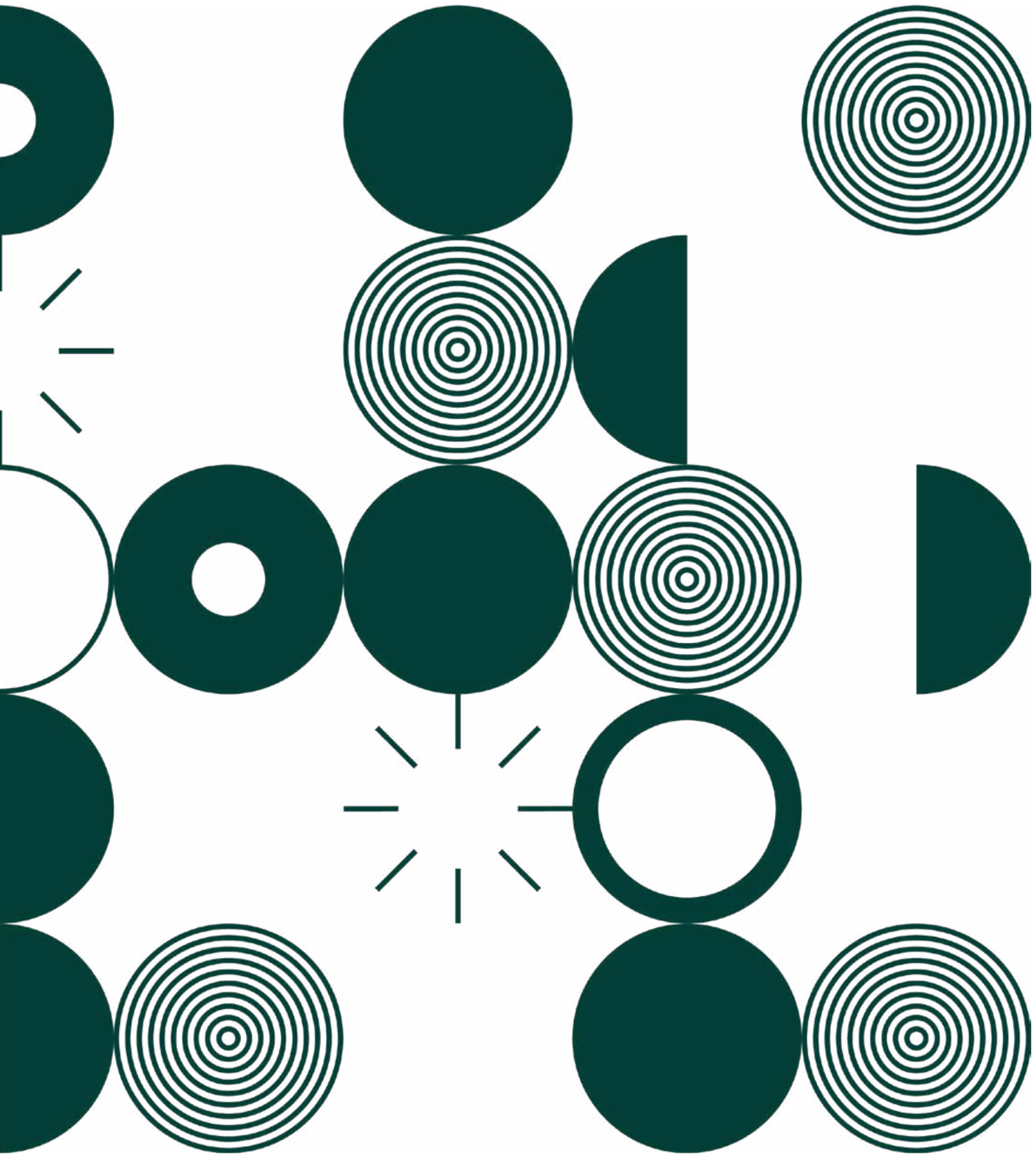
Annual Report 2022

An Coimisiún um Chosaint Sonraí
Data Protection Commission



Contents

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

Commissioner's Foreword

When the GDPR came into force less than five years ago, much commentary centred on the scale of the fines for non-compliance permitted by the Regulation. While 2022 saw significant output from the DPC in its efforts to drive GDPR compliance and protect the rights of those in Ireland and across the EU, it is perhaps both the number - and value - of the fines levied by the DPC against big technology firms that have most visibly demonstrated the GDPR's ability to enforce effective data protection.

I am pleased to present this Annual Report for 2022 which includes details of: in excess of €1billion in punitive fines issued; multiple reprimands and/or compliance orders supervised and enforced following the conclusion of 13 large-scale inquiries; 10,008 individual cases resolved; 4 successful prosecutions under the ePrivacy legislation in respect of 2 companies; observations in relation to 30 pieces of new legislation provided to Government and the Oireachtas; over 300 European Data Protection Board meetings contributed to.

Two-thirds of the fines issued across Europe last year, including the EU, EEA, and UK, were issued by the DPC on foot of detailed and comprehensive investigations, a fact that underlines both the outsized role, and exceptional performance, of the organisation in effectively holding those guilty of non-compliance to account. Summaries of these significant decisions are detailed on page 21 of the report, with full decisions published on the DPC's website. While the extent of these fines has garnered significant attention from stakeholders and the media in 2022, these decisions also demonstrate the DPC's willingness to use other potentially more significant corrective powers, such as orders, to bring about improvements in corporate behaviour and avoid further transgressions.

Progress on other large-scale inquiries, including the DPC's investigation of Facebook's transfers of EU personal data to the USA, are further detailed on pages 27 to 29. Final decisions in several of these cases will be reached in the coming months.

Many of the concluded cross-border DPC decisions have had legal proceedings lodged against them by the relevant regulated entity, including appeal and judicial review proceedings in Ireland. Fines cannot be collected until the Irish courts confirm the fine. An application to confirm the fine cannot be made by the DPC while an appeal is lodged against it. This can amount to a lengthy process. In addition, the relevant regulated entities have also in a number of cases lodged annulment proceedings against European Data Protection Board (EDPB) decisions that informed the adoption of the final decision by the DPC in those cases. A decision of the General Court of the CJEU (T-709-/21) in December 2022 found WhatsApp's application for annulment of the European Data Protection Board (EDPB) decision of July 2021 against the company to be inadmissible as WhatsApp, the court said, lacked the necessary standing to make the application. Despite the binding nature of the EDPB's decisions, the law, as it now stands, states that such decisions cannot be directly challenged by the complainant or controller parties. Instead it requires WhatsApp, in this instance, to apply to the Irish High Court, as part of its appeal against the DPC's Final Decision, to make a preliminary reference to the CJEU concerning the validity of the EDPB decision. The novelty of the political and economic compromise that led to the creation of the One-Stop-Shop, in its current form, has created something of a legal maze that requires constant navigation, building an ever more complex landscape for litigators.

Big Year, Big Law

Page 33 sets out litigation involving the DPC in which written judgments issued last year.

The volume of preliminary references from national courts to the Court of Justice of the European (CJEU) Union on issues not considered "acte clair" under GDPR has continued to increase with around 45 cases currently pending decision at the CJEU. The volume of cases pending at the CJEU signals that it may take some further time before points of legal certainty are

reached on interpretations of key articles of the GDPR. Several important data protection decisions issued from the CJEU in 2022 including a far-reaching decision in August that significantly broadens the interpretation of when special category data is processed (C-184/20). The CJEU also repeated again and again (C-793/19 and C794-19) last year that EU law precludes the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime, including in a reference case from Ireland (C-140/20).

Compensation cases in the EU appear to be continuing the same trend as the last few years with only conservative awards, if any at all, made by Member State courts where cases have progressed to hearing. The first compensation case under section 117 of the 2018 Act to proceed to hearing in Ireland did not buck that trend. It was dismissed in 2022 by the Circuit Civil Court judge ordering the SIPTU members who took the case against their union to pay its costs. The case was taken after the Union inadvertently sent an email with the names and addresses of the claimants to a group of 212 other SIPTU members. The Judge, however, found that proof of more than minimal loss was necessary and that no evidence was presented of any actual loss suffered by the claimants resulting from the email distribution.

Important consultations were initiated by Government Departments with the DPC on more than 30 legislative projects and the DPC appeared before the Joint Oireachtas Committee on Justice as part of its consideration of the General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022. The DPC's observations were urgently requested by the Government on amendments to the Data Retention Act, on foot of the CJEU judgment in April, however these new provisions have not yet been commenced by Government. The Circular Economy Act, the Digital Recordings Bill, the Road Traffic and Roads Bill, and the Policing, Security and Community Safety Bill should, in due course, provide for the proportionate and necessary use of CCTV and Automatic Number Plate Technologies, with clear and precise rules as to how these technologies may be used by Local Authorities and An Garda Síochána, in circumstances where there is currently insufficient legislative underpinning for the data processing. The DPC has issued a number of decisions relating to personal-data processing by local authorities for a variety of purposes by means of CCTV technology where non-compliance with the 2018 Act and the GDPR was found.

National Decisions and Complaint-Handling

The DPC also demonstrated the extraordinary strength of its record in concluding examinations into a wide range of alleged infringements of the GDPR across various sectors last year. Enforcement action covered personal-data security matters in healthcare, banking and insurance sectors; failure to appoint and notify a Data Protection Officer to the DPC; and non-compliance with obligations under the Law Enforcement Directive. Taken in the round, they demonstrate that a failure to adequately assess the risks relating to the particular personal-data processing context of an organisation and to implement correspondingly appropriate technical and organisational measures will lead to poor outcomes for all concerned.

The handling of individual complaints is an important and high-volume area of the DPC's remit. Because of the importance of access rights to unlocking other rights under the GDPR, complaints about access to their personal data remain the most frequent type of complaint the DPC receives. There has been a marked improvement in the response of public sector bodies to access requests, likely due to Data Protection Officers gaining experience in this area and the implementation of improved procedures by these bodies. Complaints from home-occupiers about neighbours' CCTV remain frequent and often intractable where the complaints bring in many issues outside of the scope of data protection.

Cross-border complaints from individuals ground the majority of interactions between EU data protection authorities. Of complaints lodged with the Irish DPC from individuals living here that relate to the actions of a company in another EU member state, 48% have had a resolution via other EU data protection authorities. Of complaints handled by the DPC redirected by other EU authorities, the DPC has resolved 71%. The operation of the One-Stop-Shop in these matters often does not serve individuals well as a result of the way in which it is constructed. For example, an Irish citizen lodged a complaint with the DPC in 2019 about a German company from which they were seeking a spare part. The company had passed on the complainant's details, without their consent, to a UK supplier who had the required spare part. In accordance with the requirements of the GDPR, the DPC referred the complaint to the relevant German authority. Despite the apparent simplicity of the issue, the matter took more than three years to resolve. This is in part due to the requirements for constant back and forth between authorities, necessitating the translation of communications from English to German and vice versa. A final decision was eventually issued in January 2023 from the German authority, however resolution for the complainant, and the respondent, were delayed by the unnecessarily protracted process required by the operation of the One-Stop-Shop. It also involves the transmission of the complainant's personal data around an unnecessarily large number of investigative staff in various EU data protection authorities. This issue requires examination by legislators to improve the timeliness and appropriate handling of decisions for EU citizens.

EU Digital Regulation

It has been clear for quite some time that the general purpose, technology-neutral GDPR does not have, nor was intended to have, the answers to all of the potential harms that can arise online. The new wave of EU digital regulation, including the Digital Services Act (DSA) and Digital Markets Act (DMA), will ensure elements of ex-ante regulation for gatekeepers and Very Large Online Platforms, seeking to create better protections for internet users and online consumers in the EU. Co-ordination between digital regulators in Ireland and at EU level will be vital in ensuring issues relating to platform regulation do not fall between the gaps of the various legal instruments. The DPC looks forward to working with other regulators, particularly in the priority area of protection of children online.

The road ahead is long

2023 will bring big new decisions from the DPC; more judgments from the CJEU; more data protection litigation involving DPC heard in Ireland; the start of application of certain provisions of the DSA and DMA; and the commencement of the Online Safety and Media Regulation Act in Ireland, among other developments. These latter developments will see the entry of regulators of digital platforms onto the pitch. 2022 was a year in which the conclusion of comprehensive DPC enforcement action brought clarity to the application and enforcement of many novel and complex issues under the GDPR. Our work in 2023 is set to continue this trend as we seek to pursue the issues of greatest consequence for data subjects, drive compliance, and, most importantly, safeguard individuals' rights.

Helen Dixon

Commissioner for Data Protection.

Annual Report 2022

Executive Summary

Supporting Individuals

From 1 January 2022 to 31 December 2022:

- The DPC received **21,230** electronic contacts,[1] **6,855** phone calls and **1,118** postal contacts;
- The DPC processed **9,370 new cases** last year: 6,660 in the nature of queries that could be dealt with relatively expeditiously and 2,710 that progressed to a formal complaint-handling process. (9,370 in total is a decrease of 14% on 2021 case figures.)
- The DPC **concluded 10,008** cases in 2022 of which 3,133 were resolved through formal complaint-handling.

In 2022, the most frequent GDPR topics for queries and complaints were: Access Requests; Fair-processing; Disclosure; Direct Marketing and Right to be Forgotten (delisting and/or removal requests).

- Total valid breach notifications received in 2022 was **5,828**.
- Breach notifications **down 12%** on 2021 figures.

The most frequent cause of breaches reported to the DPC arose as a result of correspondence inadvertently being misdirected to the wrong recipients, at **62%** of the overall total.

Investigation and Supervision

As of 31 December 2022, the DPC had **88 Statutory Inquiries** on-hand, including 22 Large-scale Cross-Border inquiries.

In 2022, the DPC - as Lead Supervisory Authority - **received 125** valid cross-border complaints, with **246 cross-border complaints concluded** by the DPC during the year.

In the period 25 May 2018 to end 2022, the DPC received **1,205 valid GDPR cross-border complaints** as Lead Supervisory Authority. **854 (71%)** of these complaints were concluded by the end of 2022.

Through **Supervision** action, the DPC has brought about the **postponement or revision** of **seven** scheduled internet platform projects with implications for the rights and freedoms of individuals

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

Large-scale Inquiries

The DPC concluded the following Large-Scale Inquiries in 2022:

Organisations	Decision Issued	Fine Imposed	Corrective Measure Imposed
Slane Credit Union	January	€5,000	Reprimand re Articles 5(1)(f), 24, 28(1), 28(3), 30(1) and 32(1) GDPR
Personal Injuries Assessment Board	January	None	None
A Consultancy Provider	January	None	Reprimand re Article 32(1) GDPR
Bank of Ireland plc	March	€463,000	Reprimand re Articles 33, 34 and 32 GDPR Orders re Article 32 GDPR
Meta (Facebook)	March	€17 million	None
Twitter International Company	April	None	Reprimand Articles 5(1)(c), 6(1), 17(1) and 12(3) GDPR Order re Article 5(1)(c) GDPR
Pre-hospital Emergency Care Council	May	None	Reprimand re Articles 31, 37(1) and 37(7) GDPR
Allianz plc	June	None	None
Instagram	September	€405 million	Reprimand re Articles 5(1)(a), 12(1), 35(1), 24(1), 5(1)(c), 25(2), 6(1) and 25(1) GDPR Orders re Articles 5(1)(a), 12(1), 35(1), 24(1), 5(1)(c), 25(2), 6(1) and 25(1) GDPR
Airbnb Ireland UC	September	None	Reprimand re Articles 5(1)(c), 6(1), 12(3) GDPR Order re Article 5(1)(c) GDPR
Ark Life Assurance Company DAC	September	None	None
Facebook (Data Scraping)	November	€265 million	Reprimand re 25(1) and 25(2) GDPR Order re Art 25(2) GDPR
An Garda Síochána	December	None	Orders re Sections 71(1)(a), 71(1)(e), 72, 75, 75(1)(b), 75(3), 76(1), 77, 80, 82, 84 and 90(2) of the 2018 Act Temporary ban re specified ANPR cameras Reprimand re Sections 75(3), 76, 84 of the 2018 Act
Virtue Integrated Elder Care Ltd ("VIEC")	December	€100,000	Reprimand re Articles 5(1)(f) and 32(1) GDPR Order re Articles 5(1)(f) and 32(1) GDPR
Fastway Couriers	December	€15,000	Reprimand re Article 32(1) GDPR
Meta (Facebook)	December	€210 million	Order re Articles 5(1)(a), 12(1), 13(1)(c) and 6(1) GDPR
Meta (Instagram)	December	€180 million	Order re Articles 5(1)(a), 12(1) 13(1)(c) and 6(1) GDPR

Confirmation of Administrative Fines

In November 2022, the DPC had its decisions to impose administrative fines on six different organisations confirmed in the Dublin Circuit Court, ranging between €1,500 and €17 million and all of these have been collected since with the funds transferred to the central exchequer in Ireland.

- MOVE Ireland - August 2021 (€1,500)
- Teaching Council - December 2021 (€60,000)
- Limerick City and County Council - December 2021 (€110,000)
- Slane Credit Union - January 2022 (€5,000)
- Bank of Ireland plc - March 2022 (€463,000)
- Meta Platforms Ireland Limited - March 2022 (€17 million)

Engaging with Fellow Regulators

Since 1 January 2022, the DPC:

- Contributed at over **300 EDPB meetings**, which were conducted both virtually and in-person;
- Continued to have representatives on all European Data Protection Board (EDPB) subgroups; and
- Became a founding member – along with the Broadcasting Authority of Ireland, ComReg and the Competition and Consumer Protection Commission – of Ireland's first **Digital Regulators Group**, to help integrate communication with Government and drive regulatory coherence ahead of pending legislative changes at an EU level.

Mainstreaming Data Protection

2022 saw the return to increased numbers of in-person conferences and events. Staff of the DPC presented at **88 speaking events** in 2022, comprising a combination of both virtual and in-person seminars.

The DPC remains committed to driving awareness of data protection rights and responsibilities. In 2022, the DPC:

- Increased awareness-raising and communications activities on DPC social media channels had an organic reach of over **1.4 million**, with strong engagement from stakeholders;
- Produced seven pieces of substantial new guidance including three short guides for children on their data protection rights, as well as five infographics and over 15 new case studies for its website throughout the course of the year;
- Updated 11 pieces of existing guidance to ensure they reflect the most up-to-date developments in data protection law; and
- Published three reports, including the comprehensive One-Stop-Shop Cross-Border Statistics report.

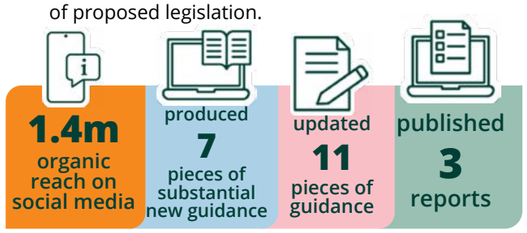
Last year, the DPC participated on the advisory board of the euCONSENT project, an EU-funded initiative to create a framework for age verification (AV) and parental consent tools and solutions to increase the protection of children online by making AV and parental consent tools more effective.

Multiple in-person meetings with NGOs active in the field of data protection.

Other Activity

In 2022 the DPC:

- was a party to 14 judgments delivered and/or final orders made in proceedings before the Irish Courts;
- Concluded **207 electronic direct marketing** investigations;
- **Prosecuted two companies** (telco and publishing house) in respect of four separate charges of sending of unsolicited marketing communications without consent (Regulation 13 of Statutory Instrument 336 of 2011). The Court returned convictions on all charges and it imposed fines totalling €6,500;
- **Received 38 and concluded 58 Law Enforcement Directive** complaints;
- Hosted a delegation of members of the EU Committee on Civil Liberties, Justice and Home Affairs (LIBE) for a productive discussion of effective GDPR enforcement.;
- **Met with EU Commissioner Didier Reynders; EU Executive Vice-Presidents Margrethe Vestager and Vera Jourova, and EU Commissioner Mairéad McGuinness** at different points throughout the year to discuss data protection and Ireland's demonstrated history of effective enforcement of the GDPR; and
- The DPC appeared before the Joint Oireachtas Committee on Justice as part of its consideration of the General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022, and provided input and observations on over 30 pieces of proposed legislation.



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

Roles and Responsibilities

Functions of the DPC

The Data Protection Commission (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

The DPC's Senior Management Committee (SMC) comprises the Commissioner for Data Protection, and nine Heads of Function. 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 2022, the SMC comprised:

- Helen Dixon, Commissioner for Data Protection;
- Ian Chambers, Head of Regulatory Activity [from November 2022];
- Tony Delaney, Head of Regulatory Activity;
- MB Donnelly, Head of Strategy, Governance, Finance, and Risk [from November 2022];
- Graham Doyle, Head of Corporate Affairs, People and Learning, Media and Communications;
- Cian O'Brien, Head of Large-Scale Inquiries and Investigations [from May 2022];
- Ultan O'Carroll, Head of Technology, Operational and Performance;
- Fleur O'Shea, Head of Legal [from April 2022];
- Sandra Skehan, Head of Regulatory Activity [from May 2022];
- Dale Sunderland, Head of Regulatory Consultation, Supervision, Guidance and International Affairs;
- John O'Dwyer, Deputy Commissioner, Head of Regulatory Activity [up to October 2022];
- Anna Morgan, Deputy Commissioner, Head of Legal [up to April 2022]; and
- Colum Walsh, Deputy Commissioner, Head of Regulatory Activity [up to June 2022].

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 **€23.234M** (2021: €19.128M) of which €15,970M (2021: €12.764M) was allocated for pay-related expenditure, and €7.264M (2021: €6.364M) of which was allocated to non-pay expenditure. The funding for 2022 represented **an increase of €4.106M** on the 2021 allocation. The DPC's 2022 Comptroller and Auditor General-audited accounts will be published on the DPC's website once complete and laid before the Houses of the Oireachtas.

Contacts, Queries, and Complaints

Complaints

Between 1 January 2022 and 31 December 2022:

- The DPC received **2,700** complaints from individuals under the GDPR and **10** complaints under the Data Protection Acts 1988 and 2003.
- Overall, the DPC concluded **3,133** complaints, including **1,920** complaints received prior to 2022.

Complaints Received under the GDPR - Top 5 Issues in 2022	No	% of total
Access Request	1,142	42%
Fair Processing	383	14%
Right to erasure	263	10%
Direct Marketing	235	9%
Disclosure	183	7%

Complaint Handling

Where possible, the DPC endeavours to resolve individual complaints informally – as provided for in Section 109(2) of the Data Protection Act 2018. The option to have their issue dealt with by amicable or less formal means is afforded to individuals throughout the lifetime of their complaint, regardless of how far the issue may have progressed through escalated channels.

Where informal and early resolution is not possible, the DPC escalates issues according to complaint category.

Access Rights Complaints

The DPC received **1,142** new access complaints and concluded **1,255** in 2022.

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 **204** new complaints in relation to electronic direct marketing in 2022. These included some 118 complaints in relation to email messages, 52 complaints in relation to text messages, 28 complaints in relation to cookies and 6 complaints concerning phone calls. A total of **207 electronic direct marketing investigations were concluded** in 2022.

This figure is made up of:

- 2 complaints from 2020;
- 50 complaints from 2021; and
- 155 complaints from 2022.

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 for these organisations to be subject to direct oversight by just one DPA, where they have a 'main establishment', rather than being subject to separate regulation by the data protection authorities of each member state. The main establishment of an organisation is generally its place of central administration and/or decision making in the EU/EEA.

In 2022, the DPC - as Lead Supervisory Authority - **received 125 valid cross-border complaints,** with **246 cross-border complaints concluded by the DPC** during the year.

Also in 2022 – as a Concerned Supervisory Authority – the DPC received 12 valid cross-border complaints which it transmitted onwards for resolution to the relevant Lead Authority in the EU.

Since 2018, the DPC has received 1,205 cross-border processing complaints through the OSS. In addition, the DPC has been a Concerned Supervisory Authority in respect of 96 cross-border complaints. The complaints handled by the DPC as Lead Authority were either lodged directly with the DPC by individuals in other EU countries, or they were lodged by individuals with other EU data protection authorities and passed to the DPC under the OSS. The table below illustrates the proportional breakdown of those **1,301 OSS complaints** into 'Lead Supervisory' and 'Concerned Supervisory' roles for the DPC:

DPC Competency	Complaints received in 2022	Complaints Concluded in 2022	Complaints received May 2018-Dec 2022	Complaints concluded May 2018-Dec 2022
DPC as Lead Supervisory Authority	125	245	1,205	854(71%)
DPC as Concerned Supervisory Authority	12	20	96	46(48%)
Total	137	265	1,301	900

Of the 1,205 complaints where Ireland acted as Lead Supervisory Authority, 71% (854) have been concluded.

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 2022, the DPC **received 38** LED complaints and **concluded 58** LED complaints (including complaints received prior to 2022) the majority of which involved An Garda Síochána as the data controller but also included organisations such as the Director of Public Prosecutions, the Irish Prison Service, the Garda Síochána Ombudsman Commission, the Department of Justice and the Department of Foreign Affairs and Trade.

Immediate 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.

Matters prioritised for direct intervention in 2022 included:

- Census data collection practices.
- Residential property sector– excessive data collection.
- Mobile home park– excessive data collection.
- CCTV in cinemas, school toilets, fast-food outlets, nursing home, medical centre.
- Remote access to CCTV as a substitute for onsite workplace supervision.

In selecting certain matters for direct intervention, the DPC is particularly cognisant of its Regulatory Strategy 2022-2027, which identifies "the elderly, non-native speakers and those from at-risk demographics such as the homeless as being in need of specific supports to ensure their data protection rights are upheld."

Complaints under the Data Protection Acts 1988 & 2003

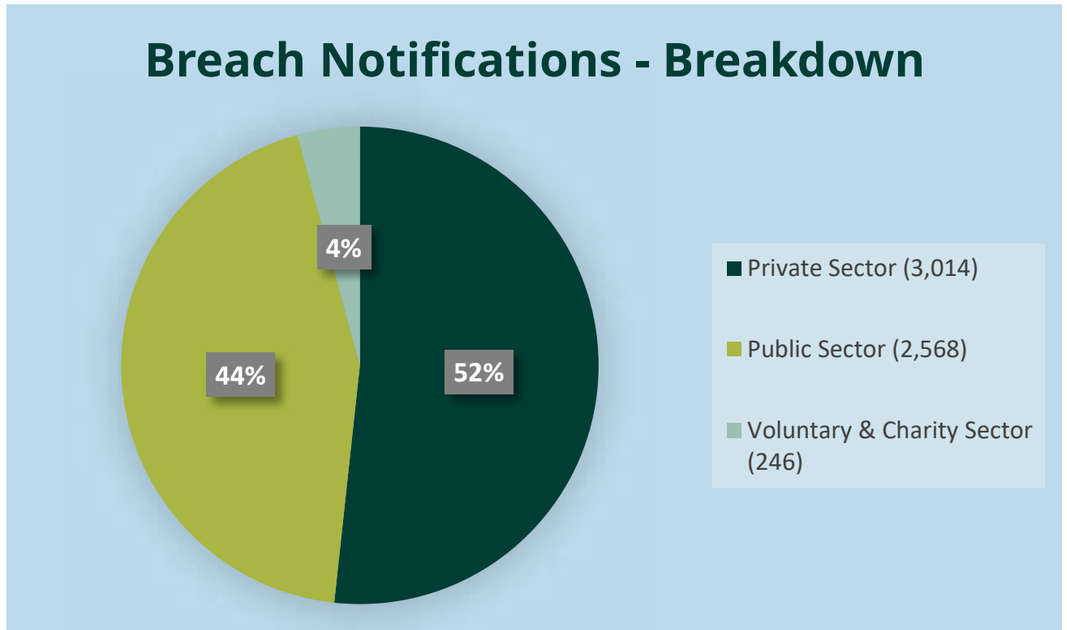
The DPC continues to receive and examine a small number of complaints that fall under the remit of the Data Protection Acts 1988 & 2003. The DPC received **12** such cases in 2022. The Commissioner issued **22** formal decisions under the Data Protection Acts 1988 & 2003 in 2022, of which 6 fully upheld the complaint, 12 partially upheld the complaint and 4 rejected the complaint.

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

Breaches

In 2022, the DPC received **5,828** personal data breach notifications. A total of **5,695** valid **GDPR** data breaches were recorded, representing a **13%** decrease (854) on the **GDPR** data breach numbers reported in 2021. Since the introduction of GDPR – and in line with previous years – the highest category of data breaches notified to the DPC in 2022 related to unauthorised disclosures, in cases affecting one or small numbers of individuals, accounting for **62%** of the total notifications.

Of the total 5,828 breach notifications that the DPC received in 2022, in terms of breakdown, 3,014 related to the private sector, 2,568 to the public sector and the remaining 246 came from the voluntary and charity sector.



Data Breach Notification by Category	Charity	Private	Public	Voluntary	Total
Disclosure unauthorised - Postal Material to incorrect recipient	18	1067	836	15	1936
Disclosure unauthorised - Email incorrect recipient	40	456	563	22	1081
Disclosure unauthorised - Other	24	294	229	24	571
Integrity - unintentional alteration (PD disclosed)		407	7		414
Unauthorised Access - Paper files/ Documents/Records	15	117	178	8	318
Paper Lost/Stolen - Official Documentation		9	236	3	248
Availability - accidental (Loss/destruction of PD)	6	47	189		242
Hacking	12	186	9	2	209
Paper Lost/Stolen	5	38	130	3	176
Processing error - (PD Disclosed)	8	87	47	6	148
Integrity - unauthorised alteration (PD disclosed)	1	80	3		84
Unauthorised Access - Online Account	1	37	22	2	62
Other					339

In keeping with the trend of previous years, public sector bodies and banks account for the "top ten" organisations in terms of the highest number of breach notifications recorded against them, with insurance and telecom companies featuring prominently in the top twenty.

As in previous years, similar issues continue to arise in the breaches notified to the DPC, particularly those from financial institutions. Notably, correspondence issuing to incorrect recipients as a result of poor operational practices and human error - for example inserting a wrong document into an envelope addressed to an unrelated third party – has featured prominently. Additionally, autofill options on email address bars have given rise to a significant number of breach notifications, where emails have been misdirected. These types of errors are attributable to both a failure on the part of organisations to update data in a timely fashion and, in some instances, customers' failure to notify organisations of a change of address.

The DPC continually monitors such breach notifications received, to identify trends and inform potential inquiries. Consequently, in 2022, the DPC issued decisions - and applied fines and sanctions - in a number of inquiries relating to the financial, insurance and public sectors, including Bank of Ireland plc, An Garda Síochána, and Limerick City and County Council. The DPC has noted in particular that its decision pertaining to Bank of Ireland has generated an increase in reports from lending institutions to the DPC, as they apply the learnings from the Bank of Ireland decision to the own processing operations and proactively seek to address any gaps in their operating practices. Details of these decisions can be found on pages 23 - 26.

ePrivacy Breaches

An ePrivacy breach is a breach that is notified to the DPC under Regulation 4 of S.I. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ('the ePrivacy Regulations'), that specifically relates to providers of publically available electronic communications services / networks, e.g. telecommunications companies or online messaging platform providers. All breaches under the ePrivacy Regulations should be notified to the DPC no later than 24 hours after the detection of the personal data breach, regardless of the degree of risk they are believed to pose.

The new European Union (Electronic Communications Code) Regulations 2022 in Ireland (SI 444/2022) E amended in September 2022 a number of definitions including the definition of "electronic communications service", such that certain services such as "over-the-top" services are now brought within the scope of that definition. This will include services such as messaging services. As a result, providers of a wider range of services were required to notify personal data breaches to the DPC.

The DPC received a total of **105** valid data-breach notifications (an increase of 176% on 2021 figure) under the ePrivacy Regulations, which accounted for just **under 2%** of total valid breach cases notified for the year.

As predicted in its 2021 Annual Report, the number of breaches notified to the DPC under the ePrivacy Regulations increased significantly in 2022, due to changes in ePrivacy legislation. The 105 valid data-breaches notified to the DPC in 2022 represents a **three-fold increase on the previous year's figures**.

Law Enforcement Directive Breaches

The DPC also received **38** breach notifications in relation to the LED, (Directive (EU) 2016/680), which has been transposed into Irish law, by certain parts of the Data Protection Act 2018.

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

European Union Justice Commissioner Didier Reynders meets with DPC staff.

Inquiries

Statutory Inquiries by the DPC

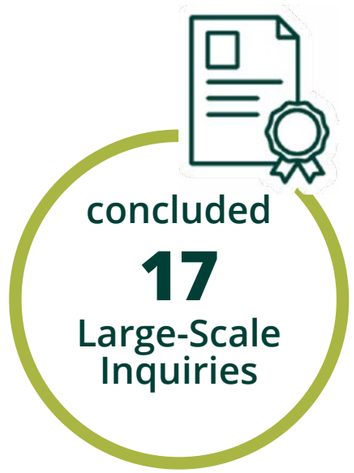
Under the Data Protection Act 2018, the DPC may conduct two different types of statutory inquiry under Section 110 in order to establish whether an infringement of the GDPR or the 2018 Act has occurred:

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

The objective of any inquiry is to:

- establish the facts as they apply to the matters under investigation;
- apply the provisions of the GDPR and/or 2018 Act as applicable to the facts as found in order to analyse whether an infringement of the GDPR and/or 2018 Act has been identified;
- make a formal decision of the DPC in relation to whether or not there is an infringement; and
- where an infringement has been identified, make a formal decision on whether or not to exercise a corrective power, and if so, which corrective power[2].

As of 31 December 2022, the DPC had **88 Statutory Inquiries** on-hand, including **22 Large-Scale Cross-Border Inquiries.**



2) Corrective powers include imposing an administrative fine (not applicable for infringements of the LED), issuing a warning, a reprimand, a temporary or definitive ban on processing or a suspension of international data transfers or a direction to bring processing into compliance, amongst others.

Large-Scale Inquiries that concluded in 2022

Organisations	Decision Issued	Fine Imposed	Corrective Measure Imposed
Slane Credit Union	January	€5,000	Reprimand re Articles 5(1)(f), 24, 28(1), 28(3), 30(1) and 32(1) GDPR
Personal Injuries Assessment Board	January	None	None
A Consultancy Provider	January	None	Reprimand re Article 32(1) GDPR
Bank of Ireland plc	March	€463,000	Reprimand re Articles 33, 34 and 32 GDPR Orders re Article 32 GDPR
Meta (Facebook)	March	€17 million	None
Twitter International Company	April	None	Reprimand Articles 5(1)(c), 6(1), 17(1) and 12(3) GDPR Order re Article 5(1)(c) GDPR
Pre-hospital Emergency Care Council	May	None	Reprimand re Articles 31, 37(1) and 37(7) GDPR
Allianz plc	June	None	None
Instagram	September	€405 million	Reprimand re Articles 5(1)(a), 12(1), 35(1), 24(1), 5(1)(c), 25(2), 6(1) and 25(1) GDPR Orders re Articles 5(1)(a), 12(1), 35(1), 24(1), 5(1)(c), 25(2), 6(1) and 25(1) GDPR
Airbnb Ireland UC	September	None	Reprimand re Articles 5(1)(c), 6(1), 12(3) GDPR Order re Article 5(1)(c) GDPR
Ark Life Assurance Company DAC	September	None	None
Facebook (Data Scraping)	November	€265 million	Reprimand re 25(1) and 25(2) GDPR Order re Art 25(2) GDPR
An Garda Síochána	December	None	Orders re Sections 71(1)(a), 71(1)(e), 72, 75, 75(1)(b), 75(3), 76(1), 77, 80, 82, 84 and 90(2) of the 2018 Act Temporary ban re specified ANPR cameras Reprimand re Sections 75(3), 76, 84 of the 2018 Act
Virtue Integrated Elder Care Ltd ("VIEC")	December	€100,000	Reprimand re Articles 5(1)(f) and 32(1) GDPR Order re Articles 5(1)(f) and 32(1) GDPR
Fastway Couriers	December	€15,000	Reprimand re Article 32(1) GDPR
Meta (Facebook)	December	€210 million	Order re Articles 5(1)(a), 12(1), 13(1)(c) and 6(1) GDPR
Meta (Instagram)	December	€180 million	Order re Articles 5(1)(a), 12(1) 13(1)(c) and 6(1) GDPR

Confirmation of Administrative Fines

In November 2022, the DPC had its decisions to impose administrative fines on six different organisations confirmed in the Dublin Circuit Court, ranging between €1,500 and €17 million and all of these have been collected since with the funds transferred to the central exchequer in Ireland.

- MOVE Ireland - August 2021 (€1,500)
- Teaching Council - December 2021 (€60,000)
- Limerick City and County Council - December 2021 (€110,000)
- Slane Credit Union - January 2022 (€5,000)
- Bank of Ireland plc - March 2022 (€463,000)
- Meta Platforms Ireland Limited - March 2022 (€17 million)

National Inquiries

Inquiries that were concluded in 2022

Slane Credit Union - (fine confirmed by the court)

A Final Decision was issued to Slane Credit Union Limited on 26 January 2022. The inquiry arose from a personal data breach that involved the unintended publication of member personal data on the internet. The decision found that Slane Credit Union had infringed of Articles 5(1)(f), 24, 28(1), 28(3), 30(1) and 32(1) of the GDPR. A reprimand was imposed for all of the infringements and a fine of €5,000 was imposed for the infringement of Article 5(1)(f) of the GDPR (principle of security of processing).

Personal Injuries Assessment Board

This inquiry was commenced in respect of a personal data breach that the Personal Injuries Assessment Board ('PIAB') notified to the DPC on 10 December 2019. The personal data breach occurred when a third party organisation ('the Third Party') contracted by PIAB returned materials containing personal data to PIAB on an unencrypted USB key in a paper envelope, which USB key was ultimately lost in the post with only a ripped envelope delivered to PIAB.

The Inquiry considered whether the PIAB had complied with its obligation to implement an appropriate level of security under Article 32 GDPR. The DPC issued its decision on 24 January 2022 and found no infringement in circumstances where PIAB had requested in advance that the Third Party not send the personal data to PIAB and where it could not have foreseen that the Third Party would post an unencrypted USB storage device in an unpadded envelope by ordinary (not registered) post.

A Consultancy Provider

This inquiry was commenced in respect of a personal data breach that the Personal Injuries Assessment Board ('PIAB') reported to the Data Protection Commission on 10 December 2019, which, as set out above, occurred when a Consultancy Provider sent an unencrypted USB storage device, containing personal data to PIAB, despite PIAB expressly stating the data was not to be sent.

The DPC issued its decision on 24 January 2022 and found that the Consultancy Provider had infringed Article 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data. The decision issued the Consultancy Provider with a reprimand in respect of the infringement.

Bank of Ireland plc - (fine confirmed by the court)

This inquiry related to unauthorised disclosures of customer personal data to the Central Credit Register and accidental alterations of customer personal data on the CCR. The decision found that Bank of Ireland plc infringed Article 33 GDPR by failing to report the personal data breaches without undue delay and by failing to provide sufficient detail to the DPC in respect of the data breaches. BOI infringed Article 34 by failing to issue a communication to data subjects without undue delay in circumstances where the personal data breaches were likely to result in a high risk to data subjects' rights and freedoms. Article 32(1) GDPR was infringed by BOI's failure to ensure a level of security appropriate to the risks involved in transferring information to the CCR. BOI was issued with a fine of €463,000 for the infringements. BOI was also reprimanded and ordered to bring its technical and organisational measures into compliance with Article 32(1).

Pre-Hospital Emergency Care Council

On 3 May 2022, the DPC issued its Final Decision in relation to an inquiry commenced as a result of a monitoring and enforcement exercise carried out pursuant to the tasks of a supervisory authority contained in Article 57 of the GDPR. The Pre-Hospital Emergency Care Council (PHECC) was one of many public sector organisations contacted during the monitoring and enforcement exercise. PHECC did not respond to any correspondence issued to it. There was no record in the DPC of the PHECC having communicated its DPO details to the DPC. In addition, there were no contact details for a DPO available on the PHECC website.

The Decision found that the PHECC infringed Article 37(1) and (7) of the GDPR by failing to designate a data protection officer for the organisation, and by failing to publish the contact details of a data protection officer and failing to communicate the contact details to the supervisory authority. The Decision also found that the PHECC infringed Article 31 of the GDPR by failing to cooperate, on request, with the DPC in the performance of its tasks. The Decision issued the PHECC with a reprimand in respect of these infringements.

Allianz

This inquiry was commenced after Allianz had notified personal data breaches to the DPC between 25 June 2020 and 31 December 2020. The decision considered whether Allianz had complied with Article 32(1) GDPR. It was held that Allianz had complied with Article 32(1) as it had implemented policies, which were specifically tailored to the risks associated with the processing. Allianz also provided repeated training to sectors of the business, which were the most susceptible to personal data breaches of this kind. Allianz also took proactive measures to counter the increasing risk profile of some business units by implementing additional security measures after some personal data breaches occurred. Accordingly, no corrective powers were exercised in this decision.

Ark Life

On 26 September, The DPC issued its Final Decision in relation to an inquiry into personal data breach notifications from Ark Life during the period December 2018 to May 2021. The data breach notifications primarily concerned the unauthorised disclosure of personal data as a result of address inaccuracies and issues within the postal and email procedures operated by Ark Life.

The decision considered whether Ark Life had complied with Article 32(1) GDPR. It found that Ark Life had implemented policies which were specifically tailored to the risks associated with the processing. Ark Life also provided repeated training to sectors of the business which were the most susceptible to personal data breaches of this kind. Ark Life also took proactive measures to counter the increasing risk profile of some business units by implementing additional security measures after some personal data breaches occurred. These measures addressed inherent flaws in their processes concerning customer contact details and dealing with returned mail.

Taking into account the quantum of data breaches, the technical and organisational measures implemented by Ark Life and the moderate to low severity of risk to data subjects, DPC concluded that Ark Life did not infringe Article 32(1). Accordingly no corrective powers were exercised in this decision.

An Garda Síochána

On 15 December 2022 the DPC issued a final Decision to An Garda Síochána (AGS), in respect of a data breach under Part 5 of the Data Protection Act 2018 (the LED), following a report by AGS to the DPC of a personal data breach. The breach involved the disclosure of personal data that was processed by AGS in Kilmainham Garda Station, and which disclosed the names and addresses of 108 data subjects, some of whom were children. The Decision found that AGS infringed Sections 71, 72, 75 and 78 of the Data Protection Act 2018. The Decision ordered AGS to bring its processing into compliance and imposed a reprimand on AGS.

Virtue Integrated Elder Care Ltd - (fine pending confirmation by the court)

In December 2022, the DPC issued a decision to Virtue Integrated Elder Care Ltd ("VIEC") regarding a personal data breach that VIEC notified to the DPC. The breach concerned an unknown actor who gained access to a VIEC manager email account, likely by way of a phishing attack, and set up mail forwarding rules to an external account. As a result of this, the personal data of residents, including special category data such as health and biometric data, was accessed by the unknown actor. The decision found that VIEC infringed Articles 5(1)(f) and 32(1) GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of resident data on its email system participants' and facilitators' personal data. The decision imposed an administrative fine on VIEC in the amount of €100,000 in respect of the infringement of Article 5(1)(f) GDPR, reprimanded VIEC and ordered VIEC to bring its processing operations into compliance with Articles 5(1)(f) and 32(1) GDPR by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Fastway Couriers - (fine pending confirmation by the court)

In December 2022, the DPC adopted a decision concerning A&G Couriers Limited T/A Fastway Couriers Ireland (Fastway) regarding a personal data breach that Fastway notified to the DPC. The personal data breach concerned unauthorised access to a significant amount of personal data.

The decision found that Fastway infringed Article 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its processing of personal data. The decision reprimanded Fastway and imposed an administrative fine in the amount of €15,000 in respect of the infringement.

Inquiries at draft decision stage by end 2022

Centric Health

The DPC commenced this Inquiry following a ransomware attack potentially affecting patient data held on Centric's patient administration system. The DPC issued its draft decision in October 2022 and is currently drafting the final decision having received Centric Health's submissions on the Draft Decision.

Kildare County Council

This Inquiry considers a broad range of issues pertaining to surveillance technologies deployed by the Council. It is one of a number of own-volition inquiries into a broad range of issues pertaining to surveillance technologies deployed by State authorities. The DPC has issued final decisions in own-volition inquiries concerning Kerry County Council, Waterford City and County Council, and Limerick City and County Council. The DPC issued its Draft Decision in November 2022.

Department of Health

An inquiry into the Department of Health was initiated in 2021. The inquiry relates to the processing of personal data by the Department of Health in its special needs education litigation files, following allegations made publicly in March 2021. The decision-making process is ongoing as of the end of 2022.

Bank of Ireland plc

This Inquiry examines a potential unauthorised disclosure of personal data in relation to the Banking 365 service arising from how customer accounts were configured. The DPC issued its Draft Decision in November 2022 to the controller.

Catholic Church (Archbishop of Dublin)

The Draft Decision has been issued in relation to 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.

Inquiries where submissions on a statement of issues or inquiry report were invited from the relevant parties by end 2022.

Department of Social Protection

This inquiry involves an examination of the processing of personal data in relation to biometric facial templates used by the Department in its Public Service Card registration process. The inquiry was commenced in July 2021 and involved on-site inspections at two locations in March of this year. An Issues Paper, setting out the facts established in the course of the Inquiry and the data protection issues to be considered by the DPC, was provided to the Department in August 2022. A Draft Decision is currently in preparation.

Permanent TSB

The DPC commenced this inquiry following three separate breach notifications from Permanent TSB in May 2022. All three personal data breach notifications concern circumstances where a malicious actor attempted to gain access to a data subject's bank account by calling PTSB's Open 24 call centre. The DPC is currently preparing a Draft Decision.

Cross Border Inquiries

Inquiries that were concluded in 2022

Meta (Facebook) - 12 Breaches - (fine confirmed by the court)

This inquiry concerned an examination into a series of 12 personal data breach notifications that Meta Platforms Ireland Limited ('Meta') notified to the DPC in the six-month period between 7 June 2018 and 4 December 2018. The DPC circulated its draft decision in the matter to the other EU supervisory authorities concerned on 18 August 2021, for the purpose of the co decision-making process outlined in Article 60 GDPR. While objections to the DPC's draft decision were raised by two of the European supervisory authorities, consensus was achieved through further engagement between the DPC and the supervisory authorities concerned.

The DPC adopted its decision in March 2022 and that decision found that Meta infringed Articles 5(2) and 24(1) GDPR by failing to have in place appropriate technical and organisational measures, which would enable it to readily demonstrate the security measures that it implemented in practice to protect EU users' data, in the context of the twelve personal data breaches. The decision imposed a fine of €17 million on Meta.

Twitter

This inquiry was commenced after a complaint was lodged directly with the DPC against Twitter International Company ("Twitter). The complainant alleged that, following the suspension of their Twitter account, Twitter failed to comply within the statutory timeframe with an erasure request they had submitted to it. Further, the complainant alleged that Twitter had requested a copy of their photographic ID in order to action their erasure request without a legal basis to do so. Finally, the complainant alleged that Twitter had retained their personal data following their erasure request without a legal basis to do so. Full details of this inquiry can be found on pages 84-86.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): processing of children's data via the Instagram service operated by Facebook - (Meta has lodged an appeal before the courts)

The DPC commenced this own-volition inquiry on 21 September 2020 and the scope of the inquiry concerned two types of processing carried out by Meta Platforms Ireland Limited ('Meta') (as the data controller of the personal data processed in the context of the Instagram platform), as follows:

1. Meta allowed child users between the ages of 13 and 17 to operate 'business accounts' on the Instagram platform. At certain times, the operation of such accounts required and/or facilitated the publication (to the world-at-large) of the child user's phone number and/or email address.
2. At certain times, Meta operated a user registration system for the Instagram service whereby the accounts of child users were set to "public" by default, thereby making public the social media content of child users, unless the account was otherwise set to "private" by changing the account privacy settings.

In December 2021, the DPC submitted a draft decision to the Article 60 process. The DPC received objections from other concerned supervisory authorities and was unable to reach consensus. Therefore, the DPC referred the objections to the European Data Protection Board ("EDPB") for determination pursuant to the dispute resolution process provided for in Article 65 GDPR. The EDPB adopted its binding decision on the subject-matter of the objections on 28 July 2022.

The DPC's adopted its Decision on 2 September 2022 and found that Meta infringed Articles 6(1), 5(1)(a), 5(1)(c), 12(1), 24, 25(1), 25(2) and 35(1) GDPR. The decision imposed administrative fines totalling €405 million on Meta. In addition to these administrative fines, the DPC also imposed a reprimand and an order requiring Meta to bring its processing into compliance by taking a range of specified remedial actions.

Airbnb Ireland UC (Airbnb)

A complaint was lodged with the Berlin Commissioner for Data Protection and Freedom of Information ("Berlin DPA") against Airbnb Ireland UC ("Airbnb") and was thereafter transferred to the DPC to be handled in its role as lead supervisory authority.

The complainant alleged that Airbnb failed to comply with an erasure request and a subsequent access request they had submitted to it within the statutory timeframe. Further, the complainant stated that when they submitted their request for erasure, Airbnb requested that they verify their identity by providing a photocopy of their identity document ("ID"), which they had not previously provided to Airbnb. Details of this inquiry can be found on pages 87-88.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited) - (Meta has lodged an appeal before the courts)

In April 2021, the DPC became aware of multiple media reports which highlighted that a collated dataset of Facebook user personal data had been made available online. The personal data related to approximately 533 million Facebook users worldwide. An inquiry was commenced in April 2021 to examine whether Meta Platforms Ireland Limited ('Meta') complied with its obligations under 25(1) and 25(2) GDPR – data protection by design and default. The Article 60 process, whereby the DPC sends draft decisions to other concerned supervisory authorities to review and raise any 'relevant and reasoned objections' that they may have, commenced in September 2022 and the Draft Decision did not receive any relevant and reasoned objections.

The DPC adopted its Final Decision on 25 November 2022. The Decision finds that Meta infringed Article 25(1) by failing to implement appropriate technical and organisational measures designed to implement the purpose limitation principle and the integrity and confidentiality principle in an effective manner. The Decision also finds that Meta infringed Article 25(2) GDPR by failing to implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing were processed; and by failing to ensure that by default the personal data were not made accessible without the data subjects' intervention to an indefinite number of natural persons. The Decision also imposes two administrative fines totally €265million, a reprimand, and orders Facebook to bring its processing into compliance with Article 25(2) GDPR.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): complaint received from NOYB concerning the Facebook service

This complaint-based inquiry concerned the legal basis on which Meta Platforms Ireland Limited ('Meta') relies to process the personal data of users of its platform and certain issues related to transparency information provided by Facebook to its users. A draft decision in this Inquiry was sent to other concerned supervisory authorities on 6 October 2021 for the purpose of the co-decision-making process outlined in Article 60 GDPR. The DPC received objections from other concerned supervisory authorities and was unable to reach consensus with the CSAs on the subject-matter of the objections. Therefore, the DPC referred the objections to the European Data Protection Board ("EDPB") for determination pursuant to the dispute resolution process provided for in Article 65 GDPR. The EDPB adopted its binding decision on the subject-matter of the objections on 5 December 2022.

The DPC adopted its decision on 31 December 2022. The decision found that Meta is not entitled to rely on the "contract" legal basis in connection with the delivery of behavioural advertising as part of its Facebook 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 Meta infringed Articles 5(1)(a), 12(1) and 13(1)(c). The DPC found that Meta did not comply with its obligations in relation to transparency as information in relation to the legal basis relied on by Meta 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 which of the six legal bases identified in Article 6 of the GDPR.

The decision ordered Meta to bring its processing operations into compliance with the GDPR within a period of 3 months and imposed administrative fines totalling €210 million.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): complaint received from NOYB concerning the Instagram service operated by Facebook

This complaint-based inquiry concerns the legal basis on which Meta Platforms Ireland Limited ('Meta') relies to process the personal data of users of its Instagram platform and certain issues related to transparency information which is provided to Instagram users. The DPC sent a draft decision in this Inquiry to other concerned supervisory authorities for the purpose of the co-decision-making process outlined in Article 60 GDPR. The DPC received objections from other concerned supervisory authorities and was unable to reach consensus with the CSAs on the subject-matter of the objections. Therefore, the DPC referred the objections to the European Data Protection Board ("EDPB") for determination pursuant to the dispute resolution process provided for in Article 65 GDPR. The EDPB adopted its binding decision on the subject-matter of the objections on 5 December 2022.

Similar to the Decision regarding the Facebook service outlined above, the DPC adopted its decision on 31 December 2022. The decision found that Meta is not entitled to rely on the "contract" legal basis in connection with the delivery of behavioural advertising as part of its Instagram 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 Meta infringed Articles 5(1)(a), 12(1) and 13(1)(c). The DPC found that Meta did not comply with its obligations in relation to transparency as information in relation to the legal basis relied on by Meta 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 which of the six legal bases identified in Article 6 of the GDPR.

The decision ordered Meta to bring its processing operations into compliance with the GDPR within a period of 3 months and imposed administrative fines totalling €180 million.

DPC Draft Decisions at Article 65 as at 31 December 2022

WhatsApp Ireland Limited (WhatsApp): complaint received from NOYB

This complaint-based inquiry concerns the legal basis on which WhatsApp Ireland Limited ('WhatsApp') relies to process the personal data of WhatsApp users. The DPC sent a draft decision in this Inquiry to other concerned supervisory authorities for the purpose of the co-decision-making process outlined in Article 60 GDPR. The DPC received objections from other concerned supervisory authorities and was unable to reach consensus with the CSAs on the subject matter of the objections. Therefore, the DPC referred the objections to the European Data Protection Board ("EDPB") for determination pursuant to the dispute resolution process provided for in Article 65 GDPR. The EDPB adopted its binding decision on the subject matter of the objections on 5 December 2022.

DPC Draft Decisions at Article 60 as at 31 December 2022

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

This inquiry concerns TikTok's compliance with the GDPR's data protection by design and default requirements as they relate to the processing of personal data in the context of platform settings for users under age 18 and age verification measures for persons under 13. This inquiry is also examining whether TikTok has complied with the GDPR's transparency obligations in the context of the processing of personal data of users under age 18. The inquiry was commenced in September 2021 and the DPC submitted its Draft Decision to the Article 60 process on 13 September 2022. That process remains ongoing.

Yahoo! EMEA Limited

The inquiry examines Yahoo! EMEA Limited's compliance with the requirements to provide transparent information to data subjects under the provisions of the GDPR. The Preliminary Draft Decision provided Yahoo! with an opportunity to make submissions prior to the matter being considered by the concerned supervisory authorities across the EU under the Article 60 process.

In line with Article 60 GDPR, the DPC subsequently issued a Draft Decision in the inquiry into Yahoo!'s processing to concerned supervisory authorities on 27 October 2022. That process remains ongoing.

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

This inquiry is concerned with examining the lawfulness of data transfers from the EU to the US in relation to the Facebook service. The own-volition inquiry relates to such data transfers generally as they apply to the personal data of Facebook users while a separate complaint-based inquiry is concerned with a complaint made by Mr Maximillian Schrems against Meta Platforms Ireland Limited (formerly Facebook Ireland Limited).

The DPC circulated its draft decision in the own-volition matter to the Concerned Supervisory Authorities in July 2022, for the purposes of the co-decision making process outlined in Article 60 GDPR. In response a number of Supervisory Authorities raised objections or made comments on the decision. The DPC issued a composite response to the objections in September 2022. A number of the CSAs maintained their objections. The DPC subsequently triggered the Article 65 dispute resolution process which is still ongoing.

Airbnb Ireland UC (Airbnb)

This inquiry was commenced following receipt of a complaint that Airbnb had unlawfully requested a copy of ID in order to verify the Complainant's identity, in particular in circumstances where the Complainant, as a registered member and host with Airbnb, had not previously provided her ID to Airbnb and that Airbnb had failed to comply with the principle of data minimisation when requesting a copy of the individual's ID in order to verify their account.

In its draft decision, the DPC noted Airbnb claimed legitimate interests pursued by Airbnb as the lawful basis for requesting a copy of ID to verify identity in order to protect the safety and security of the users of the Airbnb platform, in accordance with Article 6(1)(f) of the GDPR. Noting that the platform that Airbnb operates brings hosts and members who are unknown to each other into a situation where they may actually meet in person at the host's premises, or elsewhere, the DPC agreed that a legitimate interest existed in Airbnb ensuring it had adequate safety and security measures in place to protect users of the platform. The DPC took the view that the service operated by Airbnb is significantly different to a purely online service such as a social media platform. Given that Airbnb members stay at the premises of a host "in the real world", the DPC recognised the importance of verifying the identity of hosts to ensure that they are who they say they are. Given that other means of validating this host's identity failed, the DPC found that it was necessary to process the photo ID in pursuit of the legitimate interest. The DPC found that in a balancing test, the rights of the host were not prejudiced by this verification process.

The DPC did not receive any relevant or reasoned objections to the draft decision from the concerned supervisory authorities under Article 60(4).

Cross-border inquiries where submissions on a preliminary draft decision, statement of issues, or inquiry report were invited from the relevant parties during 2022 and inquiries that are currently at an investigative stage by end 2022

Google Ireland Limited (Google): Location data inquiry

The DPC received a number of complaints from various consumer organisations across the EU, in which concerns were raised with regard to Google's processing of location data. The issues raised within the concerns related to the legality of Google's processing of location data and the transparency surrounding that processing. As such the DPC commenced an own-volition Statutory Inquiry, with respect to Google Ireland Limited, pursuant to Section 110 of the Data Protection 2018 and in accordance with the cooperation mechanism outlined under Article 60 of the GDPR. The Inquiry set out to establish whether Google has a valid legal basis for processing the location data of its users and whether it meets its obligations as a data controller with regard to transparency. The DPC's preliminary draft decision was provided to Google in December 2021 for its submissions. The DPC received submissions from Google and prepared a Revised Preliminary Draft Decision. On 21 December 2022, the DPC provided the Revised Preliminary Draft Decision to various consumer protection agencies for the purpose of enabling those consumer protection agencies to make observations.

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

This inquiry relates to an examination of whether Facebook 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. The DPC issued a Preliminary Draft Decision to Meta Platforms Ireland Limited on 12 December 2022 for the purpose of inviting submissions.

Meta Platforms Ireland Limited breach notification issues

This inquiry relates to Meta Platforms Ireland Limited's (formerly Facebook Ireland Limited) 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. The DPC issued a Preliminary Draft Decision to Meta Platforms Ireland Limited on 12 December 2022 for the purpose of inviting submissions.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): passwords stored in plain text

This inquiry examined whether Meta Platforms Ireland Limited ('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. The DPC issued a Preliminary Draft Decision to Meta Platforms Ireland Limited on 21 December 2022 for the purpose of inviting submissions.

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 proprietary "Authorised Buyers" real time bidding advertising technology 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. As at 31 December 2022, the DPC was at an advanced stage in preparing a Preliminary Draft Decision.

Twitter: "5 Breaches"

This inquiry relates to an own-volition inquiry with respect to Twitter International Company (now "Twitter International Unlimited Company"), concerning the company's compliance with Articles 5, 24, 25, 32 and 33 GDPR in the context of a series of personal breaches notified to the DPC between August and October 2018. The decision-making stage commenced in February 2022 and the DPC is currently preparing a Preliminary Draft Decision.

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

This inquiry relates to 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. A Statement of Issues setting out the relevant factual matters and issues for determination was provided to Tiktok for its submissions in July 2022 and submissions were subsequently received on that document. The DPC is currently preparing a Preliminary Draft Decision.

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. As at 31 December 2022, the DPC was preparing a Statement of Issues for the purposes of inviting submissions from Yelp.

Twitter December 2022

In December 2022, the DPC commenced an own-volition inquiry with respect to Twitter International Unlimited Company in relation to multiple international media reports, which highlighted that one or more collated datasets of user personal data had been made available on the internet. The Inquiry is ongoing and is considering whether Twitter International Unlimited Company has complied with its obligations, as controller, in connection with the processing of personal data of its users or whether any provision(s) of the GDPR and/or the Act have been, and/or are being, infringed in this respect.

Over 100 cases involving individual complainants concluded by DPC through EU Co-Operation procedure in 2022

In addition to these large scale inquiries, the DPC also concludes individual cross-border cases through the EU Co-Operation procedure. In 2022, the DPC concluded over 100 such cases and an example can be found on page 89.

Details of these cases can be found published on the EDPB Article 60 case register.

The table on the following pages illustrates where objections were lodged in each large-scale case.

Annual Report 2022

Art 60 Draft Decisions (with objections)

	Twitter	WhatsApp	Instagram	Facebook	Facebook (NOYB)	Facebook (12 breaches)	Ryanair	Groupon	Twitter	WhatsApp (NOYB)	Instagram (NOYB)	Meta (Transfers)	Airbnb	Tik Tok	Meta (Scraping)	Yahoo! EMEA	Airbnb
Austria	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓
Belgium	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Bulgaria	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Croatia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cyprus	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Czechia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Denmark	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Estonia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Finland	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓
France	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✗	✗	✓	✓	✓	✗	✓
Germany*	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗	✓	✗	✓
Greece	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Hungary	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓
Iceland	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Italy	✗	✗	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓
Latvia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Liechtenstein	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Lithuania	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Luxembourg	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Malta	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Netherlands	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓
Norway	✓	✓	✗	✗	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓
Poland	✓	✗	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Portugal	✓	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Romania	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Slovakia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Slovenia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Spain	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓
Sweden	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓

Germany in this instance denotes the federal DPA **and all Lander DPAs*

✗ **Objection lodged** ✓ **No objection lodged**

Litigation

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
1.	Record Number: 2018/419 [2022] IECA 95	Agnieszka Nowak v DPC	Statutory Appeal Court of Appeal	Judgment dated 13 April 2022 Order dated 23 May 2022
Outcome				Current Status
Written judgment delivered on 13 April 2022, dismissing the appeal. On 9 December 2016, the DPC delivered a decision in response to a complaint by Ms Nowak against her employer, alleging that her employer had failed to comply fully with an access request she had made, within the relevant time period. In its decision, the DPC found that the employer had complied with the request, but its response was late. Ms Nowak appealed to the Circuit Court, contending that her employer (and the DPC) had misconstrued her request. The Circuit Court disagreed, upholding the DPC's decision. On a further appeal on a point of law, the High Court likewise upheld the decision. The Court of Appeal rejected Ms Nowak's further appeal, for the reasons set out in its judgment of 13 April 2022, noting that Ms Nowak had failed to identify any point of law that would warrant the intervention of the Court. Costs were also awarded to the DPC. A subsequent application by Ms Nowak for leave to bring a further appeal to the Supreme Court was unsuccessful.				The proceedings have concluded.

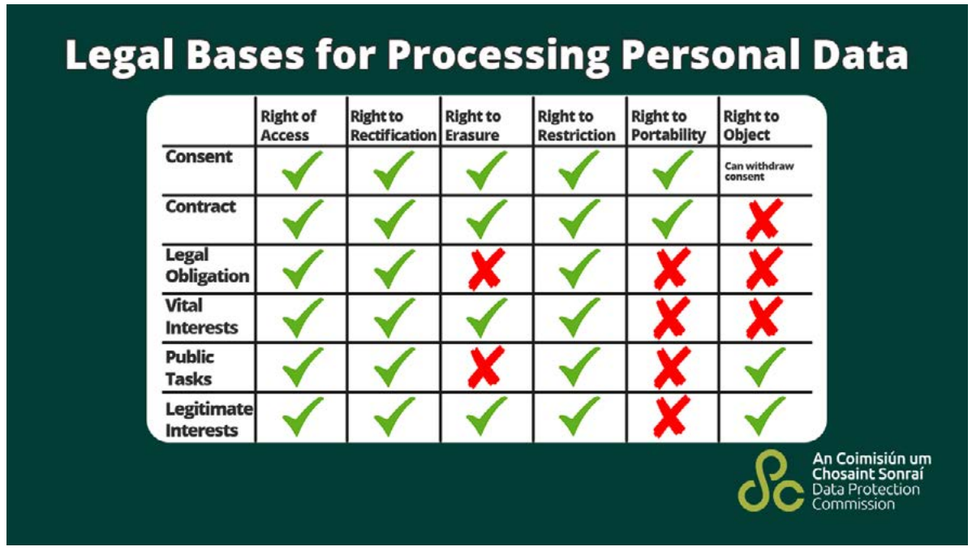
No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
2.	2021/CA005	Ellen Thorsch v DPC and WRC	Statutory Appeal Carlow Circuit Court	Order dated 31 March 2022
Outcome				Current Status
Ms Thorsch made a complaint to the DPC, alleging that the Equality Tribunal had failed to comply with an access request, within the timeframe allowed. Ms Thorsch later made a further allegation to the effect that the Equality Tribunal had wrongly published her personal data online and that, because of the manner of its publication, her data had been unlawfully transferred out of the State. The DPC delivered a decision in which it upheld Ms Thorsch's complaint insofar as the Equality Tribunal had failed to respond to her access request within the relevant time period but rejecting the other grounds of complaint. Ms Thorsch then brought an appeal to the Circuit Court in respect of the points on which her complaint had been rejected. By Order made on 31 March 2022, the Circuit Court dismissed the appeal on the basis that the appeal was time-barred, Ms Thorsch having failed to file her appeal within the relevant 21-day period. The Court further held that it had no jurisdiction to extend the 21-day period in question.				The proceedings have concluded.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
3.	Record No. 2021/00340	Director of Corporate Enforcement v. DPC and another	Circuit Court (Dublin)	01 April 2022
Outcome				Current Status
On 14 January 2021, the DPC delivered a decision upholding a complaint received from a data subject against the ODCE, finding that the ODCE had wrongly refused to provide the data subject with access to certain of his personal data in response to an access request. The decision was appealed by the ODCE to the Circuit Court. By written judgment dated 1 April 2022, the Court allowed part of the appeal on the basis that the DPC had not applied fair procedures in arriving at its decision. Specifically, the Court found that, when delivering its final decision, the DPC did not give the ODCE fair notice of certain amendments it had made to a draft version of the decision previously shared with the parties. The complaint was remitted to the DPC so that it could receive further submissions from the parties in relation to the amendments in question and then prepare a revised decision to take account of same.				The proceedings have concluded.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
4.	2019/008215	2019/008215	Statutory Appeal Dublin Circuit Court	25 April 2022
Outcome				**Current Status**
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 NGI of CCTV equipment in the National Gallery was justifiable by reference 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. Costs were also awarded to the DPC.				Mr Fox has lodged a further appeal (on a point of law) in the High Court.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
5.	2019/03674	Aimee Scott v Data Protection Commissioner	Statutory Appeal Dublin Circuit Court	Judgment: 4 May 2022 Costs Order 18 May 2022
Outcome				**Current Status**
Ms Scott submitted a complaint to the DPC, alleging that her employer had failed to comply with an access request, contending that the employer was not entitled to rely on assertions of legal professional privilege to withhold personal data from release in response to Ms Scott's access request. By decision dated 20 May 2019, the DPC concluded that the employer was entitled to rely on the privilege it had asserted. Ms Scott appealed to the Circuit Court against that decision. By written judgment delivered on 4 May 2022, the Circuit Court refused the appeal, accepting the DPC's position that the employer had made out its case in relation to its asserted entitlement to rely on privilege to withhold from releasing personal data that would otherwise need to be released in response to Ms Scott's access request. No order as to costs was made.				Ms Scott has lodged an appeal (on a point of law) with the High Court.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
6.	2020/123	The Data Protection Commissioner v Cormac Doolin and Our Lady's Hospice and Care Services (Notice Party)	Statutory Appeal Court of Appeal	Judgment: 24 May 2022
Outcome				**Current Status**
By written judgment of 24 May 2022, the Court of Appeal dismissed an appeal by the DPC against an earlier Judgment and Order of the High Court. The proceedings have their origin in a complaint made to the DPC by Mr Doolin concerning the alleged misuse by his employer of personal data collected by a security camera on his employer's premises in the context of its subsequent deployment in a disciplinary action. The DPC did not uphold Mr Doolin's complaint, finding that the data in question had not been processed in a manner incompatible with the purpose for which it had been collected. Mr Doolin appealed the DPC's decision to the Circuit Court. The Circuit Court upheld the decision. Mr. Doolin then brought a further appeal to the High Court on a point of law. That appeal was successful. The High Court disagreed with the DPC's analysis, finding (in effect) that Mr Doolin's data had been processed by his employer for a purpose other than the purpose for which it had first been collected, and where the second purpose was incompatible with the first. On further appeal, the Court of Appeal agreed with the High Court's analysis, dismissing the DPC's appeal and awarding costs to Mr Doolin.				The proceedings have concluded.



No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
7.	2021/04468	Aimee Scott v Data Protection Commissioner	Statutory Appeal Dublin Circuit Court	17 November 2022 Costs not yet dealt with
Outcome				Current Status
Ms Scott made a complaint to the DPC, alleging that a barrister had unlawfully processed her personal data in the context of an exercise to check for potential conflicts of interest before accepting instructions to act in a case for Ms Scott's former employer. The DPC delivered a decision in response to the complaint on 2 September 2022. In its decision, the DPC found that, on the facts, the GDPR did not apply at all, on the grounds that Ms Scott's personal data had been the subject of a verbal disclosure only. Without prejudice to that point, the DPC went on to find that, even if the GDPR did apply, the complaint could not be upheld because Ms Scott's personal data was processed, lawfully, by reference to the legitimate interests identified as being engaged in the case. By written Judgment delivered on 17 November 2022, the Circuit Court dismissed an appeal brought by Ms Scott against the DPC's decision.				Ms Scott has lodged an appeal with the High Court.

Commissioner Helen Dixon (DPC) and Deputy Commissioner Graham Doyle (DPC) engage with all EU Ambassadors to Ireland hosted by the French Ambassador to Ireland H. E. Vincent Guerend.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
8.	[2022] IEHC 532 [2020 No. 707 J.R.] [2020 No. 146 COM]	Maximilian Schrems v Data Protection Commission (Notice Party – Facebook Ireland Limited)	High Court (Commercial)	29 September 2022
Outcome				Current Status
On 16 July 2020, the Court of Justice of the European Union delivered judgment in Case C-311/18, DPC v. Facebook Ireland Ltd and Maximilian Schrems, making a number of findings in connection with the adequacy of the protections available in the US for European citizens where their data is transferred from the EU to the US. The judgment also ruled that the Privacy Shield mechanism under which some EU-US transfers were being undertaken did not comply with EU law and so should be struck down. Thereafter, the DPC opened an inquiry to consider the lawfulness of EU-US data transfers from Facebook Ireland Limited to its US-based processor, Facebook Inc., delivering a Preliminary Draft Decision on 28 August 2020 Facebook Ireland Limited responded to the Preliminary Draft Decision by bringing judicial review proceedings, challenging the DPC's decision to open the inquiry and taking issue with the procedures adopted by the DPC in that connection. As well as joining in Facebook's proceedings, Max Schrems separately brought his own judicial review proceedings likewise challenging the DPC's inquiry into Facebook's EU-US transfers. In a judgment delivered by the High Court on 14 May 2021, the High Court dismissed Facebook's objections to the DPC's inquiry. Thereafter, certain orders were made on consent on 20 May 2021, including an order that FBI pay 90% of the DPC's Commission's costs of the Facebook proceedings and all of Mr. Schrems' costs of those proceedings. The (separate) proceedings brought by Mr. Schrems, had earlier been settled on terms agreed between the parties. Exceptionally, the parties were unable to reach agreement on the costs of the proceedings. In a follow-on judgment delivered by the High Court on 29 September 2022, the Court decided that the DPC should pay 80% of Mr. Schrems' costs of his proceedings. The Court deducted 20% of the costs to reflect the fact that Mr. Schrems did not ultimately pursue his claim for an order quashing the DPC's inquiry or for certain of the other (ancillary) reliefs referred to in his case.				The proceedings have concluded.

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order
9.	Appeal No. 2022/47	Gerardine Scanlan v Paul Gilligan, Maurice Collins, Joe Jeffers, Shane O'Brien, Fiona O'Beirne, Grant Thornton Corporate Finance Limited, Aidan Connaughton, Ireland, the Attorney General, The Data Protection Commissioner	Court of Appeal	25 November 2022
Outcome				Current Status
By written judgment of 21 December 2021, the High Court struck out proceedings brought by Ms Scanlan against multiple parties on grounds that the proceedings constituted an abuse of process; the Court also granted an Isaac Wunder Order, prohibiting the issuing of further proceedings by Ms Scanlan against certain defendants unless Ms Scanlan first obtains the permission of the Court. Ms Scanlan brought an appeal to the Court of Appeal against the judgment of the High Court. By judgment of 25 November 2022, the Court of Appeal upheld the earlier High Court judgment. The Court of Appeal specifically found that the High Court trial Judge was entitled to find that the plaintiff's claims against the DPC were bound to fail and, as such, constitute an abuse of the Court's process.				The proceedings have concluded.

Supervision

Supervision

Engagement with public and private sector organisations, policy makers and legislators enables the DPC to understand the ways in which personal data are being processed by data controllers and processors, and enables the DPC to proactively identify, at a high level, data protection concerns and, in the case of new products or services to ensure that organisations are aware of their compliance obligations and potential problems in advance of the commencement of the processing of personal data.

The aim of supervision engagement is to offer guidance to stakeholders and to connect proactively as a regulator with a visible presence, ensuring the data protection rights of service users are upheld. In this context, the DPC promotes and aims to maintain open and regular communication with such stakeholders which includes organisations. In this way, the DPC advocates for the rights of individuals by mitigating against potential infringements before they occur. The Supervision function also facilitates prompt reaction by the DPC, where appropriate, to data protection concerns as they emerge.

The supervision function is an important part of the regulatory framework, as ensuring best practice is applied at project planning stages results in better outcomes for data subjects and less need for resource-intensive ex-post activity for the DPC. However, 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

The DPC received **322 consultation requests** during 2022. The sectoral breakdown is as follows:

Sector	#	%
Private Sector	131	41%
Public Sector	135	42%
Multinational Tech Sector	7	2%
Health Sector	34	11%
Voluntary/Charity Sector	7	2%
Law Enforcement Sector	8	2
Total	**322**	

Legislative Consultation

The DPC provided guidance and observations on **30** proposed legislative measures in 2022. 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 2022, some of the legislative measures that the DPC engaged in consultation on were:

- Civil Law (Misc. Provisions) Bill 2022, known as the Ukrainian crisis omnibus Bill
- Courts and Civil Law (Miscellaneous Provisions) Bill 2022
- Communications (Retention of Data)(Amendment) Act 2022
- The Gambling Regulation Bill 2022
- Garda Siochána (Digital Recording) Bill
- Regulation of Lobbying (Amendment) Bill 2022
- Local Government (Surveillance Powers in Relation to Certain Offences) Bill 2021
- Criminal Justice (Sexual Offences and Human Trafficking) Bill 2022
- The Construction Safety Licensing Bill 2022
- Communications (Retention of Data)(Amendment) Bill 2022
- Department of Health - Human Tissue (Transplantation, Post-Mortem, Anatomical Examination, and Public Display) Bill 2022
- Mother and Baby Institutions Payment Schemes Bill 2022
- Health (Termination of Pregnancy Services (Safe Access Zones)) Bill 2022.
- European Union (Money Laundering and Terrorist Financing: Use of Financial Information) Regulations 2022
- Part 22B (Vacant Homes Tax) in the Taxes Consolidation Act 1997 (TCA)
- Temporary Business Energy Support Scheme (TBESS)
- Rent Tax Credit
- Electricity Costs (Domestic Electricity Accounts) Emergency Measures Act 2022
- Disabled drivers and disabled passengers fuel grant scheme regulations (2021/22)
- Loan Guarantee Schemes Agreements (SBCI) Act 2021

The DPC also contributed the Oireachtas Joint Committee on Justice as part of the discussion on the **General Scheme of the Communications (Retention of Data) (Amendment) Bill 2022**.

Throughout 2022, the DPC continued its engagement with DPOs, stakeholders, government departments, state agencies and advocacy groups across all sectors on a wide range of issues including:

Public Sector, Health and Voluntary

Online Publication of Planning Data

During 2022, the DPC engaged in multi-stakeholder engagement to resolve issues arising from the online publication of personal data provided to local authorities in the course of the planning process.

The DPC recognises that transparency is fundamental to the integrity of the planning process, and maintaining the trust and confidence of the public in the work of the planning authorities. However, the requirement to publish information relating to planning applications must be balanced with the legitimate privacy concerns and data protection rights of individuals. Particular concerns can arise, for example, where applicants submit special category personal data relating to family members, who may be children or vulnerable adults, in support of their planning application. Planning applicants, and those making submissions in relation to applications, can also occasionally provide information relating to third parties, without their knowledge.

The DPC engaged with the Local Authorities Data Protection Officer Network, the Local Government Management Agency, and the Department of Housing, Local Government and Heritage and a set of principles was collectively developed for policies to be implemented to ensure that an appropriate balance is struck in the online publication of planning material between the transparency requirements of the planning process and the data protection rights of individuals. These policies will ensure that excessive or irrelevant data is not inappropriately published, in particular information about people's health or children' data.

There will also be opportunity for applicants to request that their data be reviewed subsequent to publication, taking into consideration their own circumstances. In the interests of transparency in the planning process, it will always be necessary for certain elements of personal data to be made available to the public, and it is important that this is explained in a clear and understandable way to planning applicants.

As the planning process moves towards a national ePlanning model, the DPC will continue to engage with stakeholders to ensure that data protection implications are considered appropriately.

Housing Agency Collaboration on Owners' Management Companies guidance

In 2022, the DPC published detailed guidance on the Data Protection Considerations Relating to Multi-Unit Developments and Owners' Management Companies (OMCs), following extensive collaborative engagement with the Housing Agency.

For some time, both the DPC and the Housing Agency had identified the OMC sector as a regular source of data protection queries relating to a number of issues. Examples of this include access to and use of data held on the register of company members, personal data of tenants, and the deployment of CCTV in common areas. Involvement with OMCs is an ever-increasing part of the Irish housing landscape, and the sector's activities entail significant data processing between residents (owner-occupiers and tenants), landlords, and property management agents.

The development of this guidance document represented a positive engagement between the DPC and another statutory body (The Housing Agency), combining specific sectoral knowledge with the application of the principles of data protection to bring forward a solution to an identified problem area. In line with the DPC's commitments under its Regulatory Strategy 2022-2027 to promote data protection awareness, and to support organisations and drive compliance, the DPC will continue to look for opportunities to work with other statutory bodies and sectoral representative groups to develop targeted and relevant guidance.

Adult Safeguarding and Data Protection

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, in 2022, the DPC commenced a process of stakeholder engagement to discuss data protection concerns arising in the context of adult safeguarding. The first strand of these discussions addressed, in particular, the processing of sensitive personal data and information relating to those living in adult residential care settings. Concerns that can arise in this context, and that may result in safeguarding actions which require the processing of personal data, can include allegations of inappropriate or potentially illegal behaviour onsite, and suspicions of financial abuse or coercive control of residents by third parties. Questions can also arise in these contexts regarding the sharing of information with family members of residents.

The aim of the DPC's engagement with stakeholders in this sector is to assist in providing clarity and certainty to adult safeguarding organisations regarding their data protection obligations, in particular when dealing with sensitive situations. The DPC has already issued some guidance to the stakeholders on processing particularly sensitive information arsing in certain situations, including handling requests for information from concerned family members.

The DPC's overall aim is to foster a consistent approach to data protection across the wider sector, to promote equality, prevent discrimination and ensure that the data protection rights of vulnerable groups are given appropriate consideration. This consultative engagement process will continue in 2023, looking at additional solutions to identified sectoral issues including, for example, published guidance, and the possibility for the development of codes of conduct.

Public Sector, Law Enforcement and Social Protection

Local Authority CCTV scheme

In early 2022, the Data Protection Commission received a Data Protection Impact Assessment (DPIA) from a local authority seeking to implement an expansive city-based community CCTV scheme. The cameras were technologically sophisticated and had Pan Tilt, Zoom and other 'smart' capabilities. It was the intention of the local authority to effectively use these cameras for 24/7 surveillance of certain high-crime areas.

The proposed locations for the cameras were primarily open public spaces. However a number of these cameras were to be in positions where they could capture images from the upstairs windows of private dwellings.

The DPC raised a number of concerns about this planned data processing, in particular about the justification for 24/7 surveillance and the intrusiveness of some of the cameras 'smart' capabilities. The DPC emphasised the necessity for robust security measures, the need to respect the privacy rights of residents and the responsibility on the local authority, as a data controller, to protect the public and mitigate the risks this processing could have for children and vulnerable members of society.

In response to these concerns, the local authority decided to disable the auto-scan and roaming capabilities of all cameras and also chose to turn off a number of the cameras, following a further necessity analysis. In response to the DPC's concerns about protecting individual privacy rights and the need to safeguard the vulnerable, the local authority implemented further security measures, including regular staff training, strict access controls, shortened retention periods, strict procedures to view and download camera footage, the implementation of an oversight board, and other measures. The local authority also revised its plans for 24/7 monitoring by default to

only commencing monitoring at the direct request of An Garda Síochána.

Charitable Preschool

The balancing of the data protection rights of children against the interests of their parents is an area data controllers and processors must navigate as part of their daily functions. In 2022, the Information Officer of a charitable preschool contacted the Data Protection Commission (DPC) following an estranged parent's request for access to all of their child's records held at the preschool.

The preschool had concerns for the welfare of both the custodial parent and child should they provide all the information, and were seeking to clarify whether the preschool could refuse the information request.

The DPC informed the preschool that as the data controller, they have an obligation to ensure that the right of access does not adversely affect the rights and freedoms of others under Article 15(4) GDPR. This includes the rights of the child and the other parent. Data controllers may restrict a parent's right of access to their child's data where they have reasonable grounds to believe this would not be in the best interests of the child.

This is not to say that an access request should be dismissed entirely. The DPC informed the preschool that they should provide a response to the request. However, the preschool may redact certain information where they deem it necessary to safeguard the rights and freedoms of the child or custodial parent.

Following these initial recommendations, the charitable preschool informed the DPC that exemptions and redactions, as necessary and proportionate in light of the circumstances, were applied to the relevant records before they were released.

Technology Multinationals

TikTok Legitimate Interest Assessment

In June 2022, TikTok publicly announced that several changes were being made to the TikTok Privacy Policy. One change of note was that the lawful basis being relied on for first party personalised advertising for users aged 18 and over would change from consent to legitimate interest. Following an intervention by the DPC, TikTok agreed to pause the change in lawful basis to allow for further assessment by the DPC and other EU/EEA supervisory authorities of the justification for relying on the legitimate interests lawful basis for the processing concerned.

The DPC subsequently raised a number concerns with the company, in particular that, in the view of the DPC and other supervisory authorities, TikTok had not yet sufficiently demonstrated that it could rely on legitimate interests. Further information and clarity on a number points was sought and engagement with TikTok on this matter is ongoing.

Chrome Privacy Sandbox engagement and co-operation with the other Supervisory Authorities

During 2022 the DPC, as Lead Supervisory Authority, co-ordinated and facilitated several meetings between Google and members of the European Data Protection Board (EDPB). These meetings allowed Google to update supervisory authorities on the continuing development of the Google Privacy Sandbox as well as providing the DPC and other supervisory authorities the opportunity to probe Google's plans and to raise questions and/or concerns. Engagement with Google on the Privacy Sandbox will continue in 2023.

Google Workspace recommendations

The DPC undertook a high-level review of 'Workspace' Google Cloud Privacy Notice during 2022. Workspace Google Cloud Privacy Notice covers the processing of personal data in relation to a collection of Google's cloud computing, productivity and collaboration tools, software and products. Several recommendations were made to Google to improve contextual transparency including in relation to the definition of terms used and retention periods as well as other transparency requirements pursuant to GDPR Articles 12, 13 and 14. In response, Google has sought to provide more granular detail on retention periods for service data, with indicative examples to provide additional meaning and context. Google has also published an updated version of the Google Cloud Privacy Notice.

Apple Maps

Engagement with Apple on the collection of data for Apple Maps continued into 2022. Following a review of Apple's collection processes and in particular the retention of unblurred images captured to support the "Look Around" feature", the DPC queried why raw data was being retained for 18 months from date of publication of the updated street views. In response Apple confirmed that the retention period would be reduced to 12 months. The Apple Maps Image collection website and policies for all EU/EEA countries were subsequently updated to reflect the 12-month retention period.

Meta Emotional Health Hub

The DPC concluded in 2022 engagement with Meta on the Emotional Health Hub. The Hub is a website with a collection of resources on various mental health topics, primarily provided by third parties (NGOs, World Health Organisation, charities, etc.). Facebook users and non-users can access these resources, follow links to third party sites, and use the Hub to message a Facebook contact to talk about the issues they are facing.

Meta collects various information including the time spent by a user on the Hub, the time spent on each resource within the Hub, the number of clicks on each resource, what resources a user clicks on, the location of the user, and data regarding the title of the resource being clicked.

Having identified a number of transparency related concerns, the DPC made a number of recommendations to Meta to improve transparency to users particularly concerning processing purposes.

Meta subsequently implemented a number of updates to the Hub. These included updates to placing the in-context Help Centre article in a more prominent and easily accessible position within the Hub. Additionally, for ease of access to users and non-users, a link to Meta's Data Policy and the purposes of processing are now provided through the Help Centre article.

Combatting Child Sexual Abuse Material

During the year the DPC engaged with several providers of interpersonal communications services such as Meta, LinkedIn, Microsoft, Google and Twitter, to review their policies, procedures and technologies relating to the processing of personal data for the purpose of combating online child sexual abuse material.

The DPC has made a number of recommendations to providers in areas such as Transparency, Retention and Purpose Limitation. In response, Meta, for example, has notified the DPC that they will be updating User Notices to enhance transparency including in relation to the appeals mechanism. Engagement with the large platform providers will continue into 2023.

Private and Financial Sector

Migration of customer data from KBC Bank to Bank of Ireland

The DPC proactively engaged with both KBC Bank and Bank of Ireland for the migration of most of the KBC customer database of mortgage holders and persons who had credit facilities, (i.e. credit cards, loans, deposits) to Bank of Ireland. This porting of customer data is due to KBC's pending exit from the Irish market. During its interaction with both banks, the DPC provided guidance on many issues including security of transfer, accuracy of data, providing full information to all customers and ensuring that the customers' data protection rights were not adversely affected.

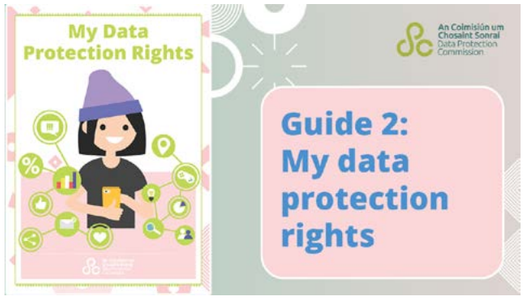
Children's Data Protection Rights

Guidance for Children on their Data Protection Rights

In May 2022, the DPC published three short guides for children aged 13 and over on their data protection rights. These guides are intended mainly for children aged 13 and over, as this is the age at which children can begin signing up for many forms of social media on their own.

The protection of children's personal data is an important priority for the DPC, and is one of the five strategic goals of its 2022-2027 Regulatory Strategy. In furtherance of this objective, the DPC published the final version of its comprehensive 'Fundamentals' guidance on children's data protection rights at the end of 2021. The purpose of the Fundamentals is to help organisations provide the special protection children merit when processing their personal data. However, an equally important element of protecting children's personal data is giving children themselves the awareness and tools that they need to be safe online. With this in mind, the DPC has published the following short guides:

"My data protection rights**"** This guide is a series of one-page primers which each introduce children to a separate GDPR right and how to use it.



"Top tips for keeping your data safe online**"** This guide has 15 useful tips to help children - and indeed everyone - keep their personal data safe when they go online.

"Data protection - what's it all about?**"** This guide introduces children and young people to the idea of personal data and data protection, and why it's important for them to know about it.

The DPC hopes that these guides will not only help children keep their data safe, but will also be useful for parents, educators and anyone interested in children's safety and wellbeing online.

Targeting Children with social media advertising

In September 2022, the DPC received a query from a public sector organisation about whether they could use social media advertising tools to target children with ads about beneficial initiatives and services that they offer for children. The organisation noted that the age of digital consent in Ireland is 16 and surmised that parental consent would be required for children under this age. The organisation asked whether their understanding was correct and whether social media ads for children under 16 should be directed at parents.

The DPC advised that the public body was likely to be a joint controller – together with the social media platform – for any processing of personal data for targeted advertising. Therefore, the public body would share responsibility for ensuring that the processing was compliant with data protection law. In practice, this would mean preparing the necessary compliance documentation in consultation with their Data Protection Officer, to set out the justification and legal basis for this processing and to identify and mitigate any potential risks to children.

The DPC also advised that, in the context of preparing their DPIA, the organisation should consider whether consent would be the most appropriate legal basis for this processing, as it would in practice be difficult for children or parents to give meaningful and distinct consent to targeted advertising in circumstances where they must accept it as a condition for using the service in the first place. The DPC advised that alternate legal bases under Article 6 of the GDPR may be more appropriate, but it was for the public body itself to determine this, taking into account its context, statutory remit, objectives and obligations under the law.

The advice that the DPC gave in this case is relevant to any public sector organisation that is considering whether to use social media to target children. Such organisations should in particular bear in mind the following considerations. First, the DPC cannot give blanket endorsements of social media advertising tools and it is therefore up to the organisation itself to determine on a case-by-case basis whether it can use such tools in a proportionate and privacy-preserving manner for a purpose that reflects the best interests in the child. An organisation that wants to use social media advertising to pursue its objectives cannot assume that the associated data protection compliance is the sole responsibility of the social media company itself. Second, there is a lot of confusion around the appropriateness of consent as a lawful basis and in particular the role of the age of digital consent. Public sector organisations in particular should consider whether alternate legal bases are more appropriate, taking into account their particular duties and obligations in relation to children and any other relevant contextual factors.

euConsent Project

In 2022, the DPC participated on the advisory board of the euCONSENT project, an EU-funded initiative to create a framework for age verification (AV) and parental consent tools and solutions to increase the protection of children online by making AV and parental consent tools more effective.

Data Protection Officers

The DPC emphasises open engagement with data controllers when seeking to drive compliance with the GDPR. In this way, and where appropriate, the DPC can support organisations in providing the individuals they interact with the full protections and considerations of the GDPR. However, where a data controller fails to engage with the DPC and/or comply with their obligations, the DPC will consider utilising its enforcement powers in order to ensure compliance.

The DPC continued its programme of engagement with data controllers on compliance with the requirements of Article 37 of the GDPR concerning the designation and notification of a Data Protection Officer (DPO). At the end of 2021 all but one public sector body had been brought in to compliance with Article 37 of the GDPR. The remaining public sector body, the Pre-Hospital Emergency Care Council (PHECC), failed to respond to repeated efforts from the DPC querying the organisation's designation of a DPO.

The DPO wrote to the PHECC five times, via various mediums, without response, before opening an Inquiry in February 2022 in accordance with section 110(1) of the Data Protection Act 2018.

The Inquiry was commenced to establish whether the PHECC was required to designate a DPO pursuant to Article 37(1) of the GDPR and whether the PHECC had done so. In addition, the Inquiry sought to establish whether the PHECC infringed Article 37(7) of the GDPR concerning publication of the DPO contact details and communication of those contact details to the DPC. The Inquiry also examined whether the PHECC infringed Article 31 of the GDPR by failing to cooperate, on request, with the DPC in the performance with its tasks.

The DPC's Decision in the Inquiry finalised in May 2022 accepted that the failure to cooperate with the DPC was without intent, but noted that it cannot be the case that a public authority or body (or any data controller), can fail to answer, in any way, repeated efforts to monitor and enforce the GDPR. The PHECC was issued with a reprimand in respect of infringements of Articles 31, 37(1) and 37(7) of the GDPR. A further update on this inquiry can be found in the inquiries chapter on page 21.

DPO Network

The DPC remains committed to supporting DPOs and their teams. In 2022, the DPC hosted 32 online webinars for members of the DPO Network, covering topics ranging from responding to access requests to compiling records of processing activities. Additionally, DPC staff continued to take part in events organised by sectoral DPO Networks, from both the public and private sector. The DPC also hosted a conference in May – as part of the EU ARC Project – which drew many members of the DPO Network to the event. A more detailed report of the conference event can be found on page 50

Kate Colleary, Graham Doyle, Steven Roberts, Rob van Eijk - ARC Conference

International Activities

European Data Protection Supervisory Bodies

During 2022, the DPC continued to participate in the work programmes of the European supervisory bodies.

EU Cooperation

Despite ongoing travel restrictions preventing in-person meetings of the European Data Protection Board (EDPB) in 2022, the DPC continued to attend and actively participate at all virtual monthly plenary meetings, as well as expert subgroup meetings (over 300 in total).

Schengen Information System

The Schengen Information System (SIS) compensates for the removal of internal border controls between Schengen countries in Europe. It is a tool for border, immigration, police, customs and judicial authorities in the EU and the Schengen associated countries to share information on people and objects in one common database. Ireland is part of the SIS system.

As part of the DPC's ongoing international work,in 2022, staff from the DPC acted as Member State Lead Expert in three separate evaluations of the application of SIS II in Sweden, Denmark and Iceland.

The respective teams were led by staff of the European Commission and included experts from other Member States.

The on-site teams visited multiple locations in the preparation of their reports, including:

- Swedish Authority for Privacy Protection;
- Swedish Police Headquarters;
- Swedish Migration Agency;
- Border Control Police at Arlanda Airport;
- Icelandic Data Protection Authority;
- Icelandic National Police Commissioner´s office;
- Directorate of Immigration´s office, Kópavogur;
- Reykjavík Metropolitan Police Station;
- Datatilsynet - Danish DPA;
- Danish Immigration Service;
- Danish National Police; and
- Copenhagen Airport.

The three evaluation groups each produced reports on the manner in which Sweden, Denmark and Iceland implement and apply the European Union's Schengen acquis against the background of data protection requirements, including areas where the on-site team considers there is need for improvement, as well as best practices observed during the on-site visit.

Cooperation with other EDPB supervisory authorities 2022

The DPC continued to invest considerable resources in the day-to-day operation of the OSS 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 SAs of updates on supervision cases and inquiries and sharing of documents.

Formal Mutual Assistance requests are used to formally request information from another SA or to request that an SA take certain actions

International Transfers - Binding Corporate Rules (BCRs)

A key focus in the area of international transfers for the Data Protection Commission is the assessment and approval of Binding Corporate Rules (BCRs) applications from multi-national companies.

BCRs 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.

During 2022, the DPC continued to act or commenced acting as lead reviewer in relation to **27** BCRs applications from **16** different companies. **Three** of those applications were given approval in 2022 – Controller BCRs for Groupon International Limited and Controller and Processor BCRs for Ellucian Ireland Limited.

The DPC also assisted other European Data Protection Agencies by acting as co-reviewer or on drafting teams for Article 64 Opinions on **6** BCRs in this period.

Furthermore, once the BCRs are approved, the DPC continues to have a significant oversight role upon receiving annual updates on all BCR's. In 2022 the DPC led on **23** BCRs for **16** different companies which are already approved.

The EDPB issued Article 64 opinions on 23 BCRs applications in 2022 and the DPC checked and offered feedback on each of these applications.

BCR Training Workshop, Dubrovnik

In May 2022 a Training Workshop on BCRs was held in Dubrovnik, Croatia where staff from the DPC delivered a session on progressing a BCRs application from start to finish which was well received by attendees from all EEA supervisory authorities.

Siniša Kovačić (AZOP), Deputy Commissioner Igor Vulje (AZOP), MB Donnelly (DPC), Commissioner Helen Dixon (DPC), Ashwinee Kumar (VUB) - ARC Conference

Spring Conference of Data Protection Commissioners

In May 2022 the DPC participated in the Spring Conference of Data Protection Commissioners in Cavtat, Croatia. This was the first time the conference had been held since 2019 was attended by all EU data protection authorities, as well as representatives from the EU Commission and from the legal and academic spheres. The 2022 event was an in-person event, hosted by the Croatian Data Protection Authority over the course of three days. The DPC took part in the expert panel discussions and presented the initial findings of the ARC project to attendees.

ARC Project

In 2022 the DPC's successful participation in the EU-funded ARC project came to an end. The ARC Project had its inception in 2019, when the Croatian Data Protection Authority, AZOP, submitted a proposal to the EU Commission seeking funding for a project that would focus on supporting the compliance efforts of small-to-medium enterprises; specifically because the often limited resources of SMEs presented an additional challenge when complying with data protection legislation.

Funding was awarded on the basis of a consortium approach, and AZOP approached the DPC and Vrije University, Brussels with an invitation to join them in their efforts to support SMEs. The DPC recognised this as an excellent opportunity for international cooperation and for providing support to one of its own key stakeholder groups. Having taken the decision to join the consortium, the project was formally launched in February 2020, will a full programme planned of national and international engagements and workshops.

Within a month, the entire landscape of events for which the project had been designed had been significantly altered. The ARC Project needed to be radically reconceived in order to meet the needs of a cohort that was changing by the hour.

The ARC team followed the path set out by the needs of the SME cohort and it too transitioned to an online environment. Where in-person workshops and events had been planned, these were replaced with online substitutes to ensure that learning and engagement continued. Online engagement had the advantage of allowing attendees to join who might otherwise have been prevented by distance from joining an in-person event, however the drawback was that it didn't allow attendees to engage with each other. The project team persevered nonetheless, and in all the ARC project delivered over 100 workshops for both Irish and Croatian SMEs between 2020 and 2022.

In its formal evaluation of the project, the EU Commission noted that the ARC had been:

".. assessed as very good and no shortcomings were identified. The content of the deliverables is satisfactory and of high quality, despite the circumstances caused by the pandemic.

The project can have long-term impact on the project groups and the society, as well as on EU Legislation and/or policies and can serve as a pool of knowledge for other Data Protection Authorities as well."

The ARC Project drew to a close in 2022, with a very well attended conference for DPOs - and others in the data protection space - which was held in Croke Park in May. In a happy turn of events, the DPC was finally in a position to host an in-person conference, and was delighted to welcome representatives from our consortium partners in AZOP and Vrije University.

Commissioner Helen Dixon - Keynote, ARC Conference

DPC Conference for SMEs

Background to the Conference

On May 11th, 2022, the DPC hosted a large-scale in-person conference for SMEs in Croke Park, Dublin, as part of its commitments to the EU-funded ARC project. The structure of the day was based on the findings of a survey of the SME sector (an earlier deliverable of the ARC Project), which had identified **Legal Bases, Accountability, and Data Breach mitigations** as areas of particular difficulty for Irish SMEs.

Conference Goals

The goal of the conference was to give SMEs access to the type of expert legal and regulatory advice that they may not be in the position to acquire for themselves, for financial or other reasons. Accordingly, panellists from the DPC were joined on the day by some of the top data protection and legal specialists currently operating both in Ireland and internationally.

A secondary goal of the conference was to create an environment where SMEs could engage in the peer-to-peer networking that had been denied them for the previous two years, due to the Covid restrictions in place in Ireland. The DPC wanted to work towards mitigating the sense of isolation that many SMEs and DPOs have acknowledged when it comes to dealing with compliance challenges. It was important to the DPC and its stakeholders that the conference be an in-person event, to facilitate the softer networking and relationship building that helps build a culture of compliance among regulated entities.

Adding value – planning the content

The driving principles of the conference were **practicality** and **applicability**. This included a strong emphasis on workshop style presentations that essentially "walked" attendees through the steps necessary to meet the threshold of accountability for their respective businesses. Q&A sessions were also built into each panel, allowing the audience to ask for clarifications on specific points.

Serving SMEs – the contents of the conference

In preparation for the conference, the DPC had liaised with the various SME representative bodies in Ireland to ensure we reached our target audience of small and medium enterprises. 340 delegates attended the event and the panel sessions on the day were extremely well received, with many compliments from the audience for the quality of the panel participants and a strong desire for future, similar events which is something that the DPC will actively pursue in 2023 and beyond.

Communications

Media Engagement

The DPC published a total of 15 press releases over the course of 2022, leading to significant coverage on international and national level media. Specific announcements included the publication of a **Statistical Report** on the DPC's handling of cross-border complaints under the GDPR's One-Stop-Shop (OSS) mechanism, the conclusion to an inquiry into Meta Platforms Ireland Limited (Instagram) imposing a fine of €405 million and a range of corrective measures, and the confirmation of administrative fines imposed on six different organisations - ranging between €1,500 and €17 million.

Direct Engagement

Despite the ongoing restrictions in place, direct engagement with stakeholders remained a high priority throughout 2022. The DPC continued to engage with a variety of both Irish and international stakeholders. The Commissioner and members of staff contributed to **over 80 events** in 2022.

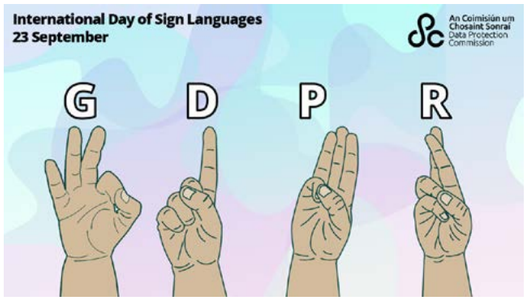
Guidance and Educational Material

The DPC remains committed to driving awareness of data protection rights and responsibilities. In 2022, the DPC:

- Produced 7 pieces of substantial new guidance (including three specifically tailored towards children), 5 infographics, and over 15 new case studies for its website throughout the course of the year;
- Updated 11 pieces of existing guidance to ensure they reflect the most up-to-date developments in data protection law; and
- Published three reports, including the comprehensive One-Stop-Shop Cross-Border Statistics report.

Social media

The DPC's social media platforms continued to play an important role in the communications of the DPC in 2022. The growth of the DPCs social media presence across Twitter and LinkedIn, was integral to the support of its awareness-raising and communications activities. The combined followers across both platforms has **increased by over 7,500 during 2022, to over 42,000.** There was an organic reach of over **1.4 million**, with strong engagement across the board. The DPC's Social Media Policy can be viewed on our website.



DPC Website

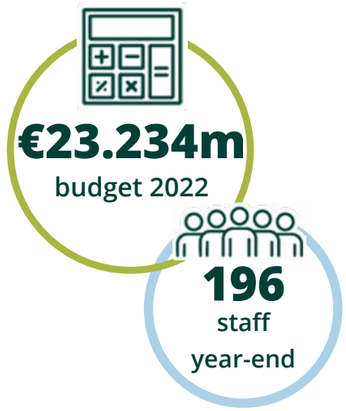
The DPC website (www.dataprotection.ie) continues to be an important resource for individuals and organisations throughout 2022. The DPC's webforms provide website users with a convenient means of submitting complaints, breach notifications, and general queries directly to the DPC. In addition, press releases, statements, and guidance on topical issues of relevance to our stakeholders were published frequently throughout 2022.

Corporate Affairs

DPC Funding and Staffing

The 2022 gross estimate provision for Vote 44 — Data Protection Commission was **€23.234M** (2021: €19.128M) of which €15,970M (2021: €12.764M) was allocated for pay-related expenditure, and €7.264M (2021: €6.364M) of which was allocated to non-pay expenditure. The funding for 2022 represented **an increase of €4.106M** on the 2021 allocation.

The number of DPC staff at year-end 2022 was 196. The DPC will continue to drive recruitment during 2023 through a combination of open recruitment and the promotion and development of DPC staff.



Work continued on the DPC's Learning & Development strategy in 2022. An Employee Engagement Forum was established following the transfer of staff to the DPC as an independent body in 2021. The Forum has a diverse and inclusive membership, with representation at each grade an essential requirement. Its purpose is to contribute to the DPC's commitment to becoming an Employer of Choice through enhancing the employee experience for staff. Employee experience is about creating a great work environment for people and involves understanding the role that trust plays in the employment relationship and making sure people are listened to and have a voice in issues that impact them.

In support of this, the Employee Engagement Forum focused on Trust and Culture throughout the year, and identified these as underlying themes in the development of the DPC's Employee Engagement Strategy, which is due to be finalised in 2023.

Having identified "retaining and amalgamating the expert capacities of its staff to ensure operational effectiveness" as a strategic priority and a key driver of successful organisational change, the DPC's SMC leverages employee engagement to support the achievement of objectives in the DPC's Regulatory Strategy.

In 2022, the DPC continued to prioritise the professional development of all of our 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.

DPC staff attended 634 courses via OneLearning in 2022. Additionally, several courses were delivered in the DPC in 2022, these courses covered Data Protection Training, Leadership Development, Line Manager Training, De-escalation & conflict management as well as Interview Skills sessions throughout the year. In 2022, the DPC delivered the Winter Wellbeing programme which centred on topics around Mens/Womens Health, Stress, Mental Health, Money Skills for Life & Self-Care.

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 2022 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 first term of the Audit and Risk Committee concluded on 31 December 2022. When invited, all current serving members were pleased to continue in their roles for a second term, which will take effect from 01 January 2023 and run for three years.

The members of the Committee are:

- Conan McKenna (chairperson);
- Karen Kehily;
- Bride Rosney;
- Michael Horgan; and
- Graham Doyle.

Six meetings of the Audit and Risk Committee were held in 2022.

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.

Risk Management

The Risk Management Policy of the DPC outlines its approach to risk management and the roles and responsibilities of the SMC, as well as managers and staff. The policy also outlines the key aspects of the risk-management process, and how the DPC determines and records risks to the organisation. The DPC implements the procedures outlined in its risk-management policy and maintains a risk register in line with DPER guidelines. This includes carrying out an appropriate assessment of the DPC's principal risks, which involves describing the risk and associated measures or strategies to effectively control and mitigate these risks. The risk register is reviewed by members of the Senior Management Committee and Audit and Risk Committee on a regular basis.

Building organisational capacity to meet the enhanced functions of the organisation under the GDPR and national legislation continued to be a key priority for the DPC in 2022 and the challenges around meeting this objective were reviewed regularly as part of risk management.

Official Languages Act 2003

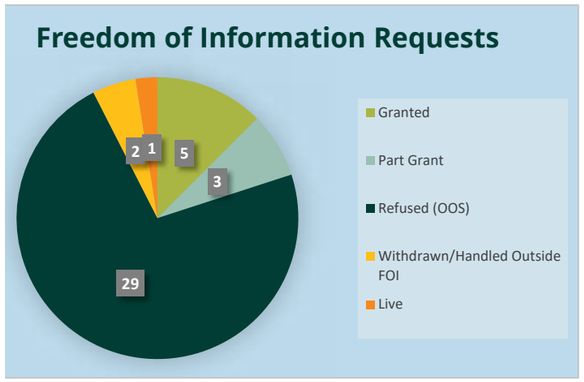
The DPC's fifth Language Scheme under the Official Languages Act 2003 commenced on 21 December 2020 and will remain in effect until 21 December 2023.

The DPC continues to provide, and improve Irish language services with enhancements of services, as per the Language Scheme held in regard.

Freedom of Information (FOI)

In 2022, the DPC received a total of 40 FOI requests.

Five were granted, three were partially granted and 29 were deemed out of scope. 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 Commissioner for Data Protection is a Designated Public Official (DPO) 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 (DPER) Circular 25 of 2016, the DPC provides a dedicated mailbox to address the queries of Oireachtas members and to receive feedback.

In 2022, the DPC further reinforced its engagement with Oireachtas members by appointing a Deputy Commissioner with responsibility for Government and NGO Relations. Engagement of this nature is vital to the integrated future of Ireland's Digital Economy, in anticipation of the increased volume of digital regulation that is imminently pending.

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 developed and implemented a number of ways to communicate with stakeholders in an accessible manner. 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.

During 2022, the DPC continued to review its service delivery and sought to ensure that it continued to be accessible to customers whilst DPC staff returned to the office on a blended basis. 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 website.

Customer Charter

The DPC's Customer Charter and accompanying Quality Customer Service Action Plan and Managing Unreasonable Behaviour and Contacts Policy for 2021 – 2023 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.

Commissioner Helen Dixon, European Union Commissioner Mairead McGuinness - Brussels

MB Donnelly (DPC) with former Minister for Justice Nora Owen - Guest Speaker at DPC All-Staff Communications Day October 2022

Commissioner Helen Dixon - IAPP Data Protection Congress 2022

Appendices

Appendix 1: Protected Disclosures

Report on Protected Disclosures received by the Data Protection Commission in 2022

The policy operated by the Data Protection Commission (DPC) under the terms of the Protected Disclosures Act 2014 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 requires public bodies to prepare and publish, by 30 June in each year, a report in relation to the previous year in an anonymised form.

Pursuant to this requirement, the DPC confirms that in 2022:

- No internal protected disclosures (from staff of the DPC) were received.
- 13 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). Five of the disclosures were accepted as valid protected disclosures.

Reference Number	Type	Date Received	Status	Outcome
01/2022	Section 7 (external, to 'prescribed person'	05 January 2022	Closed	Not accepted as a valid protected disclosure. Referred as a potential complaint.
02/2022	Section 7 (external, to 'prescribed person'	28 January 2022	Closed	Insufficient detail provided, complaint did not follow up when requested.
03/2022	Section 7 (external, to 'prescribed person'	22 March 2022	Closed	Insufficient detail provided, complaint did not follow up when requested.
04/2022	Section 7 (external, to 'prescribed person'	28 March 2022	Closed	Accepted and referred for potential investigation. Case concluded.
05/2022	Section 7 (external, to 'prescribed person'	05 April 2022	Open	Accepted and referred for potential investigation. Ongoing at year-end.
06/2022	Section 7 (external, to 'prescribed person'	23 May 2022	Closed	Insufficient detail provided, complaint did not follow up when requested.
07/2022	Section 7 (external, to 'prescribed person'	19 August 2022	Closed	Complaint withdrawn.
08/2022	Section 7 (external, to 'prescribed person'	25 October 2022	Closed	Not accepted as a valid protected disclosure, referred as a potential complaint.
09/2022	Section 7 (external, to 'prescribed person'	26 October 2022	Closed	Not accepted as a valid protected disclosure, referred as a potential complaint.
10/2022	Section 7 (external, to 'prescribed person'	27 October 2022	Open	Accepted and referred for potential investigation. Ongoing at year-end.
11/2022	Section 7 (external, to 'prescribed person'	08 November 2022	Open	Accepted and referred for potential investigation. Ongoing at year-end.
12/2022	Section 7 (external, to 'prescribed person'	15 November 2022	Open	Accepted and referred for potential investigation. Ongoing at year-end.
13/2022	Section 7 (external, to 'prescribed person'	08/12/2022	Under Consideration	Currently under consideration.

Annual Report 2022

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

Overview of Energy Usage

General

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

Over the last 12 months, the DPC has made a large reduction in its energy consumption across the offices.

Office	% reduction on last 12 months validated data	% Reduction in last 3 years validated data
Fitzwilliam Sq - Electricity	26%	80%
Satellite Office – Electricity	26%	48%
Portarlington - Electricity	12%	48%
Portarlington – Natural Gas	16%	32%

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 2021 (last validated SEAI figures available) is as follows:

	Electrical	Natural Gas
Dublin		
Fitzwilliam Sq.	18,820KwH	
Satellite Office	46,395KwH	
Portarlington	21,100KwH	33,335

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
- Sensor lighting in use in one office (Satellite)
- Introduction of Government Energy Conservation plans
- Sensor lighting introduced in Bathrooms Portarlington Office

Reduction of Waste Generated

- DPC uses a default printer setting to print documents double-sided.
- DPC has also introduced dual monitors for staff to reduce the need to print documents to review / compare against other documentation during case work.
- DPC provides General Waste and Recycling bins at stations throughout the offices.

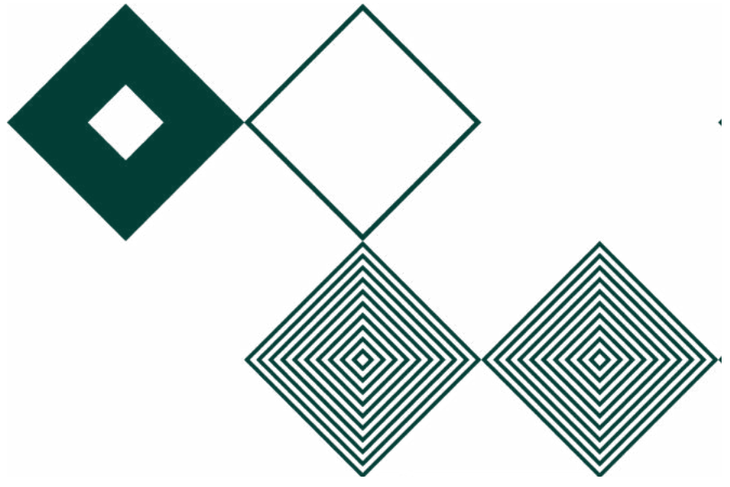
Maximisation of Recycling

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

Sustainable Procurement

DPC procurements and processes are fully compliant with Sustainable Procurement.

Catering contracts stipulate the exclusion of single use plastics**.**



Appendix 3: DPC Statement of Internal Controls

The Financial Statement of the Data Protection Commission for the year 1 January 2022 to 31 December 2022 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 2022 by the Comptroller and Auditor General.

Commissioner Helen Dixon, Founding Partner Browne Jacobson LLP Dublin Jeanne Kelly, Former Minister for Justice Nora Owen, James Lawless, TD – Chair of Oireachtas Committee on Justice - DPC All-Staff Communications Day October 2022

Commissioner Helen Dixon and Deputy Commissioner Graham Doyle meet with European Union Justice Commissioner Didier Reynders - Brussels

Commissioner Helen Dixon, keynote address - Arthur Cox Data Protection Leadership Forum

Appendix 4: Case Studies

Case Studies: Complaints

Case Study 1:

Failure to respond to an Access Request

The DPC received a complaint from an individual regarding a subject access request made by him to an organisation (the data controller) for a copy of all information held regarding his engagement with the data controller. The individual did not receive a response to this request.

The DPC intervened to see if the matter could be informally resolved. The complainant was in particular not satisfied with the fact that certain documents had not been provided in response to his access request. The position of the data controller was that the documents were not provided as the personal data had been provided "in another format".

Data protection access rights are not about access to documents per se. They are about access to personal data. An access request may be fulfilled by providing the individual with a full summary of their data in an intelligible form. The form in which it is supplied must be sufficient to allow the applicant to become aware of the personal data being processed, check they are accurate and being processed lawfully.

Having examined what data the controller did provide in this case, the DPC was satisfied to advise the complainant that he had been provided with all of the data to which he was entitled under data protection legislation.

Case Study 2:

Failure to respond to an Access Request (II)

The DPC received a complaint from an individual regarding a subject access request made by her to a service establishment (the data controller) for a copy of CCTV footage relating to their visit to the data controller's premises on a particular date. The individual did not receive a response to this request.

This DPC intervened to see if the matter could be informally resolved.

By the time the DPC had received the complaint, it transpires that the data controller no longer held any information relating to her as it was not aware of the access request until it was brought to its attention by this office. This was because the email address to which the access request was sent was not an address that was regularly used, despite this being the email address contained in the data controller's Privacy Policy. The data controller further stated that CCTV footage is retained for 14 days due to the system storage capacity and it was therefore not in a position to provide the requested CCTV footage as more than 14 days had elapsed.

Having examined the matter thoroughly, it was apparent to this office that the data controller contravened Article 12(3) of the GDPR as controllers have an obligation to provide a response to the individual's subject access request within the statutory timeframe as set out in Article 12 of the GDPR, even where the controller is not in possession of any such data. The failure by the data controller to monitor the inbox associated with the email address in its Privacy Policy resulted in its failure to secure the relevant CCTV footage before it was deleted in line with its retention policy. In this regard, the failure to have relevant organisational measures in place resulted in the data controller being unable to fulfil the subject access request.

The DPC issued directions to the data controller reminding it of its obligation to monitor any email mailbox which they provide for data subject requests. The DPC will take enforcement action if a repeat of this issue arises with the same controller.

Case Study 3:

Fair obtaining complaint made against a Golf Club

An individual made a complaint to the DPC concerning the data controller's use of CCTV footage to investigate an incident in which the individual was involved.

The individual had organised an event in a leisure facility (the data controller), and displayed signage in relation to Covid-19 procedures to assist attendees. At the end of the event, the individual inadvertently removed a different sign also in relation to Covid-19 procedures when removing the signage they had installed for the event. The data controller reviewed its CCTV footage to establish who had removed the sign.

The complainant was of the opinion that the data controller did not process their personal data in a proportionate or transparent manner, and that it did not comply with its obligations as a data controller in how it investigated the incident. Accordingly, the individual lodged a complaint with the DPC.

The DPC intervened to seek to resolve the matter informally and the parties reached an amicable resolution when the leisure centre agreed to undertake an audit of its use of the CCTV system and to restrict access to review CCTV footage to designated staff members.

The individual thanked the DPC for handling their complaint in a professional and helpful manner and further stated that they were reluctant to submit the complaint initially as they are aware of the volume of complaints the DPC deals with and the accompanying constraints on resources. The complainant stated that they felt confident that the issue will not arise in the future as a result of the involvement of the DPC. The individual wished to express their appreciation and acknowledge the DPC's efficiency in dealing with the matter.

Case Study 4:

Right to be Forgotten (Microsoft)

The complaint concerned the individual's dissatisfaction with Microsoft Ireland Operations Limited's (Data Controller) response to their right to be forgotten request pursuant to Article 17 GDPR. The individual requested the delisting of two URLs that were returning on the Data Controller's search engine when searching the individual's name.

The Data Controller confirmed to the individual that the URLs were delisted. However, a search of the individual's name, carried out by their legal representative, showed that the URLs continued to be returned. The DPC reviewed the URLs when receiving the complaint and confirmed that the URLs were still being returned.

The DPC intervened to seek to swiftly and informally resolve the matter.

The DPC corresponded with the Data Controller and noted that despite confirmation that the URLs were delisted, they continued to return when searching the individual's name. The Data Controller investigated the request further and confirmed to the DPC that the URLs had now been delisted.

Following further investigation by the DPC, it was determined that while the original URLs requested for delisting no longer appeared, a different URL was now appearing, distinct from the other URLs, redirecting to the same content. The Data Controller delisted this URL also at the request made by the DPC on behalf of the individual.

The DPC wrote to the individual and outlined the Data Controller's actions. The DPC confirmed that all three URLs had been delisted by the Data Controller.

This case demonstrates the importance of Supervisory Authorities, in this case the DPC, carrying out their own investigations and ensuring that individuals' requests are fulfilled in line with GDPR. The above is an example of how the DPC took extra measures to ensure that the individual could comprehensively achieve a satisfactory outcome, rather than having to submit a new complaint for the new URL.

Case Study 5:

Access and Erasure request (Pinterest)

The complaint concerned the individual's dissatisfaction with Pinterest Europe's (**Data Controller**) response to his access and erasure requests pursuant to Article 15 GDPR and Article 17 GDPR, respectively.

The individual submitted his requests following the suspension of his account, in order to obtain a copy of all of his personal data and to have it deleted from the Data Controller's systems. The individual's account was suspended due to a violation of the Data Controller's policies regarding spam. The Data Controller responded to the requests via automated response which stated that it had reviewed the account and decided not to reactivate it because it noticed activity that violated its spam policy. As a result, the individual was no longer able to access his personal data stored on their account. The individual maintained that this information could not be correct as they seldom used their account and sought a more substantial response to their access and erasure requests.

The DPC took up the complaint with Pinterest.

The DPC outlined the individual's concerns in relation to his access and erasure requests and requesting that the Data Controller address those concerns more substantively. The DPC also requested that the Data Controller indicate whether the individual was provided with an opportunity to appeal his account suspension and, if so, describe the procedure for such appeals.

The Data Controller responded to the DPC stating that it had investigated the matter and explained that once an account is suspended on the basis of a spam violation, all correspondence is automatically directed to its Spam Operations team. The Data Controller further explained the appeal process and noted that the individual corresponded with the Spam Operations team in relation to the appeal of their suspension. The Spam Operations team failed to identify that the correspondence also included the individual's access and erasure requests and therefore this was not addressed in its response.

The Data Controller's response also noted that, although the Spam Operations team had rejected the individual's appeal of their account suspension, it had since carried out another review in light of its updated spam policies. Following this review, the Data Controller re-activated the individual's account.

The Data Controller also acknowledged the delay in responding to the individual and confirmed that it had since taken steps to ensure that such delays would not occur in responding to future requests.

The Data Controller confirmed that it had actioned the individual's access and erasure requests. It also confirmed that it had reached out to the individual to inform him of the steps it had taken in response to the DPC's correspondence and provided the individual with the explanations set out above.

The actions taken and explanations given by the Data Controller were also outlined to the individual by the DPC. The individual informed the DPC that they were satisfied with the actions taken by the Data Controller in response to the DPC's correspondence as it allowed him to download his data and delete his account.

This case study illustrates how often simple matters – such as a complaint being forwarded to the wrong unit in an organisation – can become data protection complaints if the matter is not identified appropriately.

Case Study 6:

Right to be Forgotten (Microsoft)

The complaint concerned the individual's dissatisfaction with Microsoft Ireland's (**Data Controller**) response to their right to be forgotten request pursuant to Article 17 GDPR. The individual requested to have 7 URLs delisted from being returned in a search against their name on the Data Controller's search engine. The individual stated that their National Identity number was contained in the URLs returned and raised concerns that the availability of their National Identity number increased the risk of identity theft.

The DPC intervened on behalf of the complainant.

The Data Controller originally refused the delisting request, stating that the URLs contained information of public relevance, and that the information

was published in an official bulletin of a government body; in this case, the Spanish Government.

The DPC corresponded with the Spanish Data Protection Authority in relation to the information published in the URLs. The Spanish Data Protection Authority stated that due to the introduction of the GDPR, the Spanish Data Protection law was modified and the Government is no longer permitted to disclose citizens' complete National Identification number alongside their name and surnames when publicising administrative acts.

Following clarification from the Spanish Data Protection Authority, the DPC informed the Data Controller of the change in the Spanish Data Protection law. The Data Controller stated that based on the update in Spanish Data Protection law, it would delist all requested URLs from being returned against the individual's name pursuant to Article 17 GDPR.

This case highlights the importance of communicating with other supervisory authorities during the complaint resolution process. In these circumstances, the DPC was provided with clarification on how Spain has adapted its national legislation to comply with the GDPR. It also allowed the Data Controller to adapt its current procedure to ensure that requests involving the delisting of URLs containing full National Identity numbers are handled in accordance with the updated national legislation.

Case Study 7:

Restrictions to the Right of Access – files from An Garda Siochána to the Director of Public Prosecutions

An individual complained to the DPC about the restrictions applied by the Director of Public Prosecutions (the DPP) in response to an access request. The person outlined they were a victim of a crime but a decision was reached by the DPP not to prosecute.

The DPC noted that the DPP imposed restrictions on access to the investigation file, the statement of a witness, memorandums of interviews taken as part of the investigation as well as correspondence between the DPP and An Garda Síochána (AGS). The DPC probed the restrictions applied by the DPP further as any restriction relied upon by data controllers must respect the essence of the fundamental rights and freedoms of individuals.

The data protection rights conferred under the Law Enforcement Directive as transposed in the Data Protection Act 2018 pertain solely to personal data relating to an individual's own personal information and do not confer a right of access to the personal data of a third party. In this case, the DPP clarified that it restricted the right of access of the individual in question under Section 94(2)(e) of the Act in order to protect the rights and freedoms of other persons. The DPP also cited 91(7) of the Act which provides that a data controller shall not provide individuals with personal data relating to another individual where doing so would reveal, or would be capable of revealing, the identity of the other individual. The only circumstances in which 91(7) does not apply is where a third party consents to the provision of their information to the individual making the request as set out in 91(8) of the Act.

With regard to the investigation file submitted by AGS to the DPP and correspondence between the DPP and AGS, under Section 162 of the Act, individual data subject rights and controller obligations do not apply as far as these relate to personal data processed for the purpose of seeking, receiving or giving legal advice. Equally, such rights and obligations do not apply in respect of which a claim of privilege can be made for the purpose of or in the course of legal proceedings. The DPC noted the Act explicitly outlines that these legal proceedings include personal data consisting of communications between a client and his or her legal advisers or between those advisers. After seeking further clarification, it was apparent to the DPC that the restrictions invoked were valid and legal privilege applied to the data sent between AGS and the DPP.

The DPC handled several similar complaints during 2022 against the DPP in relation to subject access requests. Each complaint examined followed a procedure whereby the DPC probed further with regard to any restrictions applied by the DPP on a case-by- case basis, in addition to querying any privilege claimed in respect of data withheld.

In 2022, a complaint against the DPP examined by the DPC in 2020 was the subject of a challenge by the complainant in Carrick-on-Shannon Circuit Court (civil) with regard to the DPC's acceptance of the restrictions applied by the DPP. The Court noted that the DPC had queried the reasons given by the DPP to the appellant for withholding certain personal data and that the DPP had provided the DPC with a further detailed response. The Court stated that it was clear from the pleadings that the handling of the complaint was not a rubber-stamping exercise and that the DPC had examined all matters. The Court stepped through each of the three documents withheld by the DPP and the privilege claimed in respect of each and found no error in respect of any of the three categories.

Case Study 8:

Disclosure Without Consent

An individual complained to the DPC that the Criminal Assets Bureau (CAB) disclosed his personal financial details without his consent, to a number of individuals against whom CAB had taken legal proceedings. CAB advised the DPC that the proceedings in question were under the Proceeds of Crime Act, 1996-2016 (PoCA), the purpose of which is to identify and confiscate property, established to the satisfaction of the High Court, to be the proceeds of crime. CAB stated the information contained in the subject documentation was required to establish the provenance of property the subject matter of the proceedings. CAB outlined that the personal data of the complainant was intertwined with the personal data of the individuals being prosecuted and could not be redacted from the court documents. The DPC noted such proceedings are governed by section 158(1) of the Data Protection Act, 2018 (the Act) which provides that the GDPR and Law Enforcement Directive as transposed in the Act may be restricted in order to ensure the protection of judicial independence and judicial proceedings.

As set out in Section 101(2) of the Act, the DPC is not competent for the supervision of data processing operations of the courts when acting in their judicial capacity. The DPC advised the complainant that CAB prepared the court documents for the purposes of court proceedings and that supervision of data processing operations of the courts when acting in their judicial capacity is assigned to a Judge appointed by the Chief Justice pursuant to section 157 of the Act. The DPC provided the complainant with the contact details for the assigned judge.

Case Study 9:

Disclosure of Sensitive Data

An individual complained to the DPC that a Clothing and Food Company disclosed their personal medical information by issuing postal correspondence with the words "Coeliac Mailing" printed on the outside of the envelope. As part of the Stores Value Card facility, the individual in question had signed up to receive an 'Annual Certificate of Expenditure' of gluten free products purchased during the year, which could be used for tax purposes. The DPC advised the Store that under Article 9 of the GDPR, health data is deemed sensitive data and is afforded additional protection and that displaying the words "Coeliac Mailing" has to be examined in light of Article 9 of the GDPR. In response, the Store advised the DPC that it instructed its marketing department to cease using this wording on the outside of envelopes for all future mailings. The DPC welcomes the positive outcome to this engagement.

Case Studies: Electronic Direct Marketing

Case Study 10:

Prosecution of Guerin Media Limited

In January 2022, the DPC received two complaints from two individuals regarding unsolicited marketing emails received from Guerin Media Limited. In response to the DPC's investigation of the complaints, Guerin Media Limited explained that the two individuals' email contact details had previously been removed from all marketing lists held by the company with the exception of a Gmail contact list that it maintain. It stated that due to human error and the fact that their details remained on the Gmail contact list, both individuals were sent marketing emails from Guerin Media Limited that should not have occurred.

The DPC had previously prosecuted Guerin Media in 2019 for breaching Regulation 13 of the ePrivacy Regulations in relation to previous complaints regarding similar incidents of unsolicited email marketing. Accordingly, the DPC decided to proceed to another prosecution arising from these complaint cases.

At Naas District Court on 5 December 2022, Guerin Media Limited pleaded guilty to three charges under Regulation 13(1) of the ePrivacy Regulations. The District Court convicted Guerin Media Limited on all three charges and it imposed fines totalling €6,000. Guerin Media Limited agreed to pay €1,000 towards the DPC's legal costs.

Case Study 11:

Prosecution of Vodafone Ireland Limited

In July 2021, the DPC received one complaint from an individual regarding an unsolicited marketing telephone call received from Vodafone Ireland Limited. In response to the DPC's investigation of the complaint, Vodafone Ireland Limited explained that the existing customer had opted out of receiving marketing communications in March 2018. Despite this, Vodafone Ireland Limited had carried out a manual check of preferences in advance of conducting a marketing campaign, and due to human error, the complainant was included in the marketing campaign.

The DPC had previously prosecuted Vodafone Ireland Limited in 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 27 June 2022, Vodafone Ireland Limited pleaded guilty to one charge under Regulation 13(6) of the ePrivacy Regulations. 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. Vodafone Ireland Limited agreed to discharge the DPC's legal costs.

Case Study: One-Stop-Shop Complaint

Case Study 12:

Erasure request to Tinder by Greek data subject, handled by the DPC as Lead Supervisory Authority

This case study concerns a complaint the DPC received via the One-Stop-Shop (OSS) mechanism created by the GDPR from an individual regarding an erasure request made by them to MTCH Technology Services Limited (Tinder).

As way of background, the individual's account was the subject of a suspension by Tinder. Following this suspension, the individual submitted a request to Tinder, under Article 17 of the GDPR, seeking the erasure of all personal data held in relation to them. When contacting Tinder, the individual also raised an issue with the lack of a direct channel for contacting Tinder's DPO. As the individual was not satisfied with the response they received from Tinder, they made a complaint to the Greek Supervisory Authority. The individual asserted that neither their request for erasure nor their concerns about accessing the DPO channels, had been properly addressed by Tinder. As the DPC is the Lead Supervisory Authority (LSA) for Tinder, the Greek Supervisory Authority forwarded the complaint to the DPC for handling.

The DPC intervened to seek a swift and informal resolution of the matter in the first instance.

The DPC put the substance of the complaint to Tinder and engaged with it. In response and by way of a proposed amicable resolution, Tinder offered to conduct a fresh review of the ban at the centre of this case. Following this review, Tinder decided to lift the ban. The lifting of a ban by Tinder allows an individual to be then in a position to access their account on the platform. The individual can then decide if they wish to use the self-delete tools to erase their account from within the Tinder platform. In addition to the above, Tinder provided information for the individual in relation to its retention policies.

In relation to the matter of individuals being able to contact its DPO, on foot of the DPC's engagement with Tinder, the platform agreed to strengthen its existing processes by posting a dedicated FAQ page on its platform. This page now provides enhanced information to individuals on specific issues relating to the processing of personal data and exercising those rights directly with Tinder's DPO.

Via the Greek Supervisory Authority, the DPC informed the individual of the actions taken by Tinder. In their response the individual confirmed that they were content to conclude the matter and, as such, the matter was amicably resolved pursuant to section 109(3) of the Data Protection Act 2018 (the Act), and the complaint was deemed to have been withdrawn

This case study again demonstrates the benefits — to individual complainants — of the DPC's intervention by way of the amicable resolution process. The DPC's engagement with the controller also resulted in Tinder improving the information that it makes available to all of its users on its platform.

Case Studies: Data Breach Complaint

Case Study 13:

Law Enforcement Directive (LED)

The Garda Síochána Ombudsman Commission (GSOC) sent a letter containing the outcome of its investigation into a complaint to an address where the person who made the complaint no longer resided. The DPC established the letter was posted to the address where the individual lived at the time of a previous complaint that they had made to GSOC. The individual in question had subsequently informed GSOC they no longer lived at that address and that with regard to the new complaint they were only contactable by email.

The DPC liaised extensively with GSOC regarding this complaint. GSOC reported the data breach to the DPC through the normal breach reporting channels. To avoid this type of incident happening again, GSOC advised the DPC that an email issued internally to all staff advising of the importance of ensuring the accuracy of personal data entered onto the Case Management System (CMS). GSOC also outlined that it sent a separate email to all line management in the GSOC Casework section advising them of the necessity to accurately input personal data on the CMS and to amend this information whenever updated information is received.

Case Study 14:

Disclosure of account statements by a bank to the representative of a joint account holder

The complainant in this case held a joint bank account with a family member. Following a request from the solicitors of the other joint account holder, the bank (the data controller) disclosed copies of bank statements relating to the account, which included the complainant's personal data, to those solicitors. The complainant was concerned that this disclosure did not comply with data protection law.

During the course of the DPC's handling of this complaint, the bank set out its position that any joint account holder is entitled to access the details and transaction information of the joint account as a whole. The bank further took the view that, in relation to solicitors who are acting for its customers, it is sufficient for it to accept written confirmation from a solicitor on their headed paper that the solicitor acts for the customer as authority for the bank to engage with the solicitor in their capacity as a representative of the bank's customer.

Data protection law requires that personal data be collected or obtained for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes (the "purpose limitation" principle). In this case, the DPC noted that the bank had obtained the complainant's personal data in order to administer the joint account which the complainant held with the other account holder, including the making of payments, the collection of transaction information and the preparation of bank statements. It appeared to the DPC that it was consistent with the bank's terms and conditions for the joint account, and the account holder's signing instructions on the account (which allowed either party to sign for transactions without the consent of the other account holder), that the administration of the account could be completed by one account holder without the consent of the other. In the light of this, the DPC considered that the disclosure of bank statements to the solicitors of the other joint account holder was not incompatible with the specified, explicit and legitimate purpose for which the complainant's personal data had been obtained by the bank, i.e. for the administration of the joint account.

Second, the DPC considered whether the bank had a lawful basis for the disclosure of the complainant's personal data, as required under data protection law. In this regard, the DPC was satisfied that the bank was entitled to rely on the "legitimate interests" lawful basis, which permits the processing of personal data where that processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party. In this case, the bank had disclosed the complainant's

personal data on the basis that the solicitor was acting for the other joint account holder and was seeking the statements for legitimate purposes, namely to carry out an audit of the other account holder's financial affairs. In circumstances where, pursuant to the signing instructions on the account, the other account holder would have been entitled to administer the account, the DPC was satisfied that the bank would not have had any reason to suspect that the disclosure would be unwarranted by reason of any prejudice to the complainant's fundamental rights or freedoms. Accordingly, the DPC considered that the bank had a lawful basis for the disclosure, regardless of whether the complainant had provided consent.

Finally, the DPC considered whether the bank had complied with its obligations under data protection law to take appropriate technical and organisational measures to ensure security of personal data against unauthorised or unlawful disclosure. In this regard, the DPC accepted the position of the bank, set out in its policies, that it was appropriate to accept written confirmation from a solicitor that they were authorised to act on behalf of an account holder, without seeking further proof. The bank's policy in this regard was based on the fact that a solicitor has professional duties as an officer of the court and as a member of a regulated profession.

Case Studies: Data Breach Notification

Case Study 15:

Inaccurate data leading to potential high risk resulting from inaccurate Central Credit Register data

The DPC received a notification from a financial sector data controller concerning an individual whose account had been incorrectly reported to the Central Credit Registrar (CCR). The controller had purchased the individual's account as part of a portfolio sale in 2015 and was not aware that the individual had been adjudicated bankrupt in 2014. Individuals who have been declared bankrupt fall outside the scope of reporting obligations to the CCR. In addition, accounts with returns prior to the commencement of the CCR on the 30 June 2017 are not reportable to it.

The individual experienced difficulty obtaining a loan because their CCR record, which is visible to other lending institutions, had been reported in error by the controller as live and in arrears. The risk to the rights and freedoms of the individual was assessed as high and the breach was accordingly communicated by the controller to the individual under Article 34 of the GDPR.

The DPC confirmed with the controller that the individual's CCR record had been amended. By way of mitigation, the controller introduced measures which require sellers of portfolios to disclose information on individuals such as bankruptcies.

This case highlights the importance of having systems in place to ensure the security and integrity of personal data under Article 5(1)(f) GDPR . Controllers should be aware of the personal data they hold on individuals and have measures in place to validate and understand the data when acquiring it from other parties. The case also demonstrates that controllers have a duty to prevent any alteration to or unauthorised disclosure of personal data, incorrect or otherwise to the CCR which poses risk to individuals.

Case Study 16:

Hacking of third party email

A Hospice Care Centre (Data Controller) utilises the services of Microsoft Office 365, a cloud based email service and also engaged third party IT Consultants.

An Office 365 Audit was conducted by the IT Provider every quarter, where a number of recommendations by the service provider were identified including but not limited to all user accounts to have Multifactor Authentication (MFA) and the disabling of forwarding rules on all accounts.

A user's credentials were subsequently compromised and the IT Consultants established that the credentials were obtained as a result of a brute force attack, which may have been prevented had the controller introduced Multi-Factor Authentication as recommended at the time of the audit. On the advice of the IT Consultants, the compromised user password was reset and MFA introduced for this user. The controller has now commenced the introduction of MFA to all users.

This breach could likely have been prevented if the recommendations of the audit were introduced in a timely manner.

Case Studies: Inquiries

Case Study 17:

Enforcement follow-through: Surveillance Technologies and Data Protection in Limerick

As reported in last year's annual report the DPC issued a decision to Limerick City and County Council in December 2021 regarding a broad range of issues pertaining to surveillance technologies deployed by the Council, in 2022 the DPC followed up on the decision's twenty-one corrective actions to be taken by Limerick City and County Council to ensure that these were implemented within the specified timeframes.

Amongst the issues of concern in the decision were the Council's use of CCTV cameras where no authorisation from the Garda Commissioner was received, no lawful basis for the use of traffic management CCTV cameras, access from Henry Street Garda Station to the Council's CCTV cameras in specified locations, the use of automatic number plate recognition technology and drones in public places which were used for the purposes of prosecuting crime or other purposes. The DPC in its decision imposed a temporary ban on the Council's processing of personal data in respect of certain CCTV cameras and ordered the Council to bring its processing into compliance by taking specified actions. The Council was also reprimanded by the DPC in respect of infringements, and an administrative fine in the amount of €110,000 was imposed.

By way of follow-up enforcement action in respect of the implementation of the corrective actions, the DPC wrote to Limerick City and County Council and met virtually with them on a number of occasions in 2022 in order to monitor progress. On 27 July 2022, the DPC carried out an onsite inspection at Limerick City and County Council to verify that all corrective actions had been carried out.

At the end of this process, the DPC was satisfied that Limerick City and County Council had implemented the corrective actions required by the DPC's decision. Amongst the issues of note in that regard were the following:

- Authorisation of the Garda Commissioner under Section 38 of the Garda Síochána Act, was obtained for 353 CCTV cameras across Limerick City and County;
- A joint controller agreement between An Garda Síochána and Limerick City and County Council in respect of the authorised cameras was put in place;
- All automated number plate recognition capability was removed from all sites where it had been in operation;
- All traffic management cameras were disconnected;
- CCTV cameras that previously focussed on traveller accommodation sites were removed;
- The link from some of the Council's CCTV cameras to Henry Street Garda Station was disconnected;
- Drones were grounded;
- New CCTV signage was erected across all CCTV sites;
- Plans to implement real-time monitoring of CCTV cameras in fourteen towns and villages across Co. Limerick were abandoned; and
- 126 no. of CCTV cameras are no longer in operation.

In addition, in late November 2022, the Circuit Court confirmed the DPC's decision to impose an administrative fine of €110,000 on Limerick City and County Council in relation to the GDPR infringements identified in the decision.

Case Study 18:

Article 60 decision concerning Twitter International Company – ID Request, Erasure Request

A complaint was lodged directly with the DPC on 02 July 2019 against Twitter International Company ("**Twitter**"), and accordingly was handled by the DPC in its role as lead supervisory authority. The complainant alleged that, following the suspension of their Twitter account, Twitter failed to comply within the statutory timeframe with an erasure request they had submitted to it. Further, the complainant alleged that Twitter had requested a copy of their photographic ID in order to action their erasure request without a legal basis to do so. Finally, the complainant alleged that Twitter had retained their personal data following their erasure request without a legal basis to do so.

The complainant's Twitter account was suspended as Twitter held that the complainant was in breach of its Hateful Conduct Policy. Once Twitter suspended the account, the complainant sought that all of their personal details, such as email address and phone number, be deleted. They submitted multiple requests to Twitter asking that their data be erased. Twitter asked the complainant to submit a copy of their ID in order to verify that they were, in fact, the account holder. The complainant refused to do so. In the premises, Twitter ultimately complied with the erasure request without the complainant's photographic ID.

The DPC initially attempted to resolve this complaint amicably by means of its complaint handling process. However, those efforts failed to secure an amicable resolution and the case was opened for further inquiry. The issues for examination and determination by the DPC's inquiry were as follows: (i) whether Twitter had a lawful basis for requesting photographic ID where an erasure request had been submitted pursuant to Article 17 GDPR, (ii) whether Twitter's handling of the said erasure request was compliant with the GDPR and Data Protection Act 2018 and (iii) whether Twitter had complied with the transparency requirements of Article 12 GDPR.

In defence of its position, Twitter stated that authenticating that the requester is who they say they are is of paramount importance in instances where a party requests the erasure of their account. It states that unique identifiers supplied at the time of registration of an account (i.e. email address and phone number) simply associate a user with an account but these identifiers do not verify the identity of an account holder. Twitter posited that it is cognisant of the fact that email accounts can be hacked and other interested parties might seek to erase an account particularly in a situation such as this, where the account was suspended due to numerous alleged violations of Twitter's Hateful Conduct Policy. The company indicated

that it retains basic subscriber information indefinitely in line with its legitimate interest to maintain the safety and security of its platform and its users.

Twitter further argued that, as it did not actually collect any ID from the complainant, Article 5 (1)(c) was not engaged. Notwithstanding this, it stated that the request for photo identification was both proportionate and necessary in this instance. It indicated that a higher level of authentication is required in circumstances where a person is not logged into their account, as will always be the case where a person's account has been suspended.

Having regard to the complainant's erasure request and the associated obligation that any such request be processed without 'undue delay', Twitter set out a timeline of correspondence pertaining to the erasure request between it and the complainant. Twitter stated that the Complainant had made duplicate requests and, as such, had delayed the process of deletion/ erasure themselves. Regarding data retention, Twitter advised the DPC that it retained the complainant's phone number and email address following the completion of their access request. It stated that it retains this limited information beyond account deactivation indefinitely in accordance with its legitimate interests to maintain the safety and security of its platform and users. It asserted that if it were to delete the complainant's email address or phone number from its systems, they could then use that information to create a new account even though they have been identified and permanently suspended from the platform for various violations of its Hateful Conduct Policy.

Following the completion of its inquiry, on 27 April, 2022 the DPC adopted its decision in respect of this complaint in accordance with Article 60(7) of the GDPR. In its decision the DPC found that the data controller, Twitter international Company, infringed the General Data Protection Regulation as follows:

- **Article 5(1)(c):** Twitter's requirement that the complainant verify his identity by way of submission of a copy of his photographic ID constituted an infringement of the principle of data minimisation, pursuant to Article 5(1)(c) of the GDPR;

- **Article 6(1):** Twitter had not identified a valid lawful basis under Article 6(1) of the GDPR for seeking a copy of the complainant's photographic ID in order to process his erasure request;

- **Article 17(1):** Twitter infringed Article 17(1) of the GDPR, as there was an undue delay in handling the complainant's request for erasure; and

- **Article 12(3):** Twitter infringed Article 12(3) of the GDPR by failing to inform the data subject within one month of the action taken on his erasure request pursuant to Article 17 of the GDPR.

The DPC also found in its decision that Twitter had a valid legal basis in accordance with Article 6(1)(f) for the retention of the complainant's email address and phone number that were associated with the account. It also found that, without prejudice to its finding above concerning the data minimisation principle with regard to photo ID, Twitter was compliant with the data minimisation principle as the processing of the email address and phone number data was limited to what was necessary in relation to the purposes for which they are processed.

In light of the extent of the infringements, the DPC issued a reprimand to Twitter International Company, pursuant to Article 58(2) (b) of the GDPR. Further the DPC ordered Twitter International Company, pursuant to Article 58(2)(d), to revise its internal policies and procedures for handling erasure requests to ensure that data subjects are no longer required to provide a copy of photographic ID when making data erasure requests, unless it can demonstrate a legal basis for doing so. The DPC ordered that Twitter International Company provide details of its revised internal policies and procedures to the DPC by 30 June 2022. Twitter complied with this order by the set deadline.

Case Study 19:

Article 60 decision concerning Airbnb Ireland UC – Delayed response to an Access Request and an Erasure Request

A complaint was lodged with the Berlin Commissioner for Data Protection and Freedom of Information ("**Berlin DPA**") against Airbnb Ireland UC ("**Airbnb**") and was thereafter transferred to the DPC to be handled in its role as lead supervisory authority.

The complainant alleged that Airbnb failed to comply with an erasure request and a subsequent access request they had submitted to it within the statutory timeframe. Further, the complainant stated that when they submitted their request for erasure, Airbnb requested that they verify their identity by providing a photocopy of their identity document ("**ID**"), which they had not previously provided to Airbnb.

The DPC initially attempted to resolve this complaint amicably by means of its complaint handling process. However, those efforts failed to secure an amicable resolution and the case was opened for further inquiry. The issues for examination and determination by the DPC's inquiry were as follows: (i) whether Airbnb had a lawful basis for requesting a copy of the complainant's ID where they had submitted an erasure request, pursuant to Article 17 GDPR, (ii) whether Airbnb's handling of the said erasure request was compliant with the GDPR and Data Protection Act 2018 and (iii) whether Airbnb's handling of the complainant's access request was compliant with the GDPR and Data Protection Act 2018.

Airbnb responded to the complainant's allegations, justifying its request for photographic ID given the adverse effects that would flow from a wrongful deletion of an account. Airbnb highlighted that fraudulent deletion of an Airbnb account can lead to significant real-world harm including, in the case of hosts, the economic harm through cancelled bookings and loss of goodwill built up in the account and, in the case of guests, the potential loss of accommodation while travelling abroad. Airbnb stated that these are not trivial risks and appropriate steps must be taken to address them. It further stated that the provision of an ID document to authenticate an erasure request is a reliable proof of identification and that it does not place a disproportionate burden on the individual making the erasure request. It posited that photographic identity can be considered to be an evidential bridge between an online and an offline identity.

Airbnb ultimately complied with the complainant's erasure request, validating their identity by providing them with the option of logging into

their account to verify their identity, without the necessity to provide ID. Following intervention by the DPC, Airbnb complied with the complainant's access request. Having completed its inquiry, on 14 September 2022, the DPC adopted its decision in respect of this complaint in accordance with Article 60(7) of the GDPR. In its decision the Data Protection Commission found that the data controller, Airbnb Ireland UC, infringed the General Data Protection Regulation as follows:

- **Article 5(1)(c) of the GDPR**

The DPC found that Airbnb's requirement that the complainant verify their identity by way of submission of a copy of their photographic ID constituted an infringement of the principle of data minimisation, pursuant to Article 5(1) (c) of the GDPR. This infringement occurred in circumstances where less data-driven solutions to the question of identity verification were available to Airbnb;

- **Article 6(1) of the GDPR**

The DPC found that, in the specific circumstances of this complaint, the legitimate interest pursued by the controller did not constitute a valid lawful basis under Article 6 of the GDPR for seeking a copy of the complainant's photographic ID in order to process their erasure request; and

- **Article 12(3) of the GDPR**

The DPC found that Airbnb infringed Article 12(3) of the GDPR with respect to its handling of the complainant's access request. This infringement occurred when Airbnb failed to provide the complainant with information on the action taken on their request within one month of the receipt of the access request.

In light of the extent of the infringements, the DPC issued a reprimand to Airbnb Ireland UC, pursuant to Article 58(2)(b) of the GDPR. Further the DPC ordered Airbnb Ireland UC, pursuant to Article 58(2)(d), to revise its internal policies and procedures for handling erasure requests to ensure that data subjects are no longer required to provide a copy of photographic ID when making data erasure requests, unless it can demonstrate a legal basis for doing so. The DPC ordered that Airbnb Ireland UC provide details of its revised internal policies and procedures to the DPC by 4 November 2022. Airbnb complied with this order by the set deadline.

Case Study 20:

Cross-border complaint resolved through EU cooperation procedure

Background

In February 2021 a data subject lodged a complaint pursuant to Article 77 GDPR with the Data Protection Commission concerning an Irish-based data controller. The DPC was deemed to be the competent authority for the purpose of Article 56(1) GDPR.

The details of the complaint were as follows:

a. The data subject emailed the data controller in January 2021 to request erasure of his personal data.

b. The data subject did not receive any response from the data controller

Following a preliminary examination of the material referred to it by the complainant, the DPC considered that there was a reasonable likelihood of the parties concerned reaching informal resolution of the subject matter of the complaint within a reasonable timeframe.

Informal Resolution

The DPC engaged with both the data subject and the data controller in relation to the subject-matter of the complaint. Further to that engagement, it was established that during the week in which the data subject sent his erasure request by email to the controller a new process to better manage erasure requests was implemented by the controller. The data controller informed the DPC that it was in a transition period during the week the email came in and it appears a response was missed. New personnel were being trained on how to manage these types of requests during this transition period. The data controller stated that it was an oversight, possibly due to the technical transition or human error, and it regretted the error. In the circumstances, the data controller agreed to take the following actions:

1. The data controller agreed to comply with the erasure request; and

2. The data controller sincerely apologised for the error.

In January, 2022 the DPC informed the data subject by email of the final outcome of its engagement with the data controller. When doing so, the DPC noted that the actions now taken by the data controller appeared to adequately deal with the concerns raised in his complaint. In the circumstances, the DPC asked the data subject to notify it, within two months, if he was not satisfied with the outcome so that the DPC could consider the matter further.

On the following day the data subject informed the DPC by email that he agreed with the informal resolution given his concerns regarding the data controller were now satisfied. The DPC was subsequently informed by the data controller that the erasure request was completed and that the personal data of the data subject had been erased.

Confirmation of Outcome

For the purposes of the GDPR consistency and cooperation procedure, the DPC communicated a draft of the outcome which confirmed that:

- The complaint, in its entirety, had been amicably resolved between the parties concerned;
- The agreed resolution was such that the object of the complaint no longer existed.

No relevant and reasoned objections were received from the concerned supervisory authorities concerning the draft and the DPC subsequently closed the file in this case.

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