is an example of how the DPC inquiry found where a data controller in seeking to meet their obligations under GDPR still failed to do so fully. DPC's intervention resulted in an order, in accordance with Article 58(2)(d) of the GDPR for the controller to revise its internal policies and procedures as regards the information to be provided to data subjects pursuant to Article 12, to ensure that, where it informs data subjects on foot of requests made under Articles 15 to 22 of the GDPR where it has decided not to take action on the request, that data subjects are informed in all cases of their right to seek a judicial remedy.

Enforcement of Corrective Powers exercised by the DPC

Throughout 2023, the DPC took action to ensure compliance with a range of corrective powers exercised, including orders to bring processing into compliance and bans on processing. This section outlines some examples of this enforcement action.

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

Throughout 2023, the DPC supervised compliance by Meta with two orders for compliance made by the DPC 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) 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) GDPR, and the consent lawful basis under Article 6(1)(a) GDPR following the finding that Meta could not rely on the contract lawful basis under Article 6(1)(b) GDPR.

In April 2023, Meta sought to rely on the 'legitimate interests' basis for the processing as set out in Article 6(1)(f) GDPR. On 4 July 2023, the Court of Justice of the European Union delivered the CJEU Bundeskartellamt Judgment, concerning, amongst other things, Meta's processing of personal data on the basis of Article 6(1)(f) GDPR.

On 18 August 2023, following consultation and cooperation with other supervisory authorities across Europe, the DPC concluded that Meta had not demonstrated compliance with the 'legitimate interests' basis for processing set out in Article 6(1)(f) GDPR to process personal data of Facebook and Instagram users for the purposes of behavioural advertising.

Meta then instead decided to seek consent under Article 6(1)(a) GDPR from data subjects for its processing of personal data for the purposes of behavioural advertising. The DPC informed Meta that is was required to implement its consent-based model, and to obtain valid consent from data subjects, by 24 November 2023 at the latest. The DPC set this deadline to ensure that Meta's user flows and its proposed consent-based model would be properly developed and subject to scrutiny from the Data Protection Authorities before being presented to the public.

In October 2023, a Supervisory Authority requested the European Data Protection Board to adopt an urgent binding Decision under Article 66 of the GDPR instructing the DPC to ban Meta's reliance on Article 6(1)(b) and 6(1)(f) GDPR within 2 weeks. The European Data Protection Board adopted a binding Decision on 27 October 2023 to that effect. The DPC then issued an enforcement notice to Meta to ban it from processing personal data for the purposes of behavioural advertising on the basis of Articles 6(1)(b) or 6(1)(f) GDPR.

Meta launched a new consent model on 10 November 2023. By year's end, the DPC was retrospectively leading a review of that consent model in conjunction with European supervisory authorities. In parallel, Meta is bringing three legal challenges to the December 2022 Decision before the Irish Courts and the CJEU. Meta had also brought legal challenges to the enforcement notice that the DPC issued.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): 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) 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. In parallel, Meta had 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. The DPC subsequently engaged with Meta throughout 2023 on the appropriate compliance measures required to comply with the Decision. As a result of this process, Meta implemented further changes in December 2023 which were being reviewed by year's end.

Meta Scraping Inquiry

In November 2022, the DPC issued a Final Decision in this inquiry, which was commenced following media reports into the discovery of a collated dataset of Meta personal data that had been made available on the internet. The inquiry found infringements of the GDPR in respect of the manner in which data subjects were searchable within some features of the Facebook and Instagram applications and ordered Meta to bring its processing into compliance. Meta brought legal proceedings to appeal of the DPC Decision.

In parallel, Meta provided a compliance report in February 2023. The DPC analysed that report on a legal and technical basis. The DPC then circulated its views to other Supervisory Authorities concerned for their input on compliance. On foot of engagement from the DPC, Meta agreed to certain changes and to provide a series of submissions outlining how those changes were rolled out to its systems. Meta also carried out updates to its systems to change the information available to data subjects so as to ensure that the systems changes were transparent to its users.

Airbnb

In 2023, the DPC completed follow-up enforcement action related to two Decisions concerning Airbnb that it had issued in September, 2022 and in June, 2023 respectively. In both Decisions, the DPC had exercised corrective powers in the form of orders made pursuant to Article 58(2)(d) of the GDPR and it set deadlines by which Airbnb was required to notify the DPC of the actions taken to comply with the orders.

Compliance reports concerning both cases were subsequently submitted to the DPC by Airbnb. Given that the Decisions related to cross-border complaints, the DPC consulted with all data protection supervisory authorities in the EU/EEA when assessing the extent of compliance by Airbnb with the orders in the DPC's Decisions. The DPC completed the assessment process for each case and notified Airbnb in August, 2023 and in November, 2023 respectively that it was satisfied that Airbnb had complied with the orders in the Decisions.

At year's end, follow-up enforcement action was underway in respect of a further three decisions concerning Airbnb that the DPC had issued in July 2023 and September 2023.

Kildare County Council: surveillance technologies deployed by Local Authorities

The DPC's investigations and enforcement actions in relation to the deployment of surveillance technologies by Local Authorities have highlighted, in particular, the operation of CCTV cameras in certain circumstances without a lawful basis that meets the standard of precision, clarity and foreseeability required under EU law.

In 2023 the DPC engaged in a number of actions to ensure that the deployment of CCTV cameras by Local Authorities is carried out in compliance with data protection law. These actions included conducting on-site inspections to verify that corrective measures set out on foot of DPC Decisions have been implemented, as well as engaging in consultation on codes of practice for the use of surveillance technologies in the context of waste enforcement and litter pollution.

In each of these engagements, the DPC's aim is to ensure that where Local Authorities utilise technological solutions in the public interest to tackle issues such as anti-social behaviour and illegal dumping, they do so in a manner that adheres to the principles of data protection, and is proportionate in terms of its impact upon the fundamental rights and freedoms of individuals.

By way of follow-up enforcement action related to the DPC Decision concerning Kildare County Council, the DPC obtained a report from Kildare County Council on the actions it had taken to comply with the corrective measures. The DPC verified the actions taken by carrying out an on-site inspection at Kildare County Council in September 2023.

In particular, this inspection confirmed that the Council had switched off certain CCTV cameras that had been operating without a valid lawful basis. At the relevant time, there was no legislation that brought clarity, precision and foreseeability to the circumstances in which CCTV cameras could be deployed by Local Authorities for litter and waste prevention. The relevant CCTV cameras had also not been approved by the Garda Commissioner in accordance with Section 38 of the Garda Síochána Act 2005.

CCTV and other technologies deployed by the State for surveillance purposes can interfere with the fundamental rights to privacy and data protection. In those circumstances, it is crucial that legislation permitting the use of such technologies for surveillance must afford adequate legal protection against arbitrariness and bring clarity to the scope of any discretion conferred on public authorities to carry out surveillance. In particular, the legislation must indicate in what circumstances and under which conditions CCTV can be deployed, thereby ensuring that the any interference with fundamental rights is limited to what is strictly necessary.

The DPC welcomes the Circular Economy and Miscellaneous Provisions Act 2022, which sets out provisions for the proposal and approval of CCTV schemes in respect of litter and waste offences, mandates data protection impact assessments as part of that process, and provides for codes of practice, which the DPC has played an active role in scrutinising. The DPC will continue to ensure that any surveillance conducted by Local Authorities, including CCTV deployed pursuant to these provisions, complies with data protection law and is proportionate to the purposes pursued.

Further information on the DPC's involvement concerning the Circular Economy and Miscellaneous Provisions Act can be found on page 65 of this report.

An Garda Síochána – Data breach at Kilmainham Garda Station (LED).

In December 2022, the DPC issued a Final Decision in this inquiry pursuant to the Law Enforcement Directive, as transposed in the Data Protection Act 2018. The inquiry found infringements in relation to the security of personal data displayed upon Intelligence Bulletin Boards in Garda Stations. The Final Decision required An Garda Síochána to bring its processing into compliance with the relevant provisions of the Data Protection Act 2018 through the implementation of appropriate technical and organisational measures in regard to the security of Intelligence Bulletins throughout its network of Garda stations in Ireland.

During 2023, An Garda Síochána provided a series of submissions in relation to progress in implementing this order throughout the State. As a result of the actions taken by An Garda Síochána, the vast majority of Garda Stations have now ceased to use physical Intelligence Bulletin Boards and there have been additional measures taken to increase the security of personal data in relation to visitors and contractors working in the Garda Stations nationwide. The DPC continues to review the measures implemented in this case.

Anu Bradford, Henry L. Moses Professor of Law and International Organization, Columbia University Law School, Helen Dixon, Commissioner for Data Protection, and; Chad Thomas, Bloomberg, at the 2023 Bloomberg New Economy Gateway Europe, April 2023.

Litigation

Judgments Delivered and Final Orders made in 2023

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
1.	2020/03165	John Healy v Data Protection Commissioner	Statutory Appeal Dublin Circuit Court	Judgment of O'Connor J, delivered on 29 March 2023
Outcome				**Current Status**
This appeal was concerned with a Decision on a complaint by the Appellant to the effect that information about his Irish pension had been disclosed, by his former employers, to UK Trustees in Bankruptcy in connection with other legal proceedings in the UK. The question considered by the Court was whether the disputed disclosure gave rise to a breach of the Data Protection Acts, 1988-2003. The Commission's Decision of 7 May 2020 considered two issues, namely, (i) consent and (ii) legitimate interest arising under Section 2A(1)(d) of the Acts. The Commission found in favour of the Appellant on the first point, deciding that the consent relied on was not sufficiently specific or informed. However, the Commission decided that the Trustees in Bankruptcy were entitled to rely on Section 2A(1)(d), as they identified a lawful and legitimate interest pursued by a third party, namely the administration of the Appellant's estate. By written judgment delivered on 29 March 2023 the Circuit Court rejected the appeal. The Court accepted the Commission's position and noted that the UK and CJEU case law referred to by the Appellant did not provide an absolute prohibition on the disclosure of the personal data in issue in the case. Note that the appeal was concerned with pre-GDPR data protection rules/ legislation.				Proceedings concluded.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
2.	2019/8493P	Patrick Cahill v Coyle & Ors Patrick Cahill v Ireland, the Attorney General & Ors	Plenary High Court	Judgment of Mr Justice Cregan delivered on 16 May 2023
Outcome				**Current Status**
This Judgment concerned two linked sets of proceedings, which were heard together before Mr Justice Cregan. The Commission was named in the second set of proceedings only. The second set of proceedings concerned an application by the Plaintiff for an injunction restraining the Defendants from interfering with investment properties, and applications by the Defendants to strike out the Plaintiff's claim as an abuse of process. The Commission maintained the position that it was a stranger to the underlying dispute between the plaintiff and first defendant and that there was no basis for naming the Commission as a defendant to the proceedings. The Commission successfully applied to the Court to have the proceedings struck out on the basis that no reasonable cause of action had been established by the Plaintiff, and further, that the proceedings were frivolous and/or vexatious. Subsequently, the Plaintiff brought a motion to discontinue the two sets of proceedings in their entirety. Mr Justice Creegan made an order striking out the proceedings as against the Commission together with an order for costs.				Proceedings discontinued

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
3.	2020/02457	Patrick Cahill v The Data Protection Commission	Statutory Appeal Dublin Circuit Court	Order of Mr Justice John O'Connor dated 25 May 2023
Outcome				**Current Status**
This statutory appeal related to two Decisions of the Commission dated 7 April 2020 in response to complaints from the Appellant alleging the unlawful obtaining, use of and disclosure of his personal data. The Commission did not uphold the complaints. Prior to the hearing of the appeal, the Appellant informed the parties that he wished to discontinue the appeal. Accordingly, on 25 May 2023, Mr Justice O'Connor made an order of discontinuance together with an order for costs in favour of the Commission as against the Appellant.				Proceedings discontinued.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
4.	2022/191 JR	Johnny Ryan – v – Data Protection Commission & Google Ireland Ltd (as Notice Party)	Judicial Review High Court	28 August 2023
Outcome				**Current Status**
These proceedings were issued by the Applicant seeking a declaration that the Commission had failed to carry out an investigation of his complaint in accordance with Article 57 of the General Data Protection Regulation and/or the Data Protection Act 2018. The Applicant also sought an order compelling the Commission to proceed to investigate such elements of his complaint in respect of certain data processing operations being carried out by Google Ireland Ltd that were not being included in the (separate) own-volition inquiry commenced by the Commission in respect of processing operations being carried out by Google Ireland Ltd. The Commission maintained the position that as there was a clear overlap between the issues being raised in the Applicant's complaint and the issues being considered by the Commission in the context of its own-volition inquiry, the Commission was entitled to progress its own-volition inquiry prior to resuming consideration of the Applicant's complaint. In a written Judgment dated 28 August 2023, Mr Justice Simons dismissed the application for judicial review. The Court acknowledged the discretion the language of the GDPR affords to supervisory authorities in respect of the sequencing of investigations and inquiries. The Court further held that it was entirely proportionate for the Commission to have decided to complete its own-volition inquiry first, before completing its investigation o the Applicant' complaint. The matter has now been appealed to the Court of Appeal.				Proceedings concluded

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
5.	2022 80 CA [2023] IEHC 529	David Fox v The Data Protection Commission	Appeal on a Point of Law High Court	25 September 2023

Outcome	Current Status
By way of written judgement delivered on 25 September 2023 the High Court dismissed Mr Fox's appeal on a point of law from a Decision of the Circuit Court, primarily on the basis that Mr Fox had failed to identify any point of law and as such the High Court did not have any jurisdiction. The background to this appeal was as follows. 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, being points concerned with (a) whether the installation by the National Gallery of Ireland of CCTV equipment in the National Gallery was justifiable by reference to certain interests identified by the NGI; (b) whether the deployment of certain other IT security measures was lawful; and (c) whether the NGI had complied with an access request made by Mr Fox. 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 appealed that Circuit Court Decision to the High Court, on a point of law. In its judgment delivered on 25 September 2023, the High Court dismissed Mr Fox's appeal on the grounds that Mr Fox had failed to identify any point of law and so the High Court had no jurisdiction. The High Court also found that the points that Mr Fox had sought to raise comprised a combination of (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 with respect to issues not raised before the DPC or the Circuit Court. Costs were awarded to the DPC.	Hearing concluded. The Court has invited the parties to correspond in relation to the form of the order (including costs) to be made by the Court.

No.	Record No.	Title	Type of action and venue	Date of Judgment/Order
6.	2022/003208	Peter Nowak v Data Protection Commission	Statutory Appeal DublinCircuit Court	Judgment of Mr Justice John O'Connor delivered on 9 October 2023
Outcome				**Current Status**
This statutory appeal arises in the context of several previous appeals brought by the Appellant against decisions of the Commission dating back to a 2010 complaint against the Institute of Chartered Accountants Ireland. The Circuit Court, High Court and the Court of Appeal have all issued Judgments dismissing the Appellant's various appeals. Following a Judgment of the Court of Appeal in July 2020, the Appellant identified five issues which he claimed should have been dealt with by the DPC but which had not been dealt with. In light of this claim, the DPC issued a fresh decision dealing with these five issues on 21 April 2022. In appealing this decision, the Appellant submitted that there was a serious and significant error or a series of such errors by the Commission which justified setting aside the decision: firstly, a failure to properly investigate the complaint, and secondly that the DPC erred in its conclusion on the outstanding issues identified by the Appellant as arising for investigation. The Appellant also submitted that a case should be stated to the Court of Appeal, based on his lack of confidence of the Circuit Court's ability to deal with the appeal. By way of written judgment dated 9 October 2023, Mr Justice O'Connor dismissed the appeal on the basis that the decision was not vitiated by a serious and significant error or a series of such errors such that would justify setting aside the decision. The Court further ruled that there was no basis for stating a case to the Court of Appeal, as there was no arguable case of substance. The matter returned before the Court on 4 December 2023, for the purpose of dealing with the form of the Court's Order, including the matter of costs. The Court noted that the DPC had been successful in the appeal and made an order for costs in favour of the DPC. This was stayed pending the outcome of Mr Nowak's appeal to the High Court.				Proceedings concluded. Final Orders to be drawn.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
7.	2019/236	John Paul Hickey v Data Protection Commission	Statutory Appeal (Data Protection Acts 1988 & 2003), Limerick Circuit Court	31 October 2023
Outcome				**Current Status**
This set of proceedings concerns a Decision of the DPC made on 25 January 2019. The decision concerned a complaint against the Diocese of Limerick, an access request, and redacted documents In his judgment delivered orally on 31 October 2023, Judge Daly in the Circuit Court said he was satisfied that in order to succeed with the Appeal the Appellant would have to clearly establish that there had been a serious and significant error, or series of such errors, in the DPC's Decision. The Court noted that the DPC had engaged extensively with the Notice Party in relation to the redactions applied to certain documents. The Court pointed out that the Appellant had not put forward any evidence to say that the DPC had erred in relation to the redactions. In addition, the Court noted that as the Appellant had received un-redacted copies of the documents at the centre of the dispute, the Appeal had become moot. In its Decision, the DPC had found that the Diocese of Limerick had contravened the Data Protection Acts in its delay in releasing the documents in question. The Court noted that the Appellant was seeking a further declaration from the DPC that the Diocese's delay was 'inordinate' or 'excessive', but the Court said that there was no legal basis for the Appellant to request the DPC to include any such declaration in its Decision. The Court referred to the efforts the DPC had made to investigate the Appellant's allegation that there was an additional document not provided to him. Again, the Court found that the Appellant had not put forward any evidence to support his allegation that the DPC had erred in this investigation. Lastly, the Appellant alleged that minutes of certain meetings should have been provided to him. The Court noted that the DPC was satisfied that the minutes were not held by the Notice Party and that again the Appellant had not put forward any evidence to support an allegation that the DPC had erred in that regard. By oral judgment delivered on 31 October 2023, Judge Daly concluded that the Appellant had failed to put forward any evidence to establish any error on the part of the DPC, let alone a serious and significant error. On that basis the Court dismissed the Appeal, upheld the DPC's Decision and made an award of costs in favour of the DPC.				Proceedings concluded.

Supervision

The DPC's Regulatory Strategy identifies a key strategic goal to support organisations and drive compliance. Supervisory engagement with organisations in the public, private, and voluntary sectors enables the DPC to understand how personal data are being processed, and to promote the awareness of organisations of their data protection obligations in context. This allows the DPC to support organisations in identifying potential data protection problems in the development of new products or services, and implementing best practice compliance solutions at the earliest opportunity.

The DPC promotes open and regular communication with organisations that process personal data, as well as sectoral representative bodies, DPO networks, and legislators, as a key method to drive accountability and a wider culture of data protection compliance. Supporting organisations in understanding their own obligations assists in providing them the legal clarity and consistency to develop new products and services in a compliant and accountable manner, as the GDPR was intended to do. The DPC also believes that proactive engagement with organisations advocates strongly for the upholding of the data protection rights of individuals by mitigating against potential infringements before they occur.

Supervisory engagement with organisations is an important part of the DPC's regulatory toolkit as, in addition to supporting organisations and driving compliance, it can highlight data protection concerns and provide an opportunity for the recommendation of remedial actions. Further, if during engagement with the supervision function it appears necessary for the DPC to take enforcement action against a particular organisation, the DPC is not precluded from taking relevant action in such circumstances. This approach contributes to the DPC's efforts to ensure that its resources are put where they can achieve the most good, and ultimately can produce better results for all stakeholders.

The DPC had **751 supervision engagements** during 2023. The sectoral breakdown is as follows:

Supervision Engagements 2023	
Law Enforcement	34
Health	58
Public Sector	90
Charities/Voluntaries	21
Children/Family	25
Private Sector & Financial	112
Multinational Technology	391
Other	20
Total	**751**

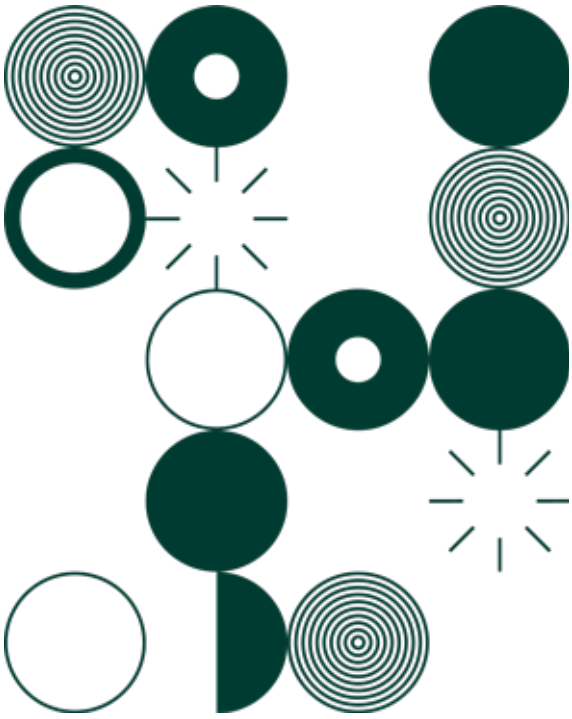
In addition, across all sectors the DPC engaged in **250 supervision meetings** with organisations in 2023.

Legislative Consultation

The DPC provided guidance and observations on **37** proposed legislative measures in 2023. In so doing, the DPC seeks to promote **data protection by design** and the upholding of data protection rights within legislation where the processing of personal data may result.

In 2023, some of the legislative measures that the DPC engaged in consultation on were:

1. Digital Services Bill 2023
2. Domestic, Sexual and Gender-Based Violence Agency Bill 2023
3. Data Protection Act 2018 (Section38(4) and Section 60(6)) (Department of Foreign Affairs) Regulations 2023
4. Finance (No. 2) Bill 2023 – amendment of Taxes Consolidation Act 1997 Share Options
5. Garda Síochána (Recording Devices) (Amendment) Bill
6. Health Information Bill 2023
7. Planning and Development Bill 2023
8. Research and Innovation Bill 2023
9. Residential Tenancies (Right to Purchase) Bill 2023
10. SI 635/2015 Disabled Drivers and Disabled Passengers Fuel Grant Regulations (2015)



Throughout 2023, the DPC continued its engagement with DPOs, government departments, state agencies and advocacy groups across all sectors on a wide range of issues including:

Codes of Practice under the Circular Economy Act

Since the entry into force of the GDPR and the Law Enforcement Directive, the DPC has conducted a number of inquiries which determined the use of CCTV by certain local authorities for the purposes of prosecuting offences related to litter pollution and waste management to be unlawful.

In 2022, the Circular Economy and Miscellaneous Provisions Act 2022, remedied the legislative gap in this context by providing for the lawful deployment of recording technology, including CCTV, for the enforcement of litter pollution and waste management legislation subject to statutory codes of practice.

In 2023, the DPC was consulted by the Local Government Management Authority ('LGMA') in relation to three draft codes of practice prepared by the LGMA under the Circular Economy and Miscellaneous Provisions Act 2022. The purpose of these codes is to provide a legal basis for local authorities to use CCTV and mobile recording devices to investigate and prosecute certain waste and litter-pollution related offences.

The DPC played an active role in the scrutiny of these codes as required under the Act and made detailed observations on all three codes. In particular, the DPC made the following general observations:

- The codes must use legally-binding language in order to make clear to local authorities that they confer concrete legal obligations and are not mere guidance or examples of best practice which they may disregard.
- The codes must encourage local authorities to carry out comprehensive Data Protection Impact Assessments that consider privacy risks to the affected individuals both in the short and the long term resulting from any deployment of CCTV on a case-by-case basis.
- The codes must make clear that CCTV and mobile recording devices can only be used when it is necessary and proportionate to do so, and that the onus will be on local authorities to demonstrate this in each case.
- The codes must not open the door to a situation in which these tools are used purely because they are more convenient or popular than other options, as this would not represent a necessary or proportionate interference in the privacy rights of local residents and other affected individuals.

Through its engagement with these codes of practice under the 2022 Act, the DPC was committed to ensuring that they provided a clear legal basis for local authorities to use CCTV and other recording technologies where it is necessary, proportionate and in the public interest to do so. By the end of 2023, the three codes of practice had been finalised. All of the DPC's recommendations were taken on board by the code authors.

Adult Safeguarding and Data Sharing

Goal 2 of the DPC's Regulatory Strategy 2022-2027 sets out a commitment to safeguard individuals and promote data protection awareness while Goal 3 commits to prioritise the protection of children and other vulnerable groups. Following on from work commenced in 2022, the DPC continued a stakeholder engagement project on data protection in the context of adult safeguarding, and the wider context of service provision to at-risk adults. This in line with the DPC's to prioritise the protection of children and other vulnerable groups.

In 2023 the DPC engaged with relevant stakeholders (including advocacy groups, service providers across the public, private, and voluntary sectors, and other relevant regulatory bodies) in order to identify data protection issues arising in the context of adult safeguarding. The purpose of DPC's ongoing engagement is to develop a shared understanding of the practical issues affecting practitioners in this field, and the types of regulatory interventions that the DPC can most usefully make.

In June 2023, the DPC published a blog post addressing concerns regarding the failure by an organisation to share relevant information with a nursing home about a resident's criminal convictions, and the risk that they presented to other residents. The DPC confirmed that in this context, data protection law provides for the sharing of personal data in this context, where deemed necessary to prevent serious harm to other people.

As part of this broader engagement, in October 2023, the DPC delivered two workshop sessions to public sector social workers on access to information and data sharing, and data protection best practices in adult safeguarding. The workshops provided the DPC with a good opportunity to engage the social workers on issues that they come across in conducting their work on daily basis and a productive forum to discuss practical solutions.

In addition the wide stakeholder engagement in this area, the DPC has conducted an analysis of issues arising in complaints and queries received by the DPC from members of the public in relation to data protection and vulnerable adults. Based upon this cross-functional approach, the DPC's goal is to publish comprehensive guidance in 2024 for this sector which will assist in providing clarity and certainty to adult safeguarding organisations regarding their data protection obligations, in particular when dealing with sensitive situations.

In 2023 the DPC also engaged with the Law Reform Commission on the development of a report on the regulatory framework for adult safeguarding in Ireland. The DPC welcomed this opportunity to contribute to the discussion of data protection in this context, in particular the interplay between GDPR and other legislative and regulatory regimes which govern this area.

Data Protection in Sports

In 2023 the DPC commenced a wide-ranging examination of issues arising in data protection in sport. This project came out of the identification of a number of concerns regarding the processing of personal data at all levels (both professional and amateur), and in particular in relation to the processing of children's data. In particular, the proliferation of the use of technology in sport at all levels, and the resulting increase in the processing of health data for performance monitoring and other purposes, requires sporting organisations to carefully consider their data protection obligations.

As part of this process the DPC has engaged with both national and international stakeholders, including participation in a Forum on Human Rights and Sport under the Enlarged Partial Agreement on Sport of the Council of Europe. This engagement helped the DPC develop a fuller understanding of the scope of data processing that occurs in sports, as well as the complex data sharing systems that can arise between clubs, competition owners, governing bodies, and commercial partners; and the types of governance mechanisms that underpin processing in these contexts.

In September 2023, on foot of concerns arising from a number of sources, the DPC commenced a process of engagement with organisations at both local and national level on the processing of children's data in football. In particular, this engagement has focussed on resolving issues arising in relation to the registration of children to participate in league competitions and the security of identification documents processed for this purpose. In this context, the DPC acknowledges that sports organisations have legitimate purposes for processing data in this context e.g. to ensure the integrity of competitions. As organisations move towards implementing new technical and online solutions to manage this data, the DPC will continue to support them in meeting their data protection obligations, in particular to maintain the security and confidentiality of children's personal data.

The DPC's next step in this project will be to issue a questionnaire to a representative sample of organisations across the spectrum of voluntary and professional sports in Ireland to assess the state of play with regard to data protection compliance, and to gain a fuller understanding of the data protection landscape in terms of the relationships between parties. This will focus on the use of technology to collect and analyse player performance data, and the primary and secondary processing purposes of this data. The questionnaire will also address transparency and look for detailed information on how data subjects are informed about the processing of their personal data, with a particular focus on children and young people.

In addition to this, the DPC will continue to engage with player representative bodies in various sports to gain a fuller understanding of the concerns of athletes, and to assess the public awareness and understanding of the risks, rules, safeguards and rights in relation to processing in the context of sport, again with a particular focus on children. This will allow the DPC to design and implement appropriate interventions, such as the publication of guidance for sports clubs and other bodies operating in this area.

Voluntary Sector Engagement

Goal 5 in the DPC's Regulatory Strategy 2022-2027 sets out a commitment to support organisations of all size and drive compliance. As part of this strategic goal, in 2023 the DPC has worked in increase engagement with not for profit organisations (NGO), as many of these bodies have limited resources to expend on data protection compliance and might not, for example, have access to designated data protection officer. The DPC understands the challenges that this sector can face, especially in dealing with sensitive situations involving vulnerable adults, children and alleged criminal matters.

As part of this wider sectoral engagement, the DPC brought together a number of NGOs involved in local community work around the country who were affected by a personal data breach resulting from the

failure of a data processor, working on their behalf, to implement adequate data protection safeguards. The primary focus of this engagement was to promote the awareness of these organisations of their responsibilities with regard to managing third-party data processing agreements. Additionally, this engagement allowed room for discussion on a number of other various day-to-day scenarios experienced by the organisations, and it facilitated a valuable platform for peer-to peer engagement and the sharing of learnings.

This allowed the DPC to further understand the data protection challenges faced in this sector, and to develop new outreach and engagement opportunities in the sector to increase organisations' awareness of their obligations and responsibilities. It also highlights the importance of following up with organisations, who may have been affected by a third party data breach involving the personal data that they process, to assist them in implementing learnings and ultimately leading to better outcomes for individuals.

In 2024 the DPC will be further engaging with organisations across the charity and voluntary sectors with the aim to deliver similar opportunities through information sessions, webinars etc. to educate stakeholders on their data protection responsibilities.

DPC Audit of the Schengen Information System in Ireland

In 2023, the DPC completed its first audit of Ireland's participation in the second-generation Schengen Information System ('SIS II'). SIS II is the EU's information-sharing system for security and border management authorities in Europe. Since Ireland connected to SIS II on 15 March 2021, Irish authorities can now access and transmit data via a shared database with their EU counterparts for police and judicial cooperation purposes.

Ireland's connection to SIS II conferred significant new responsibilities on the DPC, as Ireland's designated authority responsible for monitoring the lawfulness of the associated processing of personal data by Irish police and border management authorities. In particular, the DPC must now carry out an audit of usage of SIS II by Irish authorities every four years.

The DPC formally commenced its first SIS II audit in September 2022. The DPC issued detailed desk questionnaires to the relevant units within the Department of Justice and An Garda Síochána, following which it conducted site visits and inspections of AGS headquarters and immigration control areas at Dublin Airport. The audit was concluded in July 2023, following which the DPC issued a number of observations and recommendations in relation to the processing of personal data by police and border management authorities in order to ensure appropriate safeguarding of individual data protection rights. The DPC received full cooperation from the relevant authorities in carrying out the audit, who accepted the findings of the DPC in full.

The DPC successfully completed its first audit of SIS II two years ahead of schedule. The next audit will take place on or before mid-2027.

Planning and Development Bill Consultation

In mid-2023 the DPC engaged with the Department of Housing, Local Government and Heritage (the Department), pursuant to an Article 36(4) GDPR prior legislative consultation request on the proposed Planning and Development Bill 2022.

A key feature of this Bill was the obligation it would impose upon planning authorities to publish or make available for inspection information relating to planning applications that would contain personal data. This data would derive from submissions received by the Planning Authorities in a variety of contexts e.g. planning applications, objections, submissions on development plans, etc.

While the DPC recognises the importance of ensuring transparency in the planning process, it is equally important to ensure that planning authorities only publish information that is strictly necessary to achieve this objective, and avoid a situation where potentially vast amounts of personal data are published on planning authority websites by default.

The DPC advised that the Bill should more clearly indicate to planning authorities what personal data should be published. This greater clarity could also be provided by way of Regulations, and by the development of a coordinated policy or common Code of Practice followed by all of the Planning Authorities.

The DPC understands and supports the public interest objective of ensuring a clear and transparent planning process and our submissions on the Bill were aimed at assisting the Department in achieving this goal while respecting and upholding the privacy rights of all data subjects.

The Irish Aviation Authority

In 2023, the DPC engaged with the Irish Aviation Authority (IAA), on foot of concerns raised by a private individual. This individual was required to register their aircraft with the IAA, and was concerned about the amount of information contained in the IAA's register of aircraft owners, which it makes publicly available on its website.

The IAA is required to maintain and make available for inspection a register of all aircraft owners in Ireland, and aircraft owners are required to provide their name and address when registering. The DPC advised that although it did not dispute the need to collect the personal data in question, the concern was that the publication of the register, without any limitations, on the IAA's website, appeared to go beyond what was specifically required by legislation. The DPC further noted that this processing had the effect that the names and addresses of private aircraft owners were publicly searchable on search engines, representing a significant invasion of their privacy. The DPC advised the IAA to reconsider the necessity and proportionality of the publication of the register in this form, paying particular regard to the potential risks posed to data subjects.

Following the intervention of the DPC, the IAA agreed to amend the register in order to redact the names and residential addresses of private individuals. The DPC was satisfied that this change more appropriately upheld the privacy rights of data subjects while enabling the IAA to meet its statutory functions. This engagement highlights the importance of public bodies appropriately balancing the legitimate public interest in transparency in the delivery of public services, such a licensing or registration, and the rights of individuals in respect of their personal data. It also demonstrates that a positive outcome for individuals can be achieved by timely supervisory engagement by the DPC with an organisation, and the subsequent implementation of measures to improve compliance with data protection obligations.

CCTV

2023 saw a significant increase in the number of queries received relating to the use of CCTV in areas where there is a higher expectation of privacy. As a result, the DPC published a detailed update of its CCTV guidance to address these issues and our expectations on the use of CCTV in such areas. In addition, in December, the DPC wrote to a number of sectoral representative bodies to make them aware of these developments and to ask them to circulate the guidance to their members. A copy of the Guidance on CCTVs for Data Controllers can be found on the DPC website, and includes a specific section on 'The use of CCTV in areas of an increased expectation of privacy'.

Case Study: Use of CCTV in a restaurant restroom

The DPC engaged with (Aarval Limited a data controller who operates two McDonald's franchises in Limerick) following concerns raised by customers about the use of CCTV in its restrooms. In particular the DPC was interested in ascertaining the lawful basis of the processing of the personal data and that the processing was carried out lawfully, fairly and transparently. The DPC also engaged with the master franchisor, McDonald's Ireland Limited, who, while not the data controller, could offer direction and assistance to franchisees in this area by acting as a liaison between the DPC and data controllers.

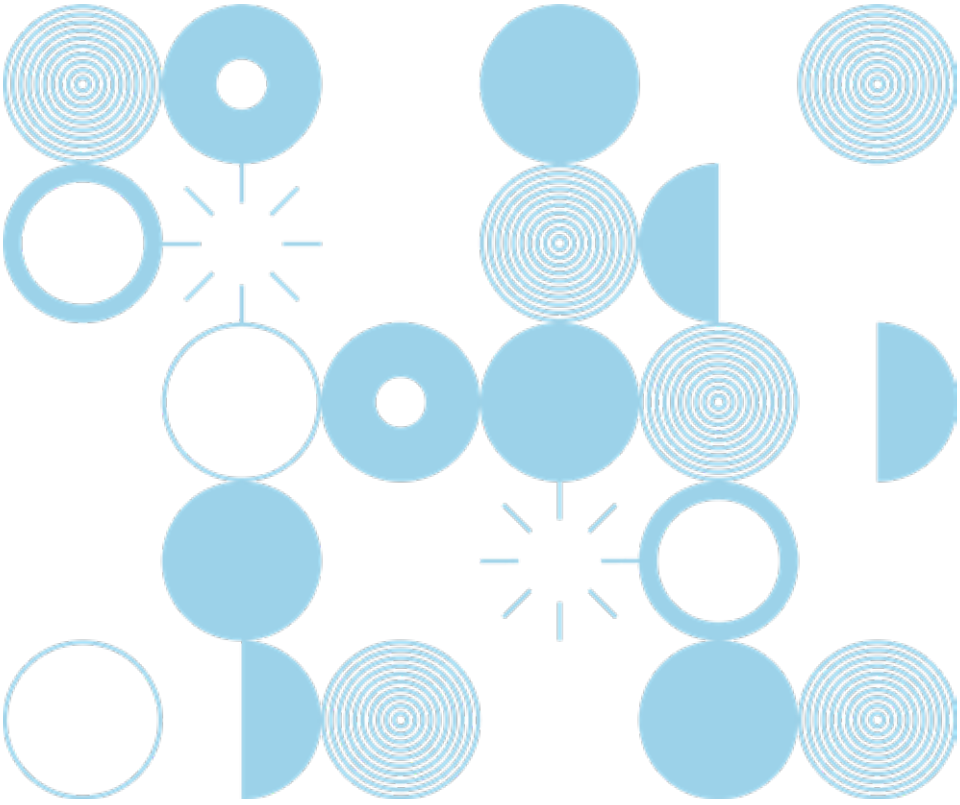
Under Article 6 of the GDPR, a data controller must have a valid lawful basis for processing personal data. One of the lawful bases that can be relied on by a data controller is that the processing is necessary for the purposes of legitimate interests pursued by the data controller (the lawful basis that the controller/restaurant sought to rely on here). The data controller in this instance claimed they were relying on a legitimate business interest to prevent anti-social behaviour and the risk of slips, trips or falls. Such legitimate interests may provide a legal basis for the processing of personal data, provided that the interests of the data controller are balanced with and not overridden by those of the individuals whose personal data are being processed. When relying on legitimate interests as a legal basis to utilise CCTV, the data controller should be able to demonstrate that it is genuinely in their interests to do so, that it is necessary to achieve their identified purpose(s), and that it does not have a disproportionate impact on the individuals whose personal data will be processed. This is of particular importance in areas such as restrooms, where individuals have a heightened expectation of privacy. The DPC considers that the threshold to be reached in any such assessment involving CCTV in restrooms will be at the very highest level.

In this case, the DPC requested a copy of the assessments conducted by the restaurant establishing the necessity and proportionality of placing CCTV in a public restroom. The DPC also requested documentary evidence of repeated anti-social behaviour in the form of incidents reported to An Garda Síochana. The data controller could not provide comprehensive assessments or evidence of anti-social behaviour. Overall, the DPC determined that the data controller did not implement sufficient measures or safeguards to counteract the risk of processing in such a private area and had not adequately demonstrated necessity for the processing or that its interest in preventing potential anti-social behaviour and/or reducing the risk of slip, trips or falls overrode the interests of its patrons who used the facilities.

Following engagement by the DPC with the data controller and McDonald's Ireland Limited , **the data controller was instructed to switch off the cameras and securely delete all footage stored** until a comprehensive assessment (which demonstrated justification for the CCTV) had been conducted. McDonald's Ireland Limited also confirmed that it had requested all its franchisees to **immediately discontinue the use of CCTV in these areas** and delete any personal data obtained from the CCTV until they are in position to demonstrate justification for the use of CCTV in restroom areas. The DPC welcomes the positive engagement demonstrated by McDonald's who fully engaged on the matter and addressed the privacy concerns of its customers.

Key Takeaway:

- The DPC strongly recommends that all data controllers familiarise themselves with our guidance on CCTV: Guidance on CCTVs for Data Controllers by including a specific section on 'The use of CCTV in areas of an increased expectation of privacy.



Vulnerable Customers

The DPC's Regulatory Strategy 2022-2027 sets out a commitment to prioritise the protection of children and other vulnerable groups. As part of this strategic goal, throughout 2023, the DPC engaged with several financial institutions and representative bodies regarding the concern whereby the GDPR and data protection law are being used as a barrier to accessing services.

One common concern raised with the DPC is the difficulties members of the deaf or hard-of-hearing community encounter in seeking assistance from a third-party interpreter to contact a service provider where data protection is being used as a barrier to such use. The DPC has previously published guidance advising that data protection law, as a rule, does not prevent organisations from dealing with somebody representing the account holder once they have taken reasonable and proportionate steps to ensure compliance with their security and confidentiality obligations.

The DPC will continue to prioritise this work throughout 2024.

Google BARD – Artificial Intelligence

In late May 2023, Google informed the DPC that it would be releasing BARD, (its experimental conversational Artificial Intelligence service) in the EU by mid-June. On reviewing the documentation provided, the DPC communicated that it had a number of observations regarding the extent of the assessments conducted by Google and lack of information in the documentation provided.

Google, following consultation with the DPC, delayed the release in order to implement initial DPC feedback and recommendations.

In doing so, Google made a number of changes regarding transparency for users prior to launch including:

- In-product contextual disclosures;
- Bard Privacy Notice webpage Bard Privacy Notice updates;
- A more prominent warning notice; and
- Additional educational content on Bard and technology.

Google also committed to undertake further reviews of risk assessments, provide updated documentation, and to further update the DPC with reports on the progress being made in terms of ensuring compliance with GDPR in relation to Bard.

As a result, the DPC has made some further recommended changes to Bard regarding information provided to users and retention periods for personal information. Given the novelty of this technology, it is incumbent upon Google to ensure that the information regarding users personal data is accessible, clear and easy to understand. The DPC continues to undertake a detailed assessment of the voluminous and evolving documentation on Bard and, as with other AI applications, aims to closely monitor developments in 2024. In addition, the DPC is leveraging existing fora hosted by the European Data Protection Board (such as its ChatGPT Taskforce, Technology Expert Subgroup) to exchange information and inform the discussion on AI and Generative AI processing with a view to establishing a consensus amongst EU regulators regarding compliance and best practice under the GDPR. The DPC will continue to work closely with our EU colleagues into 2024 to achieve these objectives.

Instagram Tagging

In November 2022, the DPC began engaging with Meta in relation to tagging on Instagram. Tagging is the process by which one Instagram user who is the original creator of a post or a reel notifies another user of the specific content they have created. In February 2023, the DPC wrote to Meta on their tagging policy and highlighted a number of areas for further consideration.

One such area related to the notification shown when users under 18 years, whose accounts are set to private by default, wanted to tag a public account that they do not follow. This notification would state, 'Account couldn't be tagged. Make your account public to tag others who don't follow you'. This notification also contained a 'Go to settings' button that took the user to a menu where they could change their account from private to public. The DPC noted that this notification did not appear to warn users who are under 18 years of the potential consequences of making this change nor did it redirect these users to any FAQ or Help Centre article.

In September 2023, Meta confirmed to the DPC that it had taken the DPC's recommendations/ guidance on board and was making changes to user notifications. The notification was updated to, 'Account couldn't be tagged. Your account is private, so you can tag only your followers. You can manage your privacy in Settings'. Furthermore, 'Go to settings' was replaced with a 'Learn more' button that takes users to a Help Center article where they can learn more about (1) how to make their user account private at any time, (2) the differences between private and public accounts, (3) how users can manage privacy on Instagram and (4) information for parents on 'who can see my teen's posts on Instagram'.

Microsoft 10 (Windows)

The DPC, in August 2023, concluded a high-level review of the Microsoft Windows 10 Privacy Statement. The review was undertaken to understand the extent of privacy information being presented to individuals in the EU/ EEA. The DPC carried out an extensive mapping exercise which highlighted numerous layers and links contained within the Privacy Statement which were not necessarily privacy related and in some instances were circular bringing the individual back to the main Microsoft Privacy Statement.

The DPC's recommendations/ guidance and observations drew attention to an organisation's transparency obligations under the GDPR.

In November 2023, Microsoft advised the DPC that it intends to conduct a thorough review of their Privacy Statement and that they are committed to making any necessary changes to reflect their goals of transparency and clarity. This engagement will continue with Microsoft into 2024.

Director of Public Prosecutions Catherine Pierse addresses DPC staff. February, 2023.

RayBan Meta Smart Glasses

In 2021, the DPC engaged with Meta on their new wearable technology product; Smart Glasses a product produced with Ray Ban. Using voice-activated controls, the Smart Glasses allow the wearer to capture images, video, call recording, and have a voice assistant. After an extensive engagement, wherein the DPC provided feedback on its concerns about the means by which those captured in the videos and photos would receive notice that they were being recorded, in 2023 Meta announced a new version of the Smart Glasses. On foot of concerns raised by the DPC, Meta had made changes to the design to increase privacy design measures and make the Smart Glasses operation less covert in nature including:

- Physical increase in size of external facing privacy LED light to give effective means of notice that recording is occurring (LED light size more than doubled);
- a blinking pattern added to the LED light when recording;
- additional controls to prevent accidental triggers of recordings; and
- additional privacy measures to prevent tampering or usage by unauthorised persons.

These changes were made to ensure a more effective means of giving notice to individuals and minimise the risk of inconspicuous media capture to address concerns raised by the DPC.

Technology companies Law Enforcement engagement policies and procedures

Under Article 57 of the GDPR, the DPC has a duty to monitor and enforce the application of the GDPR and to promote the awareness of data controllers and processors of their obligations under the GDPR. In this context, 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.

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, respect the principle of data minimisation when responding to requests for user data and the internal guidance and/ or workflows that is available to the controller's staff who process such requests.

Further to this review, the DPC wrote to each controller with feedback. Whilst many controllers had robust and well considered policies and procedures in place, a number of controllers had room for improvement. For those controllers whose policies were not considered to be sufficiently developed, recommendations were provided on further action that they could take in this regard. This included detail on useful practices that would assist with eliminating any gaps in terms of data protection.

For those organisations where the DPC identified room for improvement, they are expected to revert to the DPC during 2024 with detailed feedback on how they addressed the recommendations.

Children's Data Protection Rights

Data Protection Toolkit for Schools

In the course of its supervision and engagement activities in 2023 the DPC identified a number of areas which schools, as a sector, appeared to be finding challenging from a data protection compliance perspective. As set out above, the DPC's Regulatory Strategy 2022-2027 sets out a commitment to prioritise the protection of children along with other vulnerable groups. As part of this strategic goal, in 2023, 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 (PDST) 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), 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, the DPC commenced drafting of a new 'Data Protection Toolkit for Schools' resource, which includes a detailed guidance document, a sample Data Protection Impact Assessment (DPIA) template, a checklist for responding to subject access requests, 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 toolkit will further assist schools and the wider education sector in meeting their data protection obligations.

Children's Data Case Study:

Sporting Organisation and the Posting of Images of Children

A parent of a young child contacted the DPC as they were concerned that photographs of their child would be posted on social media by a sporting organisation. The individual had been informed that upon enrolling their child with their organisation, they were agreeing to allow photographs or videos of activities, which may include their child, being used in promotional material on their website or on social media platforms used by them for promotional purposes.

Separately the same organisation contacted the DPC raising a query in relation to the same matter. In their contact, the organisation admitted that it did not have the appropriate technical measures in place for those who did not wish to have photographs of their child published.

As the issues raised concerned the public posting of images of children, the DPC viewed this matter as serious enough to warrant examination of the issue by its Direct Intervention Unit.

The DPC engaged with the sporting organisation, highlighting the requirements under Article 6 of the GDPR (lawful basis) for such processing and provided information on the conditions of consent under Article 7. The sporting organisation actively and willingly engaged with the DPC, acknowledging that the complaint served to highlight the deficits in its data protection processes. Following this engagement, the sporting organisation updated their practices and procedures.

Key Takeaway:

- The publication of images of children must have a very specific lawful basis under Article 6 of the GDPR. If relying on consent as a lawful basis for the processing, the purpose must be made clear and a stand-alone consent should be sought.

Children's Policy Guidance

Publication of guidance for parents

In early 2023, the DPC produced four short guides for parents on children's data protection rights under the GDPR. These guides are intended to help parents to understand their children's rights and to answer questions that can arise in typical situations where those rights apply.

- **My child's data protection rights – the basics:** This guide outlines some of the issues that can arise when a parent seeks to exercise data protection rights on behalf of their child.
- **Children's data and parental consent:** This guide looks at the meaning of the 'age of digital consent' and outlines when parents' consent may be needed for processing their child's personal data, and how parents can approach those cases.
- **Protecting my child's data:** This guide is intended to help parents understand the rights that they have in relation to their children's data and gives some useful advice on how to protect their children's rights.
- **Are there any limits on my child's data protection rights?** This guide outlines some important limits to how and when children's data protection rights may be exercised, whether by children themselves or by parents on their behalf. It outlines some common situations where these can arise and suggests ways in which parents can address them.

#PauseBeforeYouPost campaign

In August 2023, the DPC launched a **#PauseBeforeYouPost** campaign on social media, aimed at raising awareness of the risks involved in posting back-to-school photos of children online. The campaign also provided tips on how to keep your children's information safe, such as avoiding oversharing information, making sure there is no identifiable information in the background of the photo, and the importance of talking to children before posting their photos online.

#PauseBeforeYouPost campaign

External engagements

In order to keep industry and the wider public abreast of the DPC's activities in the field of children's policy, staff from the DPC also spoke at numerous external events over the course of 2023, including the Children's Right's Alliance 'Know Your Rights' Conference, and the 'Growing Up in the Digital Age Summit' hosted by Google. The DPC also published a podcast on '5 Years of the GDPR – A Spotlight on Children's Data', and recorded an interview for Webwise's 'Casting the Net' podcast, a youth-led audio series hosted by teenagers, to discuss what teens need to know about data protection.

The DPC also participated as a member of a number of external working groups focused on children's data protection issues, including the International Age Assurance Working Group (a global forum for data protection authorities, online-safety regulators, and international organisations to learn from each other's experiences in the field of age assurance) hosted by UK Information Commissioners Office (ICO). The DPC is also an active member of the Global Privacy Assembly's Digital Education Working Group, and contributed to the group's roadmap for 2024.

The DPC's intensive work on children's data protection rights during 2023 saw the DPC nominated to represent the European Data Protection Board (alongside Spain and France) on the newly formed Task Force on Age Verification under the Digital Services Act. The European Commission is establishing this task force with the aim of fostering cooperation with national authorities of Member States with expertise in the field of age verification in an effort to identify best practices and standards. The role of the EDPB in this group will be to provide a data protection perspective on matters pertaining to age verification.

Engagement with statutory bodies

Throughout the course of 2023, the DPC met with several statutory bodies to discuss developments in the area of children's data protection issues, including the Federal Trade Commission (FTC) in the United States, and Ireland's Coimisúin na Meán. As part of its engagement with Coimisúin na Meán, the DPC submitted a response to its Call for Inputs on Ireland's first binding Online Safety Code. The DPC's submission focused on the areas of age assurance and safety by design. The DPC also held meetings with its French and UK counterparts, the Commission Nationale de l'informatique et des Libertés and the Information Commissioner's Office, throughout 2023 to exchange views and discuss the latest developments in both DPA's work on children's data protection rights.

The DPC also engaged with the European Commission to discuss an upcoming EU Code of conduct on age-appropriate design, a key action under the Better Internet for Kids+ strategy (BIK+). The Code will build on the regulatory framework provided in the Digital Services Act will be in line with the EU's Audiovisual Media Services Directive (AVMSD) and the GDPR.

Codes of Conduct

The DPC engaged with Technology Ireland throughout 2023 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 will focus on certain topics of the GDPR that are deemed particularly important to drive higher standards of protection for children's personal data online. The DPC will continue to engage with Technology Ireland into 2024 on this Code in line with our obligation to encourage the drawing up of codes of conduct in relation to the processing of children's personal data, as per Section 32 of the Irish Data Protection Act 2018.

European Data Protection Board (EDPB) guidance on children's data

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 DPC is pleased to be involved in such an important piece of work that seeks to harmonise the approach at an EU level, to be taken to the critical area of the processing of children's data.

The DPC is also contributing to significant work on the complex issue of age verification in the digital environment.

Data Protection Officers

Data Protection Officers (DPOs) are a key component in Ireland's data protection compliance record. For DPOs to operate effectively they need the support of Senior Management and to have regular and direct communication lines into their organisation's Management Board.

A key part of the DPC's strategic goal of supporting organisations and driving compliance is working with Data Protection Officers (DPOs) to increase the knowledge and impact of their role. DPOs play an important role in data protection compliance for the organisations in which they have been designated including through providing advice on data protection impact assessments, and monitoring the implantation and efficacy of data protection policies. As the contact point for the DPC in their organisations, DPOs are an important group of stakeholders, and the DPC is committed to supporting them (as well as non-designated data protection data protection operatives) in making their roles more effective.

As part of the requirements of GDPR, the DPC must be notified of the formal designation of a DPO by an organisation. As of the end of the 2023 the DPC has been notified of the designation of 3,520 DPO broken down by sector as follows:

Notification of Data Protection Officers	
Public Sector	357
Private Sector	2932
Not-for-profit Sector	231

DPO Networks

Since the application of GDPR in 2018, networks of DPOs coming together in various sectors have proven to be a valuable resource for the DPC in engaging with those sectors, and have also provided forums for the sharing of information and the collaborative development of compliance solutions. In 2023 the DPC engaged with a number of networks, including the Civil Service DPO Network, a grouping of DPOs from across the public sector, and the Health Research Data Protection Network, which brings together DPOs working in hospitals, academia and other settings to address issues arising in data protection and health research.

In the private and semi-state sectors, the DPC engaged with the DPO Network of the Banking and Payments Federation of Ireland, the DPO network of Telecommunications Industry Ireland/IBEC, and the Insurance Ireland DPO Network/Working Group. These engagements are valuable in allowing the DPC to platform current and upcoming data protection issues affecting these sectors.

In December 2023, the DPC brought together a group of DPOs and non-designated data protection champions working in NGOs active in the local community sector to encourage the development of a new network for information sharing and problem solving. The DPC intends to expand on this work in 2024, to increase its reach to sectors and organisations that may be less well-resourced than others when it comes to managing data protection compliance.

DPO Events

As part of its broader programme of outreach and engagement, the DPC has contributed to a number of conferences and events for DPOs and privacy practitioners including the annual conference of the Association of Data Protection Officers, and the annual PDP Data Protection Conference. In September 2023, the DPC contributed to new course run by the Institute of Public Administration, 'GDPR and Data Protection Programme for DPOs in the Public Service', aimed at providing specific and relevant information to those acting as DPOs in public bodies and agencies across Ireland. The first iteration of this course was well received, and will run again in 2024, with the DPC's continued participation.

EDPB Coordinated Enforcement Framework (CEF) 2023 CASE STUDY

The DPC participated in the 2023 Coordinated Enforcement Framework (CEF) Topic 'The Designation and Position of Data Protection Officers'. EDPB members decided to prioritise this topic given the position of Data Protection Officers ('DPOs') under the GDPR as intermediaries between Supervisory Authorities, individuals and the business units of an organisation. This action aligned with the DPC Regulatory Strategy 2022-27 to cooperate and communicate with peer data protection authorities on emerging issues and working with DPOs to increase the knowledge and impact of their role.

The DPC participated in this action as a fact-finding exercise with DPOs established in Ireland with the aims being to:

- help to identify emerging issues;
- assess the knowledge, expertise and impact of the DPOs; and
- generate deeper insights into the role at an EU level.

The DPC launched their participation in the action on the 15th of March, 2023, by means of a fact-finding exercise whereby 100 DPOs were contacted across all sectors in Ireland, private, public and not-for-profit, to participate in a questionnaire with flexibility in whether the DPOs or the organisation/controller answered the questions.

Following the collation of the completed questionnaires, the DPC produced an aggregated national report, which was fed into the broader EDPB report.

The DPC found three substantive issues in its national report:

1. The Resources of the Data Protection Officer (Article 38.2 GDPR).
2. Conflicts of Interests (Article 38.6 GDPR).
3. Tasks of the DPO (Article 39 (1) (a to e) GDPR.

Some findings in the DPC national report include:

- Approximately 33% of respondents replied that they do not have the resources sufficient to fulfil the role of a DPO. Upon further analysis of the responses it was discovered that the high majority of respondents who stated they do not have adequate resources sufficient to fulfil the role of a DPO came from the Public and Not-for-Profit Sector.
- Approximately 36% indicated that the data protection officers' tasks are performed in addition to other tasks, but not as the main task. In that regard it was noted that many of the non-data protection tasks did not compliment the role of a DPO such as Health and Safety Officer, Human Resource Officer, Employee Engagement Manager, Communications Officer.
- Approximately 80% of DPOs replied they have at least 3 + years of experience working on the application and the interpretation of data protection requirements.

The completed EDPB report including the DPC national report is available here:

https://edpb.europa.eu/news/news/2024/edpb-identifies-areas-improvement-promote-role-and-recognition-dpos_en

The DPC will be participating in the 2024 CEF action, which will concern the implementation of the right of access by controllers.

Deputy Commissioner Tony Delaney and Commissioner Helen Dixon Q&A at DPC staff day. December, 2023.

International Activities

European Data Protection Supervisory Bodies

In 2023, the DPC attended and actively participated at all monthly plenary meetings, as well as expert subgroup meetings (over **150** meetings in total).

Cooperation with other EDPB supervisory authorities 2023

The DPC continued to invest considerable resources in the day-to-day operation of the One Stop Shop under the GDPR at various levels in the performance of its role as a Lead Supervisory Authority, including seeking the assistance of other authorities on a broad range of matters as well as keeping them informed of pertinent issues and developments. Voluntary Mutual Assistance requests are used to communicate details of OSS complaints and follow up communications and actions on complaints, as well as notification to Supervisory Authorities of updates on supervision cases and inquiries and sharing of documents. Formal Mutual Assistance requests are used to formally request information from another Supervisory Authorities or to request that a Supervisory Authority take certain actions.

As part of the on-going co-operation and communication between the DPC and the other EU/ EEA Supervisory Authorities, the DPC responded to **800** voluntary and formal mutual assistance requests from other European Regulators.

In addition to engagement with other EU/ EEA Supervisory Authorities in the context of complaints and inquiries, on some **100 occasions** the DPC provided written updates to all other authorities on impending internet/ social media platform product or service launches in the EU and invited their input on identifying any data protection concerns.

Examples of issues on which other EU/EEA Supervisory Authorities were briefed and their input sought included Google BARD and Meta Threads.

In addition to extensive engagement with EU/EEA supervisory authorities, the DPC also engaged with data protection authorities across the globe, including:

- The UK's Information Commissioner's Office;
- The International Digital Regulation Cooperation Forum;
- Participation in the British, Irish, and Islands Data Protection Authorities (BIIDPA) forum;
- Bilateral engagements with the US Federal Trade Commission;
- The European Case Handling Workshop in Bern;
- The Spring Conference of Data Protection Commissioners in Hungary; and
- Supporting the University of Maastricht in delivery training sessions to data protection authorities.

In 2023, the DPC submitted the following to the GDPR Article 60 cooperation process:

Draft Decisions	Final Decisions	Article 65 Process
18	12	2

In addition, the DPC submitted through the Article 60 cooperation mechanism **229** notifications of amicable resolutions achieved in cross-border complaints.

Furthermore, as a **Concerned Supervisory Authority**, the DPC reviewed:

- **113** Article 60 Draft Decisions/ Revised Draft Decisions;
- **15** Informal Consultations; and
- **21** Preliminary Draft Decisions.

Data Protection Certification

Certification has been a growing area for the EDPB and the DPC in 2023. The DPC continues to work closely with EU Colleagues on a number of Certification Schemes. The DPC are also engaging closely with colleagues on improving internal procedures and developing further guidelines for stakeholders.

The DPC is the relevant 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. 2023 saw the DPC working 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 which is expected to be finalised in 2024.

The DPC attended two intensive workshops on Certification in 2023 hosted by the Agencia Española de Protección de Datos from Spain and the Commission Nationale pour la Protection des Données from Luxembourg respectively. These workshops were attended by representatives of data protection authorities from the EDPB. The workshop held in Luxembourg also hosted certification professionals from all over Europe (including INAB officials) to discuss the development, the challenges and future opportunities for the GDPR certification

In addition, both workshops covered a number of other areas such as:

- issues arising when using the certification as a tool for data transfers to countries outside the European Economic Area (EEA);
- the methods of cooperation between the EDPB expert groups, the national accreditation bodies and other external stakeholders for the GDPR certification schemes assessment;
- tools and methods for the criteria assessment; and
- Pre-defined set of certification and cooperation related issues that have arisen in relation to current and past certification scheme applications.

Deputy Commissioner Graham Doyle and NewsTalk tech reporter Jess Kelly discussion at DPC staff day. June, 2023.

International Transfers – Binding Corporate Rules

The DPC has a role in the assessment and approval of Binding Corporate Rules (BCR) applications from multi-national companies.

BCR were introduced in response to the need of organisations to have a global approach to data protection where many organisations consisted of several subsidiaries located around the globe, transferring data on a large scale. BCR form a legally binding internal code of conduct operating within a multinational group, which applies to transfers of personal data from the group's EU/EEA entities to the group's non-EU/EEA entities. BCR contain enforceable data subject rights and they must be approved by the competent Data Protection Authority.

During 2023, the DPC was lead reviewing supervisory authority in relation to **22** BCR applications from **14** different companies. **Four** of those applications were **given approval** in 2023 – Controller and Processor BCR for Autodesk Ireland Operation Unlimited and Controller and Processor BCR for Informatica Ireland EMEA UC.

The DPC also assisted other European Data Protection authorities by acting as co-reviewer for another SA on **5** BCR applications and acted as rapporteur on drafting teams for Article 64 Opinions on **3** BCR in 2023.

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 2023 the DPC was lead Supervisory Authority on **26** approved BCR for **18** different BCR holders. The list of these approved BCR files is listed on our website.

In addition the EDPB issued a total of **26** Article 64 opinions on BCR applications in 2023 and the DPC reviewed each of these applications.

Deputy Commissioner Ultan O'Carroll and Simon McDougall (formerly ICO) Q&A at DPC staff day. June, 2023.

DPC Attaché Position – Brussels

The DPC established a new position of Data Protection Commission Attaché in Brussels during 2023. In light of its experience in the five years since the GDPR's application, the DPC identified a strategic need for a full-time DPC presence in Brussels. Many of the DPC's key stakeholders are Brussels based or Brussels-adjacent given the DPC's unique position as the Lead Supervisory Authority in Europe for a large number of multinational technology companies.

These stakeholders include 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.

The Attaché, through attending events, meetings, and providing briefings, seeks to bolster the DPC's proactive engagement with these stakeholders in an effort to ensure the DPC's work is accurately communicated to them and understood. Equally, this engagement means the DPC can receive feedback from these stakeholder groups on an ongoing basis.

The Attaché position demonstrates the DPC's commitment to fostering fruitful relationships with international colleagues and Brussels based stakeholders so it can better deliver on its European focussed regulatory responsibilities.

Communications, Corporate Governance and Human Resources

Communicating Data Protection

In the dynamic and ever-evolving realm of data protection, effective communication and stakeholder engagement are paramount to fostering understanding, building trust, and ensuring compliance with the principles of privacy and data protection.

The DPC is committed to providing timely and accurate information to the public, fostering transparency and accountability in the data protection landscape. The DPC actively engages with the media, issuing press releases, providing interviews, and responding to inquiries to ensure that the public is kept informed of the DPC's activities and decisions.

Over the course of 2023, the DPC published a total of **14** press releases leading to significant coverage on international and national level media.

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 **6,800** during 2023, to over **48,100**, an increase of **114%** on last year's figures. There was an organic reach of over **1.4 million**, with strong engagement across the board.

New Guidance
Records of Processing (Article 30) Guidance.
My child's data protection rights – the basics.
Children's data and parental consent.
Protecting my child's data.
Are there any limits on my child's data protection rights?
Updated Guidance
Transfers of Personal Data to Third Countries or International Organisations.
Complaints handling, Investigations and Enforcement For Individuals.
Guidance on the Use of CCTV – For Data Controllers

DPC Funding and Staffing

The 2023 gross estimate provision for Vote 44 — Data Protection Commission was €26.364M (2022: €23.234M) of which €17.100M (2022: €15.970M) was allocated for pay related expenditure, and €9.264M (2022: €7.264M) of which was allocated to non-pay expenditure. The funding for 2023 represented an increase of €3.1M on the 2022 allocation.

2023 saw the on boarding of **44** new colleagues in the DPC. The number of DPC staff at year-end 2023 was **210**.

The DPC will continue to drive recruitment during 2024 through a combination of open recruitment and the promotion and development of DPC staff.

Recruitment

Following a procurement exercise, a contract was put in place with an external recruitment agency. This, along with running competitions through PAS should impact positively on the DPC's continued recruitment drive and will be a key tool in allowing the DPC to recruit the staff it needs to discharge its domestic and international functions by filling critical roles.

Competitions Run in 2023	New Joiners	Promotions
AP Confined Competition HEO Open Legal Analyst Competition HEO Open Regulatory Investigator EO Confined Competition	44 new hires in 2023	15 DPC staff members were promoted within the DPC in 2023.

Professional Development

In 2023, the DPC continued to prioritise the professional development of all of its staff, developing a Learning and Development Strategy which delivered a range of skill enhancements in the areas of leadership development, personal professional development and wellbeing.

Employee Engagement Forum

An Employee Engagement Forum was established in 2021. The Forum has a diverse and inclusive membership, with representation at each grade an essential requirement. In 2023 the Forum met five times. The purpose of the Forum is to contribute to the DPC's commitment to becoming an Employer of Choice through enhancing the employee experience for staff.

Corporate Governance

The DPC has in place a Corporate Governance Framework which sets out how the DPC is governed and describes the structures, policies and processes that are in place in order for the DPC to deliver on its statutory obligations.

Internal Control Environment

The Accounting Officer's Statement of Internal Financial Control for 2023 will be published on the DPC's website with its Financial Statement later in the year.

DPC Audit and Risk Committee

In line with the Corporate Governance Standard for the Civil Service (2015), and also with regard to the Code of Practice for the Governance of State Bodies (2016), the DPC established its own Audit and Risk Committee, as a Committee of the DPC, effective from 1 January 2020. The second term of the Audit and Risk Committee commenced on 1 January 2023 which runs for a three year period.

The members of the Committee in 2023 were:

- Conan McKenna (chairperson);
- Karen Kehily;
- Brid Rosney (RIP)
- Tara McDermott (joined Q4 2023)
- Michael Horgan; and
- Graham Doyle.

Five meetings of the Audit and Risk Committee were held in 2023.

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.

Freedom of Information (FOI)

In 2023, the DPC received a total of **52** FOI requests. Three were granted, seven were partially granted, 41 were deemed out of scope, and one was withdrawn. The DPC's regulatory activity is exempted from FOI requests in order to preserve the confidentiality of our 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.

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

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

Regulation of Lobbying Act 2015

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

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

Engagement with Oireachtas members

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

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

The DPC's Regulatory Strategy 2022 – 2027 outlines how the DPC will continue to protect the data protection rights of individuals and has particular regard to the Public Sector Equality and Human Rights Duty. The DPC website content along with other published information is designed with regard to the principles of plain English, and the DPC has also increased its publication of audio resources. The Duty is also embedded into the Corporate Governance Framework and the Customer Charter and Action plan, as well as the Protected Disclosures notice which was published to the DPC's website in 2022.

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

21 Fitzwilliam Square

Dublin 2

D02 RD28

Ireland

Email:

DPCAccessibilityOfficer@dataprotection.ie

Customer Charter

The DPC's Customer Charter and accompanying Quality Customer Service Action Plan and Managing Unreasonable Behaviour and Contacts Policy for 2024 – 2026 are published on the DPCs 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.

APPENDICES

Appendix 1: Protected Disclosures

Report on Protected Disclosures received by the Data Protection Commission in 2023

The policy operated by the 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 2023:

- **No** internal protected disclosures (from staff of the DPC) were received.
- **Twenty Two** 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). Nine of the disclosures were accepted as valid protected disclosures.

Reference Number	Type	Received	Status	Outcome
01/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Open	Accepted and referred for potential investigation. Ongoing at year-end.
02/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Open	Accepted and referred for potential investigation. Ongoing at year-end.
03/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Closed	Insufficient detail provided, complainant did not follow up when requested.

Reference Number	Type	Received	Status	Outcome
04/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Closed	Not accepted as a valid protected disclosure, referred as a potential complaint.
05/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Closed	Insufficient detail provided, complainant did not follow up when requested.
06/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Closed	Insufficient detail provided, complainant did not follow up when requested.
07/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Closed	Accepted but could not progress. Insufficient detail provided, complainant did respond when further information was requested.
08/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Closed	Not accepted as a valid protected disclosure. Contents of submission outside the remit of the DPC.
09/2023	Section 7 (external, to 'prescribed person')	Q1 2023	Open	Accepted and referred for potential investigation. Ongoing at year-end .
10/2023	Section 7 (external, to 'prescribed person')	Q2 2023	Closed	Submission was not a protected disclosure. DPC not the intended authority.
11/2023	Section 7 (external, to 'prescribed person')	Q2 2023	Open	Accepted and referred for potential investigation. Ongoing at year-end.
12/2023	Section 7 (external, to 'prescribed person')	Q2 2023	Closed	Not accepted as a valid protected disclosure, directed to make a submission as a potential complaint.

Reference Number	Type	Received	Status	Outcome
13/2023	Section 7 (external, to 'prescribed person')	Q2 2023	Closed	Insufficient detail provided, complainant did not follow up when requested.
14/2023	Section 7 (external, to 'prescribed person')	Q2 2023	Closed	Insufficient detail provided, complainant did not follow up when requested.
15/2023	Section 7 (external, to 'prescribed person')	Q3 2023	Closed	Insufficient detail provided, complainant did not follow up when requested.
16/2023	Section 7 (external, to 'prescribed person')	Q3 2023	Open	Accepted and referred for potential investigation. Ongoing at year-end.
17/2023	Section 7 (external, to 'prescribed person')	Q3 2023	Open	Accepted and referred for potential investigation. Ongoing at year-end.
18/2023	Section 7 (external, to 'prescribed person')	Q3 2023	Open	Accepted and referred for potential investigation. Ongoing at year-end.
19/2023	Section 7 (external, to 'prescribed person')	Q3 2023	Closed	Not accepted as a valid protected disclosure, referred as a potential complaint.
20/2023	Section 7 (external, to 'prescribed person')	Q4 2023	Open	Accepted and referred for potential investigation. Ongoing at year-end.
21/2023	Section 7 (external, to 'prescribed person')	Q4 2023	Closed	Not accepted as a valid protected disclosure. Complainant did not intend to submit a protected disclosure. Directed to website.
22/2023	Section 7 (external, to 'prescribed person')	Q4 2023	Under consideration	Engaging with complainant at year – end.

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

Energy Report 2023.

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 Winer 2023/24.

Over the last 12 months, we have made significant progress in meeting our energy efficiency and greenhouse gas targets across the organisation.

Office	% Reduction in actual consumption in last 3 years validated data
Fitzwilliam Sq – Electricity	44%
Satellite Office – Electricity	31%
Portarlington – Electricity	25%
Portarlington – Natural Gas	6%

DUBLIN.

21 Fitzwilliam Square

The head office of the DPC is located at 21 Fitzwilliam Square, Dublin 2. Energy consumption for the office is solely electricity, which is 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

DPC currently maintains additional office space in Dublin to accommodate the increase in staff numbers. This office was sourced by OPW and DPC took occupancy in October 2018. This office will be maintained until a new permanent head office is ready to facilitate the DPC's Dublin-based staff and operations. 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 2022 (last validated SEAI figures available) is as follows:

	Electrical	Natural Gas
Dublin		
Fitzwilliam Sq.	52,440 kWh	
Satellite Office	61,653 kWh	
Portarlington	30,600 kWh	46573 kWh

Overview of Environmental policy /Statement for the organisation

The Data Protection Commission 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.

Representatives from the DPC meet with members of the PFAI to discuss the use of player data. September, 2023.

Appendix 3: DPC Statement of Internal Controls

The Financial Statement of the Data Protection Commission for the year 1 January 2023 to 31 December 2023 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 2023 by the Comptroller and Auditor General.

**European Union Agency for Fundamental Rights Director Michael O'Flaherty and Comissioner Helen Dixon.
September, 2023.**

**Deputy Commissioner MB Donnelly, speaking at the HSE Safeguarding Conference on data sharing in context of adult safeguarding.
November, 2023.**

Appendix 4: Case Studies

A key objective of the DPC is to provide a responsive and high-quality information service to individuals and organisations regarding their rights and responsibilities under data protection legislation. The DPC achieves this through its public-information helpdesk service, which responds to queries from individuals and organisations and through its complaint handling process.

This chapter of the report highlights a selection of the types of queries and complaints the DPC has progressed in the last twelve months. Each case study provides a short summary of the key takeaways.

Case Study 1:

Organisation publishing alleged personal data

The DPC received a query from an individual relating to what appeared to be the unintentional inclusion of their property on an advert published by a property website. The individual advised that the property website had published on its website an image of a property for sale as well as a number of other neighbouring properties. The owner of one of these other properties was the individual that contacted the DPC.

The individual first contacted the DPC via email raising their concern and followed up a short time later with a phone call to the DPC Helpdesk. During the Helpdesk call, the individual advised the DPC that the image contained, a photograph of their house along with their address.

In response to this information, the individual was advised about the six lawful bases for processing personal data under Article 6 of the GDPR. They were also advised of the definition of personal data as set out in the GDPR; information concerning or relating to a living person who is identified or identifiable (such a person is referred to as a 'data subject').

The individual was further advised that while an image of a property alone may not constitute personal data, an image containing the property address as well as a house number, may entitle them to request erasure of this data from the property website. The DPC recommended that in the first instance, the individual make contact, in writing, with the owners of the property website requesting the removal of their property from the published images on the website.

Having followed the advice provided by the DPC, the individual reverted to the DPC to advise that owners of the property website had promptly complied with their request and had removed the image of their property from its website.

Key Takeaways:

- While the definition of what constitutes personal data is broad, it may not include images of a property or home when not accompanied by any other identifying information.
- While the DPC telephone Helpdesk is available to members of the public who have data protection queries, the DPC recommends that individuals consider approaching organisations in the first instance to give them an opportunity to respond to concerns in advance of raising a complaint with the DPC.

Case Study 2:

Alleged unlawful retention and alleged unlawful processing in relation to a newsletter

This case relates to an individual who alleged their personal data, in the form of their name, address and email address had been unlawfully retained and processed by a property management company.

The individual received an unsolicited email containing a newsletter from the company, despite not having a business relationship with the company for a number of years. The individual contacted the company requesting an explanation as to why the company had retained the individual's personal data. The company stated that it was previously the managing agent for a particular residential development that the individual had a business interest in. It advised that it had sent the email in error. The company informed the individual that it had now deleted their personal data from its database.

The individual was not satisfied with this response from the company and submitted a complaint to the DPC. Following engagement with the DPC the company explained it had been the managing agent for an owner management company and following the termination of its contract with the owner management company, it had failed to delete the individual's personal data from its database.

As part of the examination of this complaint, the DPC sought to establish if the company had a lawful basis for processing the individual's personal data by retaining it following the end of the respective contract. The company informed the DPC that it was relying on Article 6(1)(a) of the GDPR which states that processing shall be lawful where a data subject has given their consent. The company further stated that under the Property Services (Regulation) Act 2011 it was required to retain data for a period of no less than six years. The company further indicated that it was an oversight on its part that it had retained the individual's personal data beyond the six-year retention period. It also established that an administrative error had resulted in the individual receiving the unsolicited email.

The company acknowledged that it no longer had a lawful basis to process the individual's personal data by retaining it post the six-year period and confirmed that it had deleted all personal data relating to the individual. The company also confirmed what steps it had taken to improve the procedures for managing its database of contacts to ensure unlawful processing of this type did not recur.

Accordingly, the company did not adhere to the principles relating to processing of personal data in accordance with Article 5(1)(b) of the GDPR ('purpose limitation') when it used the individual's contact details to send them a newsletter when it should not have retained the individuals' contact details for this period of time. It also did not adhere to Article 5(1)(e) of the GDPR ('storage limitation') when it retained the individual's personal data which permitted the identification of the individual for longer than was necessary for the purpose for which the personal data was original obtained.

The DPC issued recommendations to the controller around its obligations to ensure that all processing is lawful, fair and transparent, as required under Article 5 of the GDPR and that appropriate technical and organisational measures are implemented to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

Key Takeaway:

- This case demonstrates that data controllers need to ensure there is a justification for the processing of the personal data in the first place in both the context of processing by retaining the personal data beyond the retention period and processing by using the personal data to communicate with the individual.

Case Study 3:

Partial compliance with a rectification request

Four years after the conclusion of an investigation into suspected plagiarism in an educational setting, an individual requested to have aspects of the internal report regarding the investigation rectified. The report was compiled following an independent investigation in which the individual was interviewed as a witness and not as the subject of the investigation.

The individual submitted the rectification request to the data controller, the individual's employer. As part of their request, the individual stated that there were a number of instances where the personal data in the report was inaccurate, incomplete or misleading, and requested that these instances be rectified in accordance with Article 16 of the GDPR. In its response to the individual, the education provider stated that it could not rectify the report but it could restrict access to it. As the individual was dissatisfied with this response, they submitted a complaint to the DPC.

In this instance, the DPC examined whether the educational provider was correct in its initial refusal of the rectification request. The education provider confirmed to the DPC that due to the passage of time since the report had been created, the investigator's notes had been destroyed as such it was unable to check the alleged inaccuracies and that as it was not the author of the report it could not alter the contents. The education provider offered, as a proposal for amicable resolution, to add a supplementary statement recording the individual's position to the report.

The individual refused the proposal as they were of the view that the report was incomplete as not all the evidence they provided was referred to in the report, and where it was quoted, they felt it was taken out of context.

It is important to note, that it is not the role of the DPC, nor is it encompassed within the right to rectification under Article 16 of the GDPR, to reassess or to repeat the work of an independent investigator, nor to undermine the professional opinion of an expert. The independent investigator provided their professional assessment of all evidence and testimony gathered during the investigation, and it was their professional discretion as to what material was relevant to be included in the report. The purpose of the individual's testimony was to inform the independent investigator in order to assist with the investigation. The fact that the individual disagrees with the assessment did not constitute the report as being inaccurate or incomplete.

The education provider further offered to delete the report which would cease the processing of the individual's personal data. Once again, the individual did not accept this offer.

The DPC was of the view that the report should be erased where it was no longer necessary for the education provider to retain it. Alternatively, the education provider should add the supplementary statement to provide a more accurate account of the events.

Key Takeaway:

- As with all data protection rights, the right to rectification is not an absolute right. The right must be examined on a case-by-case basis, depending on the nature of the personal data for which rectification is being sought, the purposes for which the personal data was collected and the circumstances of the case. In general, only personal data, which relates of a matter of fact, may be rectifiable. Personal data contained in opinions, whether personal or professional will generally not be amenable to the right to rectification.

General Accountability

Case Study 4:

Complaint of excessive personal data requested by a letting agent

An individual lodged a complaint with the DPC after they had viewed a rental property. In their complaint, they alleged that the letting agency had requested excessive personal data during the application process.

According to the individual, as they were unsuccessful in their application to rent the property, they made an erasure request to the letting agency under Article 17 of the GDPR for the deletion of their personal data. The letting agency responded to the individual advising that it had erased the personal data and confirmed that it had not shared personal data with any third parties. While the individual was satisfied with the response they received from the letting agent, they still had concerns regarding the amount of personal data that had been requested in the first instance. On this basis, they submitted a complaint to the DPC.

As part of the complaint handling process, the DPC contacted the letting agency requesting clarity on the different types of personal data it was requesting as part of the application process. The organisation confirmed it requested copies of identification; proof of current address; employment and previous landlord references; two-month bank statements; and a PPS number. The letting agency stated that the information was required for it to ensure the identity of the applicant and that the applicant can afford the property.

The DPC found that the organisation did not meet the principle of data minimisation under Article 5(1)(c) of the GDPR, which states: 'personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'. The DPC determined that the volume of personal data requested from the individual as a prospective tenant was excessive for the initial stage of an application process.

Key Takeaway:

- To comply with data protection requirements, requesting and obtaining specific personal information from individuals for the purpose of considering them as likely tenants would be more appropriately confined to those who will be entering into the actual letting agreement, rather than requesting all information at the start of the process. More information on this subject matter can be found at:
- **https://www.dataprotection.ie/en/dpc-guidance/requesting-personal-data-prospective-tenants**
- **https://www.dataprotection.ie/en/dpc-guidance/guidance-collection-personal-data-prior-viewing-property**

Access Request

Case Study 5:

Access request seeking third party data

An individual submitted a subject access request to their former employer. This individual then raised a concern with the DPC querying whether the company was obliged to provide them with the names of all of the employees who had been involved in compiling the response to the subject access request.

The DPC assessed the legal framework surrounding this question and responded to the query with reference to paragraph 73 of judgement C-579/21 of the Court of Justice of the European Union (CJEU) and article 15(4) of the GDPR. In this regard, the CJEU judgement had clarified that 'the employees of the controller cannot be regard as being 'recipients', within the meaning of Article 15(1)(c) of the GDPR [...] when they process personal data under the authority of that controller and in accordance with its instructions'.

Consequently, the DPC advised the individual that they were not entitled to a list of the names of the employees who had been involved in preparing their subject access request response under the category of 'recipients' as provided for in the GDPR under Article 15(1)(c) and Article 15(4) of the GDPR.

Key Takeaway:

- Individuals are only entitled to their own personal data when making an access request, generally you are not entitled to the names or other personal data of third parties, though this can be subject to certain other assessment in line with Article 15(1)(c) and Article 15(4) of the GDPR.

Access Request

Case Study 6:

Access Request Complaint where a fee was requested

The DPC received a complaint from an individual in relation to a subject access request made to a medical centre for a copy of their personal data. According to the individual, the medical centre had requested a fee to process the access request. Before contacting the DPC, the individual had already advised the medical centre that access to a copy of personal data is free under the GDPR and queried if the letter seeking a fee may have issued in error.

Following receipt of this complaint, the DPC corresponded with the medical centre to ascertain why it had sought a fee to process the subject access request and to seek confirmation that the subject access request had since been complied with.

The medical centre promptly reverted to the DPC accepting that the request for a fee should not have been made. It further outlined additional data protection training for staff regarding its obligations to patients making subject access requests would be provided. The medical centre also confirmed that a copy of the personal data was furnished to the individual with its apologies. The individual confirmed to the DPC that it had received a copy of their personal data.

Key Takeaway:

- Under Article 15(3) of the GDPR there is an obligation for a data controller, such as a medical centre, to provide a copy of the personal data free of charge. For any further copies of the personal data requested by individuals, the data controller may charge a reasonable fee based on administrative costs. However, this particular subject access request was not a repeat request and therefore there was no legal basis for a fee to be sought.

Access Request

Case Study 7:

Failure to respond to an Access Request

The DPC received a complaint from an individual who had made a subject access request to a state hospital for a copy of all information held concerning them. The individual did not receive a response to this request.

The DPC contacted the Data Protection Officer (DPO) for the Hospital Group and informed them of the complaint.

The DPC reminded the hospital of their GDPR obligations , drawing their attention to Article 12(3), which states that controllers have an obligation to provide a response to an individual's subject access request within the statutory timeframe. As part of the engagement, the DPC stipulated a timeline for the hospital to respond to the individual and provide them with a copy of the personal data. The data controller complied with the DPC's direction.

Key Takeaways:

- Organisations are required to implement appropriate organisational measures in place to ensure that they are in a position to respond to any rights requests within the stipulated timeframes under the GDPR.
- Organisations should note that the DPC maintains a record of complaints received which forms part of any consideration of potential future action, including proposals for the carrying out of an inquiry and the further exercising of formal powers such as reprimands.

Access Request

Case Study 8:

Enforcement Notice issued due to an incomplete response to an access request

The DPC received a complaint in which the complainant's representative indicated that they wished to make a formal complaint regarding the delay by Tusla to release records containing their client's personal data on foot of a subject access request. The representative further stated that a full response to the complainant's access request had not been provided and they had been receiving the records containing personal data in a piecemeal fashion for the previous two years. It was unclear to the complainant's representative the amount of personal data outstanding in relation to their client's access request.

The DPC commenced an examination of the complaint by contacting Tusla requesting that it provide the individual with a copy of all personal data held or controlled by it in relation to the individual or notify the individual of the refusal of the subject access request identifying any statutory restriction relied on by it to withhold their data.

Tusla responded indicating that it would be in a position to release personal data to the data subject within a specified timeframe. However, this deadline passed without the complete records containing personal data being released. Subsequent to further DPC engagement, Tusla outlined that, due to the volume of personal data involved, the personal data relating to the individual would issue in batches. This release would be subject to restrictions being applied to third party non personal data, personal data subject to legal professional privilege and where the release of personal data would be in contempt of court proceedings.

The complainant's representative later confirmed they had received a portion of their client's personal data but advised that it was heavily redacted. It clarified the records containing the personal data of the individual that remained outstanding and which it was seeking urgently. An extensive exchange of correspondence between Tusla and the DPC followed over an extended period of time during which several deadlines were not met by Tusla in relation to the issuing of records containing personal data and /or responding to correspondence from the DPC and the data subject's representative.

The DPC considered that an amicable resolution to this complaint was not achievable and considered it appropriate to conclude that process and issue an Enforcement Notice pursuant to Section 109(5)(d)(i) of the Data Protection Act 2018 to require the data controller to furnish the remaining records of personal data to the data subject within a specified timeframe. This notice informed Tusla of the following:

'A person (being a data controller or data processor) who, without reasonable excuse, fails or refuses to comply with a requirement specified in an enforcement notice shall be guilty of an offence under Section 133*19) of the Data Protection Act 2018 and shall be liable (i) on summary conviction, to a class A fine or imprisonment for a term not exceeding 12 months or both, or (ii) on conviction on indictment, to a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years or both.'

The issuing of this Enforcement Notice resulted in the remaining records containing personal data issuing to the data subject within the timeframe specified in the Enforcement Notice.

Key Takeaways:

- The examination of this complaint involved extensive communication between the DPC, Tusla and the data subject's representative. Had Tusla responded to the subject access request in an appropriate manner and within agreed timeframes, the issuing of an Enforcement Notice would not have arisen in this instance. This complaint demonstrates the consequences of a data controller failing to fulfil its obligations under Article 15 of the GDPR. Data controllers should consider these consequences upon receipt of a subject access request under Article 15 of the GDPR and work to ensure that the fundamental right of access is respected for all data subjects.
- Organisations should again note that the DPC maintains a record of complaints received, and that this forms part of any consideration of potential future action, including proposals for the carrying out of an inquiry and the further exercising of formal powers.

Erasure Request

Case Study 9:

An erasure request connected to a property sale

A prospective buyer initiated the facilitated purchase of a property through a real estate intermediary. Shortly after this, the vendor of the property withdrew from the sale. As part of the purchasing process, the prospective buyer had provided a copy of their ID, proof of address and bank details to the real estate intermediary. Following the breakdown in the process, the prospective buyer sought the erasure of their personal data pursuant to Article 17 of the GDPR.

The prospective buyer initially submitted this erasure request to the email address listed on the real estate's privacy policy, but this 'bounced back' as the email was not active. The prospective buyer then sent the request to the primary email address of the real estate intermediary.

As no response was received from the real estate intermediary, the individual made a complaint to the DPC. Following the intervention of the DPC, the real estate intermediary engaged with the individual concerning their erasure request. However, during the complaint handling process, the DPC established that the organisation concerned refused to comply with the erasure request. According to the organisation, it was relying on an obligation under the Property Services (Regulation) Act 2011, which created a legal requirement to retain the data for six years. The matter was referred to the Property Services Regulatory Authority for clarity, who advised that bank details were not covered by the wording of the Act and could be deleted on foot of an erasure request.

Following this confirmation, the DPC engaged with the real estate intermediary to ensure that the bank details were erased as part of the erasure request. The DPC informed the prospective buyer that certain other items of personal data, such as their name, address and contact details would not be erased as the real estate intermediary had a lawful basis to restrict the right of erasure in line with the Property Services (Regulation) Act 2011. The DPC also ensured that the real estate intermediary updated its privacy policy to accurately reflect the appropriate point of contact.

Key Takeaways:

- Organisations must ensure that they have an appropriate, monitored point of contact for facilitating the exercising of data protection rights.
- Organisations should also ensure that any restrictions being placed by them on the exercising of rights are valid and in line with any legislation pertinent to the sector, they are operating in. This should be explained to the individual.

Erasure Request

Case Study 10:

Complaint related to non-compliance with an erasure request to a prospective employer

This complaint concerned the alleged non-response to an erasure request made by an individual to a prospective employer pursuant to Article 17 of the GDPR.

Following receipt of the complaint, the DPC engaged with the individual and the prospective employer (controller) in order to establish the subject matter of the complaint and to commence with the amicable resolution process. Further to this engagement, the DPC established that the individual had since received a response from the controller. However, the individual informed the DPC that while the controller had erased their personal data, their job application 'account' was still active on the controller's website.

Having established this was the case, the DPC contacted the controller, bringing their attention to the fact that information in relation to the account had not been erased. In their response, the controller acknowledged that the information had not been fully deleted, and advised that this was due to a technical error but that they would comply with the erasure request immediately.

Subsequently, the DPC was updated by the organisation concerned that they had since fully complied with the erasure request by deleting the account. The controller also advised that they had contacted the individual to confirm the action they had taken and apologised for the delay in removing the individual's login credentials from their systems.

Key Takeaways:

- In this case, the DPC was able to quickly and effectively make the prospective employer aware that they had not fully completed the individual's erasure request. This ability to quickly contact and engage with both with parties resulted in an effective and speedy outcome. Most importantly, the individual was able to exercise their right to obtain from the controller the erasure of personal data concerning them, as afforded to them under the GDPR.
- The DPC encourages individuals to contact the data protection officer or other designated data protection contact points within an organisation, as this can assist with the proper and efficient handling of any data protection requests.

Erasure Request

Case Study 11:

Non-compliance with an erasure request associated with an online gambling account

An individual opened an online account with a bookmaker and deposited a sum of money to their account. Having attempted to download the application ('app') associated with the service, the individual quickly realised that the app was not compatible with their mobile phone. The following day the individual submitted an erasure request under Article 17 of GDPR to the bookmaker. The bookmaker refused to comply with the erasure request, stating that it had legal obligations to retain the personal data as a deposit and withdrawal of funds had taken place on the account, thus making them a 'customer'. The individual was dissatisfied with this response as they did not agree that they were a 'customer' of the bookmaker, as they did not place any bets through the account, either online or through the app.

Following engagement with the DPC, the bookmaker advised that it could not erase the individual's personal data as it was subject to Anti-Money Laundering legislation, under the Criminal Justice (Money Laundering and Terrorist Financing Acts 2010, which became applicable when the deposit and withdrawal of funds were made on the individual's account.

The bookmaker outlined to the DPC that although it was legally obliged to retain the individual's personal data it only retains the minimum amount that is necessary to fulfil this legal obligation in line with the principle of data minimisation as set out in Article 5(1)(c) of the GDPR.

Following its examination of the complaint, the DPC found that while the organisation had demonstrated a valid lawful basis for the ongoing retention of the personal data, the DPC issued recommendations to the organisation on its obligations to ensure that all processing is lawful and fair and that it is transparent about its processing activities.

Key Takeaways:

- Under the GDPR, not only must a data controller have a lawful basis for initially obtaining an individual's personal data, but it must also have an ongoing legal basis for the retention of the personal data in accordance with Article 6. Controllers need to ensure they are transparent when processing personal data.
- A proactive approach on the part of data controllers when they receive a data protection request can often resolve matters and avoid the need to engage in a lengthy complaint handling process.

Erasure Request

Case Study 12:

Non-compliance with an erasure request related to medical data

An individual contacted the DPC following the refusal of their erasure request by a health care provider. According to the individual, they had requested the erasure of all historic health records relating to them held by the health care provider, as the individual was of the opinion that the records were incorrect as they related to an alleged misdiagnosis.

As part of its examination of the complaint, the DPC requested that the health care provider set out its lawful basis for processing the individual's health records, specifically in relation to Articles 6 and 9 of the GDPR. The health care provider advised that it was relying on Article 6(1)(e) of the GDPR for processing the individual's personal data which states that processing shall be lawful if 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.

In relation to Article 9 of the GDPR, the health care provider stated that it continues to process the health records under Articles 9(2)(h) and (i) of the GDPR. Article 9(2)(h) of the GDPR states, 'processing is necessary for the purposes of preventive or occupational medicine, medical diagnosis…'. While Article 9(2)(i) of the GDPR states, 'processing is necessary for reasons of public interest in the area of public health…'.

As part of their engagement with the health care provider, the individual provided them with a contradictory diagnosis from another health care provider, which the individual stated was evidence that proved the original diagnosis was incorrect. Having reviewed the documentation provided, the health care provider noted that a medical diagnosis is a medical opinion that is given at a point in time. Therefore, any medical opinion, given at a different point in time, cannot be accepted as evidence that a historic medical opinion was incorrect. The medical provider further advised that while a medical condition may change over time, it does not eradicate the fact that an individual was, at one point, treated for a particular illness or provided with a certain diagnosis.

The DPC noted that for the purposes of the GDPR, personal data is inaccurate if it is incorrect as to a matter of fact. However, based on the information available to the DPC, the personal data held on file by the health care provider, namely the original diagnosis, was not inaccurate as it was the original diagnosis at that point in time. On this basis, the DPC found that the health care provider had a lawful basis for the continued processing of the individual's health records in accordance with Article 17(1)(a) of the GDPR.

In this regard, the processing of the personal data in the form of retaining the original diagnosis is still necessary in relation to the purposes for which the personal data was originally collected or otherwise processed. Further, the DPC found that the health care provider's refusal to comply with the individual's erasure request is consistent with Article 17(3)(c) of the GDPR in providing comprehensive medical assessment and treatment of the individual.

Following the engagement of the DPC, the health care provider added a supplementary statement on the individual's medical record to include the documentation provided by the individual, which would inform any future readers of the individual's medical file of the individual's opinion, and the contradictory diagnosis in relation to the medical diagnosis.

Note: Article 17(1)(a) of the GDPR states that a data controller shall erase personal data that is no longer necessary for its original purposes. However, Article 17(3)(c) of the GDPR excludes the application of Article 17(1) in circumstances where the processing is necessary, 'for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3).'.

Key Takeaways:

- The DPC encourages individuals to raise data protection concerns directly with the controller in the first instance so that it can address them. Data controllers should have meaningful and efficient measures in place to deal with and address data protection complaints when raised with them directly by an individual.
- This case study highlights the fact that historic medical data cannot be erased as it relates to an opinion given at a point in time and any future opinions cannot overwrite a historic opinion provided by a professional in their professional capacity. That said, there was scope to add a supplementary statement on the individual's medical record to reflect the updated medical opinion, which the health care provider could have done without the need for the individual to resort to DPC intervention. The public interest may require health care providers to ensure supplementary up to date medical records are on an individual's medical record.

Case Study 13:

Disclosure of health and financial data to a third party

An individual submitted a Freedom of Information ('FOI') request to their former employer, a State Agency. Once in receipt of the response to the FOI request, the individual became aware that the State Agency had disclosed their financial data and special category personal data, namely health data, to a connected third party. The individual subsequently submitted a complaint to the DPC in relation to this disclosure.

The DPC was tasked with examining whether the State Agency had lawfully processed, in a non-excessive manner, the individual's personal data when a staff member of the State Agency disclosed the individual's health and financial data to a connected third party.

In the circumstance of this case, the individual had communicated with a member of the Human Resources ('HR') department in their official capacity, highlighting issues connected with the individual's health, financial status and personal life. Due to issues connected to the individual's health, they were regularly in contact with the HR staff member in their official capacity.

Following a meeting between the individual and the HR staff member, the HR staff member emailed a summary of what was discussed with a connected third party i.e. a member of the Civil Service Employee Assistance Service ('CSEAS'). The CSEAS provides an internal Employee Assistance Programme to civil service staff, which employees can refer to by contacting the service. It is a shared service utilised by all State Agencies for the benefit of all employees, promoting employee wellness and organisational effectiveness.

During the examination of this complaint, the State Agency stated that the processing of the personal data, the sharing of the individual's personal data by the HR staff member to the CSEAS member, was lawful as the individual shared the personal data freely with the HR staff member, accordingly they had consented to the processing; the overlapping services and consultation between the HR staff member and the CSEAS in relation to an employee would be normal; both the HR staff member and the CSEAS member operate under strict confidentially in the performance of their duties; and what the individual shared with the HR staff member was so concerning, that the HR staff member had to urgently disclose it to the CSEAS member in order to seek appropriate guidance, and support to assist the individual. Accordingly, the State Agency's position was that there were no prohibitions on the disclosure.

Notwithstanding, the HR staff member had a genuine concern for the health and welfare of the individual, the DPC found that the circumstances did not fit the urgency associated with protecting life rather the processing occurred as the HR staff member sought direction and guidance from the CSEAS member to urgently deal with the issues raised by the individual.

The DPC also found that the State Agency could not rely on having obtained the consent of the individual to process their personal data in this manner, as although the individual shared the personal data freely with the HR staff member, they did not consent to the HR staff member disclosing this personal data to the CSEAS member.

The State Agency did not provide any other lawful bases for the processing. The DPC found that the State Agency did not have a lawful basis for the processing and accordingly, the processing was unlawful.

In consideration of the principles relating to processing of personal data the DPC found that the State Agency obtained the personal data for a specified, explicit and legitimate purpose, namely to provide the individual with HR assistance with the issues they had raised with HR. Similarly, considering the connected relationship between the HR staff member in their official capacity and the CSEAS member, the sharing of the individual's personal data was not further processed in a manner that was incompatible with the purpose for which it was obtained, as it was disclosed in order to provide the individual with assistance regarding the issues raised, which included employee wellness.

However, the DPC found that the State Agency disclosed an excessive amount of personal data than what was required in order to seek, and provide, assistance to the individual. Accordingly, the State Agency did not adhere to the principle of data minimisation, and this was identified and accepted by the State Agency.

Key Takeaways:

- In an employment context, the need to share employees' personal data with third parties frequently arises. This case illustrates that to ensure the sharing occurs in compliance with data protection requirements, ongoing training is necessary for all staff in relation to their obligations under data protection law. Furthermore, controllers must conduct due diligence to satisfy themselves that all data processing activities comply with data protection laws.
- The DPC expects accountability on the part of controllers and when handling a complaint it will scrutinise explanations and reasons given by a controller in order to ensure that the position put forward is verifiable and defensible.

Case Study 14:

Disclosure of personal data to a debt collection agency

An individual contacted the DPC after an energy service provider further processed their personal data by sharing it with a third party (data processor), a debt collection agency. According to the individual, they had completed the contract with the service provider and had received their final invoice for the services provided. The individual disputed some of the charges on the invoice; however, they did not receive a response from the service provider and were subsequently contacted by a debt collection agency.

As part of the complaint handling process, the DPC contacted the service provider and questioned the lawful basis it was relying on under Article 6 of the GDPR for sharing the individual's personal data the debt collection agency. The service provider stated that its lawful basis for processing the individual's personal data was Article 6(1)(b) of the GDPR which states that processing shall be lawful if the 'processing is necessary for the performance of a contract to which the data subject is party…'. The service provider further explained that the individual's invoice dispute related to an 'early exit fee' which was applied to the invoice as the individual had cancelled the contract with the service provider prior to the agreed contract length. The service provider also advised that its terms and conditions stated that should a customer break the contract with the service provider, they would be charged an exit fee. The service provider further advised that the individual agreed to its terms and conditions when they registered with the service provider.

However, the service provider also informed the DPC that it had failed to record the individual's dispute of the invoice. This failure to record the dispute resulted in the individual's personal data being shared with a third party incorrectly. The service provider acknowledged that it had not followed its own internal procedures for dealing with disputed debts and that this was a result of human error.

Although the service provider would normally have a lawful basis for the processing of an individual's personal data by sharing in the circumstances of this case, by not following the correct internal procedures, the service provider incorrectly processed the individual's personal data by providing their details to the third party, the data processor.

Accordingly, the service provider failed to demonstrate its compliance with a key principle of the GDPR, processing personal data in a manner that ensures appropriate security of the personal data, including protection

against unauthorised or unlawful processing, using appropriate technical or organisational measures, in accordance with Article 5(1)(f) of the GDPR ('integrity and confidentiality').

The service provider should have had regard to Article 25 of the GDPR ('Data protection by design and default'), in ensuring that the appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed, are in fact followed by all staff members.

The DPC recommended to the service provider that where there is a live dispute on the account it should ensure that its staff are aware of the internal procedure to document the dispute so that accounts are not referred to a debt collection agency until the dispute is resolved or closed.

Key Takeaways:

- Data processors may lawfully process personal data, providing there is a legal basis for the processing. Article 28 of the GDPR details the circumstances in which a data controller can engage the services of a data processor. However, in this case, the controller had disregarded previous concerns raised by the individual and failed to follow its own internal procedures.
- Data controllers must also ensure that its staff are fully trained in internal procedures, and data protection policies, to ensure appropriate security of the personal data, including protection against unauthorised or unlawful processing.

PROSECUTION

Case Study 15:

Prosecution of Chill Insurance Limited

In July 2022, the DPC received a complaint from an individual regarding unsolicited marketing SMS messages received from Chill Insurance Limited. In response to the DPC's investigation of the complaint, Chill Insurance Limited explained that it did not have consent to send these marketing communications. Following the receipt of a similar complaint in 2021 to the DPC, a full review of its marketing campaigns was carried out by the company and changes were made to said campaigns. However, all changes that were identified following that review were not implemented and this led to the further complaint in 2022. As the DPC had previously issued a warning to the company, the DPC decided to prosecute arising from this complaint case.

At Dublin Metropolitan District Court on 11 September 2023, Chill Insurance Limited pleaded guilty to one charge under Regulation 13(1) of the ePrivacy Regulations for the sending of a marketing SMS message without consent and one charge under Regulation 13(12)(c) of the ePrivacy Regulations for not including a valid opt out in that message. The District Court applied the Probation of Offenders Act 1907 in this case, on the basis of a charitable donation of €500 to Little Flower Penny Dinners. Chill Insurance Limited agreed to discharge the DPC's legal costs.

PROSECUTION

Case Study 16:

Prosecution of Hidden Hearing Limited

Four individuals lodged complaints about unsolicited marketing SMS messages, emails and telephone calls that they had received from Hidden Hearing Limited. One of the complainants replied to the sender requesting that their telephone number be removed from the company's marketing list. This request was actioned but due to a system error, the central record management (CRM) system in the company failed to synchronise with its Diary Management system, therefore the complainant's telephone number was not removed from the calling list and he was subjected to a further unsolicited marketing telephone call.

The DPC's investigation of these four complaints established that Hidden Hearing Limited had no consent to send unsolicited marketing communications to the complainants concerned. As the DPC had issued a warning to the company in a previous complaint, the DPC decided to prosecute arising from these complaint cases.

At Dublin Metropolitan District Court on 11 September 2023, Hidden Hearing Limited pleaded guilty to two charges under Regulation 13(1) of the ePrivacy Regulations for the sending of a marketing email and marketing SMS message without consent and two charges under Regulation 13(6)(a) of the ePrivacy Regulations for making marketing telephone calls without consent. The District Court applied the Probation of Offenders Act 1907 in this case, on the basis of a charitable donation of €500 to Little Flower Penny Dinners. Hidden Hearing Limited agreed to discharge the DPC's legal costs.

PROSECUTION

Case Study 17:

PROSECUTION OF THE MULTIPLE SCLEROSIS SOCIETY OF IRELAND

In April 2023, the DPC received one complaint from an individual regarding unsolicited marketing email messages received from The Multiple Sclerosis Society of Ireland. In response to the DPC's investigation of the complaint, The Multiple Sclerosis Society of Ireland explained that the individual had opted out of marketing in July 2018. However, in April 2023 as part of an ICT migration project the complainant's email address was included in error on the list of individuals who had consented to marketing. As a result, the complainant was sent unsolicited marketing email messages. As the DPC had issued a warning to the company in a previous complaint, the DPC decided to prosecute arising from this complaint case.

At Dublin Metropolitan District Court on 11 September 2023, The Multiple Sclerosis Society of Ireland pleaded guilty to one charge under Regulation 13(1) of the ePrivacy Regulations for the sending of a marketing email without consent. The District Court applied the Probation of Offenders Act 1907 in this case, on the basis of a charitable donation of €500 to Little Flower Penny Dinners. The Multiple Sclerosis Society of Ireland agreed to discharge the DPC's legal costs.

PROSECUTION

Case Study 18:

Prosecution of Vodafone Ireland Limited

In April 2023, the DPC received one complaint from an individual regarding an unsolicited marketing email message received from Vodafone Ireland Limited. In response to the DPC's investigation of the complaint, Vodafone Ireland Limited explained that the individual had opted out of marketing in December 2021. However, it was found that three recent email marketing campaigns were incorrectly designed as a result of human error which resulted in marketing messages being sent to 20,790 customers who had opted out of marketing. Once this error was identified the campaigns were stopped and not reused. This individual was one of the customers impacted.

The DPC had previously prosecuted Vodafone Ireland Limited in 2022, 2021, 2019, 2018, 2013 and 2011 for breaching Regulation 13 of the ePrivacy Regulations in relation to previous complaints. Accordingly, the DPC decided to proceed to another prosecution arising from this complaint case.

At Dublin Metropolitan District Court on 11 September 2023, Vodafone Ireland Limited pleaded guilty to one charge under Regulation 13(1) of the ePrivacy Regulations for the sending of a marketing email without consent. The District Court convicted Vodafone Ireland Limited on the one charge and imposed a fine of €500. Vodafone Ireland Limited agreed to discharge the DPC's legal costs.

Key Takeaway:

- These prosecution cases highlight the importance of having systems in place that accurately record a data subject's consent wishes, particularly when an organisation is migrating data to new business systems or beginning new marketing campaigns, and that organisations should regularly review any customer consent lists that they have.

CCTV

Case Study 19:

Fair processing complaint relating to CCTV in the workplace

An individual raised a concern with their employer in the beauty industry regarding what they believed was excessive use of CCTV cameras in the workplace. The individual stated that they were not informed that the cameras were being installed and had concerns that the devices were capable of recording both audio and video. In response to their concerns, the organisation advised the individual that the cameras were installed for the safety of staff and that no audio was recorded.

The individual then submitted a complaint to the DPC as they were dissatisfied with the response received from the organisation. As part of its examination, the DPC queried the organisation on the alleged audio recordings via the CCTV cameras. The organisation provided the DPC with evidence in the form of a letter from the CCTV system supplier, which confirmed that the cameras did not have audio recording capability.

Regarding the background as to why the organisation made the decision to install CCTV cameras, the organisation informed the DPC that it initially installed the cameras following a series of security issues including incidents of theft. However, it also stated that the cameras were installed for the safety of staff when working alone. Whilst the individual claimed that they were unaware the cameras had been installed, the organisation stated that the cameras had been in place for three years prior to the individual making a complaint to the DPC and that the individual had provided training to the staff in relation to same.

The organisation cited a number of lawful basis for the processing of data in this manner, including Article 6(1)(d) of the GDPR as its lawful basis stating that the cameras are necessary to protect the vital interests of its staff. Article 6(1)(d) of the GDPR states that the processing of personal data shall be lawful if 'processing is necessary in order to protect the vital interests of the data subject or of another natural person'. It further cited Article 6(1)(f) of the GDPR which states that processing shall be lawful if 'processing is necessary for the purposes of the legitimate interests pursued by the controller…' as the organisation has a legitimate interest in the security of the workplace, safety of staff and prevention of crime.

In response the DPC informed the organisation that Article 6(1)(d) of the GDPR may only be relied upon by an organisation where the processing of personal data is necessary to protect a person's life or mitigate against a serious threat to a person. As such, the DPC advised the organisation that it could not rely on Article 6(1)(d) of the GDPR as its lawful basis for the use of CCTV cameras in the workplace. Regarding its reliance on Article 6(1)(f) of the GDPR, the organisation confirmed that it had conducted a legitimate interest balancing test prior to the installation of the CCTV cameras. The organisation further stated that the processing was limited to what is necessary and cited its requirement for safety purposes. It stated that footage was retained for a period of 20 days and had put in place access controls to the footage.

Following its examination of the complaint, the DPC found that the organisation had demonstrated a valid lawful basis for the processing of personal data by means of CCTV cameras under Article 6(1)(f) of the GDPR.

Key Takeaways:

- There must be a lawful reason for the use of CCTV, such as crime prevention, health and safety of workers. The use of CCTV must be necessary and proportionate.
- Organisations should take into account what benefits can be gained; whether better solutions exist; and what effect it may have on individuals before installing such systems.
- More information on this subject matter can be found at:

  https://www.dataprotection.ie/en/dpc-guidance/guidance-use-cctv-data-controllers

CCTV

Case Study 20:

CCTV in Restrooms

Each year the DPC receives numerous queries and complaints from various individuals complaining specifically about the use of CCTVs in restroom areas by various organisations such as public houses, nightclubs, restaurants and transport depots. More particularly, the complaints allege that the cameras are pointing over specific areas in restrooms where there is an increased expectation of privacy, such as over cubicles or urinals.

While, the DPC has engaged with organisations on a one-to-one basis, the issue of the lawfulness of the processing of personal data by way of CCTVs in restrooms needs to be considered more generally. Consequently, the DPC has examined these issues further and updated its Guidance on CCTVs for Data Controllers by including a specific section on 'The use of CCTV in areas of an increased expectation of privacy.

Key Takeaways:

- Organisations should avoid using CCTV where a reasonably high expectation of privacy exists (for example, over cubicles). The threshold for the use of CCTV in restrooms more generally, remains very high, and requires data controllers to identify and examine all the legitimate issues arising and to assess and implement appropriate measures which adequately protect the interests of individuals using those facilities which must be evaluated prior to the deployment of any system.
- The DPC strongly recommends that all data controllers familiarise themselves with this updated guidance.

Breach

Case Study 21:

Breach Complaint related to employment information

The DPC received a complaint from an individual against their employer relating to a data breach. The breach occurred when a HR folder, which contained the individual's personal data, was placed on an open drive that was accessible to third party individuals.

Having reviewed the information provided, the DPC noted that the employer had notified the breach to the DPC. As part of its notification, it advised that, due to human error, a folder, which contained the personal data of a number of employees, was accidently transferred to a common internal shared drive. It further advised that this folder was not accessible to anyone outside of the organisation. Once the employer became aware of this breach, it took immediate action to secure the files affected. The Human Resources folders were secured by removing them from the shared drive and relocating them to the appropriate local HR drive.

The employer investigated this incident and confirmed that no further processing of personal data occurred in this instance. The employer informed the affected individuals of this breach and provided various updates regarding same via email. The employer subsequently provided the individual with a detailed list of the categories of personal data which were involved in this data breach.

The DPC conducted an inspection at the employer's premises. Having assessed the breach notification, the complaint received and the information established during the inspection, the DPC reminded the employer of its obligations under Article 5(1)(f) and Article 24 of the GDPR. The employer has since confirmed to the DPC the technical measures put in place to prevent a recurrence of such an incident in the future.

Key Takeaway:

- Organisations should ensure that they have appropriate controls and monitoring in place when using facilities such as shared folders and drives. If such are being used, they should be regularly audited to ensure that there is no personal data accessible.

Breach

Case Study 22:

Data Processor in the Charity Sector Breach

The DPC became aware of a breach which had occurred at a data processor when eighteen (18) organisations (data controllers) operating in the charities sector used a data processor based outside of the DPC's jurisdiction. The organisations provided services largely aimed at supporting vulnerable individuals and are not for profit with many of their personnel working on a volunteer basis.

The breach occurred when a bad actor gained access to the data processor's network. The data processor was unable to confirm how long the bad actor may have infiltrated its systems before the discovery of the breach. This resulted in the exfiltration of some data, the deletion of a database that held the data and a ransom note demanding payment. The bad actor made direct contact with the data processor and provided evidence of the exfiltrated data.

The data processor did not pay the ransom and stated that it had restored its systems from backup. However, the exfiltrated data remained a risk.

Only eight of the eighteen organisations were able to confirm having an existing Breach Incident Response Plan, which is a plan to respond to data breaches. Many of the data controllers demonstrated a lack of IT experience in any form and did not appear to recognise the extent of their Article 24 GDPR obligations (appropriate technical and organisational methods).

Most of the organisations had varying degrees of understanding of the personal and special category data which they held and a number were not able to confirm the categories of data held.

Most of the organisations did not have in place a controller – processor contract pursuant to Article 28(3) GDPR. Instead, these data controllers relied on a Software as a Service Subscription Agreement, which appear to favour the data processor in terms of obligations to respond or provide information related to a security incident.

A number of the organisations did not conduct a Data Protection Impact Assessment (DPIA) despite the nature of the organisation and the clients for whom they cater. Some organisations stated the inability to perform a DPIA due to the data processor's refusal to supply information about its systems and the breach.

The DPC engaged with the Data Protection Authority in the country where the processor was located to gather and share information. The DPC further engaged with the organisations, both from a regulatory and supervisory capacity. The DPC provided a number of recommendations, which emphasised the organisations obligations in the areas of awareness on the categories of personal data they processed pursuant to Article 4(1) and Article 9 GDPR. The DPC also emphasised the importance of vetting any third party they were choosing to engage with prior to permitting the processing of personal data (Article 28(1) GDPR), as well as their obligation to ensuring that a processing agreement is in place setting out clearly the responsibilities of both parties (Article 28(2) GDPR) and is tested regularly.

Key Takeaways:

- The key takeaways are that an organisation may outsource its processing of personal data activities to a third party but it cannot outsource its responsibility and obligations under the GDPR. Particular care is needed when sharing with third parties the data of individuals especially their special category data. Data protection is a fundamental human right and organisations in the charities sector must recall that people trust them with keeping their data safe.
- Appropriate technical and organisational methods can be put in place by organisations who can seek the advice of peer organisations or the DPC.

Breach

Case Study 23:

SECOND LEVEL SCHOOL A VICTIM OF A WHALE PHISHING ATTACK

The DPC received a breach notification from a school in relation to a bad actor who accessed and infiltrated a school's ICT systems, including the email system, for an unknown length of time. The bad actor gathered information before sending a phishing email and tricked the administrator for financial accounts into directing payments into a fraudulent account.

The bad actor sent an email to the accounts administrator, pretending that it had come from the email of the school principal. This practise is referred to as spoofing and has the appearance of being from a trusted individual and being a valid request. This email contained fraudulent duplicates of invoices relating to legitimate work performed in the school. However the bank account details were manipulated by the bad actor to redirect the payment to an unknown recipient and the school, who were unaware of this, carried out the transaction.

The breach was discovered when the legitimate supplier reported that they had not been paid.

The DPC engaged with the school and recommended that the school take a number of actions to recover from the breach and mitigate against a recurrence including the implementation of Multifactor Authentication, ongoing monitoring and reminders on its email usage policy.

Key Takeaway:

- A key takeaway is that any organisation which employs a third party email system must ensure that its use within the organisation ensures an appropriate level of security and this can be achieved through configuring appropriate security option and providing clear guidance to staff on the correct usage of the software being used.

Breach

Case Study 24:

CCTV POLICIES AND PROCEDURES

A customer of a restaurant lost their belongings while in the premises. They then requested that a staff member provide them with access to the restaurant CCTV footage to assist in finding out what happened to their belongings.

The staff member, using their phone, took a photo of the footage and then allowed the customer to view the image however:

1. They did not prevent the customer from using their mobile phone to take a copy of the image.

2. Did not log the customers contact details should the need arise to make contact relating to the image.

Having become aware of the incident, the restaurant manager submitted the breach as low risk, however following a DPC risk analysis the risk level was increased to high due to the lack of internal controls and policies in place.

When the owner/occupier of a premises installs a CCTV system, having justified it as a necessary and proportionate measure, they as a data controller must give due consideration to the safe storage of personal data and the implementation of appropriate security measures. Data controllers are obliged to implement technical and organisational measures to ensure that personal data are kept secure from any unauthorised or unlawful processing and accidental loss, destruction or damage. In this case, the staff member should not have allowed the individual take a photo of the image.

The restaurant was not able to mitigate the risks associated with this breach, as it was unable to contact the customer to request/ confirm the deletion of the image from all locations.

The DPC engaged and advised the restaurant that it should review CCTV Policies and Procedures. In particular, it drew its attention to risk factors around:

1. Authorisation of access to CCTV footage
2. Restrictions and logging of any duplication of CCTV footage.
3. Awareness training for staff of the risks involved in the sharing of the CCTV footage. This should be clearly called out in its CCTV usage policy.

Key Takeaway:

- A key takeaway is that the use of CCTV within any organisation should be underpinned by appropriate policies and guidance and enforced through training and awareness, to ensure that there is an appropriate level of security to mitigate any risks that may arise.

Breach

Case Study 25:

Transfer of hard copy paper documents

The breach concerned an organisation who has a function in conducting independent reviews. The organisation was returning documents following the completion of their review process. The organisation normally encourages the use of a file transfer system for the transfer of subject records but also facilitates the sending of hard copies. In this instance, the sending organisation requested that the copies of records it had sent in hard copy be returned to it. The organisation returned these documents by post and the envelope was reinforced and secure when it left the organisation. However, it was stated that it was not sent by registered post, which was the normal policy for the organisation when requesting hard copies from organisations to support the appeal / assessment process. When the envelope arrived back to the sending organisation the envelope had all of the seams split and badly torn and three pages were missing from the package.

The documents contained details related to vulnerable individuals, the nature and category of data related to Article 4(1) GDPR and while it did not contain any medical data, certain medical information could be inferred from the fact that the service user had engaged with the sending organisation.

The organisation had engaged with the postal service used when returning the details to the requesting organisation and as part of its investigation into the missing three pages, it was established that the envelope was received undamaged by the postal service, however it was not sent as registered post and so postal tracking was not available.

The organisation has committed to enforcing the use of registered post and updating its policy to direct staff that when returning hard copies to the data controller, that steps are taken in line with Article 5(1)f GDPR and Article 32 GPDR to implement appropriate technical and organisational measures such as ensuring the correspondence is registered with the postal service and that appropriate reinforced envelopes are used to ensure a level of security and protection appropriate to any risk.

It was noted that the organisation had engaged with the postal service as part of its investigation into the missing three pages and had established that the envelope was received undamaged by the postal service. However as it was not sent as registered post the tracking of the envelope was not available.

It also identified that while the policy in use by the organisation did call out the use of registered post as the preferred method of postage it was only mentioned in relation to the receipt of hard copies from the sending organisations. The organisation recognised this as an oversight within its own policies.

The DPC engaged and advised the organisation to update its policy on the returning of hard copies to organisations and that it should include this in staff training and awareness campaigns.

Key Takeaway:

- A key takeaway is that the transference of any hardcopies containing personal data within or external to an organisation should be underpinned by appropriate policies and guidance and enforced through training and awareness, to ensure that there is an appropriate level of security to mitigate any risks that may arise.

Breach

Case Study 26:

Transfer of hard copy paper documents while moving premises

A medical General Practitioner ('GP') who operated his practice from his own home was moving work premises. The GP stated they had 4000 patients attending the practice over time and operated both digital storage and paper files. The GP engaged a local delivery van to transport the paper medical files connected with the practise. The medical files were put into boxes and placed in the private delivery van.

The breach was discovered during a system audit which followed the move. A box containing medical files, which had been transported, was missing. The van driver confirmed that he had deposited all the boxes in the reception area of the new premises. The GP reported the loss of the box of files to the local Garda Station. It was established that the box, which contained over 2000 medical files, could not be located and the GP confirmed that there was no backup of these records. The missing files related to medical diaries and timesheets, vaccination records and clinical records pertaining to the assessment and treatment of private patients.

The DPC engaged with the GP and established that the GP did not intend to notify affected individuals. The GP advised that he was liaising with the HSE on the matter and that they had aligned their practises with the HSE policy on record keeping (HSE Standards and Recommended Practices for Healthcare Records Management, QPSD-D-006-3 V3). The GP initially stated that the risk was low as the missing data was not incomplete.

Following further engagement, the DPC drew the GP's attention to the obligations under Article 34 of the GDPR to notify the affected individuals without undue delay. Following this engagement, the GP confirmed that he had sent a notification to every affected patient or minor patient's parent or guardian by either email or by postal letter.

The personal data in question encompassed both Article 4 and 9 GDPR. Some of the personal data included names, address, dates of birth, PPSNs and vaccination details.

The GP engaged with the HSE on the management of medical records. New measures have since been introduced by the GP to digitise the remaining medical records held.

In line with the obligations set out under Article 5(1)(f) GDPR and Article 32 GPDR to implement appropriate technical and organisational measures appropriate to any risk, practical steps such as having an individual in attendance to receive any medical records being transported have also been introduced.

It was noted that the GP had operated from their home for over 20 years and while he used secure filing cabinets, appropriate measures were not taken when transporting the files.

The DPC engaged with the GP and issued recommendations regarding the GP's obligations as a controller under Article 24 GDPR and directed him towards the guidance provided on the DPC Website. The DPC further referred the GP to the data protection guidance published by the Irish College General Practitioners (ICGP).

Key Takeaway:

- A key takeaway is that the when transferring any hardcopies containing personal data such as when moving premises, an organisation (or individual where they are the controller) must take into account all the potential risks and ensure there are appropriate technical and organisational measures in place to prevent or mitigate the risks.

BREACH

Case Study 27:

RISKS POSED BY USERS OF VIDEO CONFERENCING

The DPC received a notification from a statutory body tasked with investigating complaints about the professional conduct of experts. The breach occurred during the course of a public hearing, which was held remotely, when access permissions were incorrectly provided to attendees including journalists.

This error made visible documents revealing personal data, that members of the public were not entitled to view as they did not form part of the hearing. The personal data, which was unintentionally disclosed during the hearing was subsequently published by journalists in numerous media outlets.

The breach was assessed as high risk because the data subject's location which was published could be inferred from the data disclosed.

By way of mitigation, the statutory body confirmed removal of the personal data by the media outlets. In addition, the organisation updated their technical and organisational measures to restrict access to personal data.

KEY TAKEAWAY:

- This case highlights the potential risks posed by users of video conferencing. Controllers should ensure that individuals operating such technologies are familiar in their use and are done in compliance with the standard operating policies and procedures.

Cross Border

Case Study 28:

Cross-Border Complaint Concerning Right to Erasure Request to an Online Financial Company Amicably Resolved

The DPC as Lead Supervisory Authority received a complaint via the One-Stop-Shop (OSS) mechanism created by the GDPR from an individual in Germany regarding an erasure request, pursuant to Article 17 of the GDPR to an online financial company based in Ireland.

Having submitted the erasure request to the company for the deletion of their personal data from the company's database, the individual received a refusal from the company to their request. The company informed the individual concerned that it had a legal obligation that required it to retain the data. In the complaint, the individual stated that the company did not provide further information for the basis of its refusal of their request, or information on how long it would retain their data.

The individual then lodged their complaint via the North Rhine-Westphalia Data Protection Authority, who then transferred the complaint to the DPC as the Lead Supervisory Authority.

The complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018.

As part of the amicable resolution process, it was established that the company was a financial regulated entity obliged by law to keep the personal data related to closed accounts for a period of seven years, and, upon the expiry of this period, it deletes the personal data associated with a closed account. The company confirmed the date the individual's data would be deleted, and confirmed that until such a time as it could comply with the erasure request, the individual's personal data would be safeguarded.

The DPC communicated this information to the individual via the North Rhine-Westphalia Data Protection Authority. The individual responded, confirming the information provided by the DPC had led to the amicable resolution of their complaint.

Key Takeaway:

- This case study demonstrates the benefits to individuals of the DPC's intervention by way of its complaint handling and amicable resolution process, which allows it to get to the root of issues between Data Subjects and Controllers. The process allows the DPC to assist individuals in EU States – by addressing their concerns, and providing clarification on data protection procedures and the individual's rights under the GDPR.

Cross Border

Case Study 29:

Amicable Resolution of a Cross Border Complaint regarding a Right to Erasure Request

The DPC received a complaint via the One-Stop-Shop (OSS) mechanism from an individual regarding the handling of an Article 17 GDPR erasure request made by them.

The individual in this matter had made an erasure request to have their social media account, as well as any subsequent personal data belonging to them, erased by the controller. The individual also noted as part of their complaint that they had lost access to the account in question. Therefore, they could not delete the account on their own accord using the controller's self-deletion tool, due to inaccessibility. The individual first raised their request with the controller directly, but was left dissatisfied with the controller's response to their request. The individual then contacted their national supervisory authority, seeking assistance in acquiring the erasure of the account and related personal data.

The DPC identified the complaint as potentially being capable of amicable resolution under Section 109(2) of the Data Protection Act 2018. The DPC commenced an examination of the complaint by contacting the controller and outlining the details of the complaint.

In its response to the DPC, the controller acknowledged that it appeared that the individual was unable to access their account as asserted by the individual in their complaint. On foot of the DPC's intervention, the social media company contacted the individual directly and its specialist team assisted the individual in regaining access to their account. This enabled the individual to then initiate the process of self-deleting their account and related personal data. The individual subsequently notified the DPC that they considered that their complaint had been amicably resolved.

Key Takeaway:

- This case demonstrates that organisations cannot always rely on automated systems to address customer concerns and that they need to be mindful of the small percentage of users who cannot exercise their rights through the automated mechanisms in place.

Cross Border

Case Study 30:

Cross-Border Complaint: Delisting Request pursuant to Article 17 GDPR

Via the One-Stop-Shop (OSS) mechanism, the DPC received a complaint related to a 'Right to be Forgotten' request made to a large multinational technology company pursuant to Article 17 GDPR. The individual requested the delisting of three URLs that were being returned in a search against the individual's name on the controller's search engine. The URLs in question related to their now-deregistered business. The individual's personal telephone number and residential address were visible through the URLs in question (the individual having operated their previous business at that same address).

The individual submitted their request along with supporting documentation to verify themselves for the purposes of their request. However, the supporting documentation the individual provided was flagged as being illegible, which the individual disputed, and the Data Controller did not appear to have considered the substantive request itself. The individual was not satisfied with the Data Controller's response and subsequently made a complaint to the Bavarian Data Protection Authority (Concerned Supervisory Authority), who transferred the complaint to the DPC for investigation, as the company complained of, has its main establishment in Ireland.

In response to the DPC's investigation, the Data Controller agreed to review the individual's request in full and, having considered the information provided with the request as to the personal details contained in the URLs, determined that the complained-of URLs were eligible for delisting. As a result, the Data Controller delisted the URLs from being returned in a search of the individual's name and informed the individual directly of same. The Data Controller stated that, should the individual have any further URLs or search terms it wished to submit for the purposes of a delisting request, the most efficient and effective means of doing so was through its online form.

The individual subsequently responded to the DPC to confirm their satisfaction with the actions taken by the controller.

Key Takeaway:

- Delisting and "right to be forgotten" requests need to be considered properly and a balancing test carried out to establish whether the public interest in accessing the information outweighs the rights of the individual to have that same information deleted, or vice versa.

Notes

Notes

Index

A

B

C

D

E

F

G

L

N

P

R

T

www.dataprotection.ie

21 Fitwilliam Square South
Dublin 2
D02 RD28
Ireland

01 7650100 or 1800 437 737

An Coimisiún um Chosaint Sonraí
Data Protection Commission