

Annual Report 2021



**An Coimisiún um
Chosaint Sonraí**
Data Protection
Commission



Glossary	4
1. Foreword	5
2. Executive Summary	11
3. Mission, Vision and Values at the DPC	15
4. Regulatory Strategy	17
5. Roles and Responsibilities	19
6. Contacts, Queries and Complaints	22
7. Breaches	49
8. Inquiries	57
9. Significant Sanctions and Corrective Measures	67
10. Litigation	78
11. Supervision	86
12. Children's Data Protection Rights	94
13. Data Protection Officers	97
14. International Activities	99
15. Communications	102
16. Corporate	104

Appendices

Appendix 1: Report on Protected Disclosures received by the Data Protection Commission in 2021	108
Appendix 2: Report on Energy Usage at the Data Protection Commission	110
Appendix 3: Barnville Judgment: Facebook Ireland Limited v. Data Protection Commission and Maximilian Schrems	112
Appendix 4: Audits of Political Parties	117
Appendix 5: Financial Statement for the year 1 January 2021 to 31 December 2021 and the DPC's Statement of Internal Controls	119

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

1



Foreword

Introduction

For the DPC, 2021 was characterised by significant momentum gain. Leveraging our experiences of the GDPR's first three full years of implementation, 2021 saw the DPC resolving thousands of complaints; processing thousands more data breach notifications; imposing fines and corrective measures on foot of detailed decisions; auditing the gamut of Irish political parties; settling its enforcement action in relation to certain processing elements of the Public Services Card on terms protective of the data rights of citizens generally; assessing multiple Binding Corporate Rules applications; contributing heavily at several hundred meetings of the European Data Protection Board; progressing scores of large-scale investigations; publishing comprehensive final guidance on protecting children's data; guiding and overseeing organisations and sectors in the practical application of the GDPR on an ongoing basis, and much more.

What gets measured gets done

Whilst the volume of work being completed by the office is ever-intensifying, what has remained elusive in 2021 is any agreed standard by which to measure the impacts and success or otherwise of a regulatory intervention in the form of GDPR that applies to literally everything. If the collective goal of all of us is to ensure better protection of people from misuses of their personal data and, indeed, to ensure they are not dis-advantaged by "over-implementation" of GDPR rules, the types of quantitative and qualitative metrics that need to be assessed must be carefully laid out. Further, enforcement priorities must be set and the impact of different enforcement measures and sanctions must be tracked and analysed over time for impact and value-for-money.

Whilst open in our acknowledgment that, in some respects at least, we need to do more, and better, a shared understanding of what measures we are tracking against in this combined individual rights-based/systemic supervision area of regulation would benefit all.

Perhaps more importantly, and emphasising that we take no issue with criticism motivated by a desire to improve the position of data subjects (and hold recalcitrant controllers, or indeed this office, to meaningful account), in the absence of an agreed set of measures to determine achievements or deficiencies, the standing of the GDPR's enforcement regime in overall terms is at risk of damage. This is particularly so when certain types of allegations levelled against this office serve only to obscure the true nature and extent of the challenges presented by the particular framework by which the EU member states are bound to legislate for the enforcement of data protection within the EU as a whole.

Several important considerations are engaged here.

Firstly, as flagged in my foreword to last year's annual report, the data protection space is one in which, as levels of consciousness of data protection as a concept have grown exponentially, a tendency has emerged in which a myriad of every-day exchanges, a large proportion of which do not engage any issue of data protection at all, are nonetheless presented on the basis that the application of data protection rules are central to their resolution.

Secondly, some commentators have expressed resistance to any kind of suggestion that the DPC would identify, in advance, the regulatory priorities it intends to bring to bear on its work over a defined period or that, in so doing, it would engage with the idea that, when assessing how to address two or more scenarios in which data protection concerns may be said to arise, the DPC might elect, on objective grounds, to prioritise its response to one over the other. Whilst this is undoubtedly difficult and sensitive territory, not least given the nature of the rights conferred on data subjects, not just by the GDPR but also by the Charter, it is nonetheless the case that, if it is to maximise the impact of its interventions and deliver meaningful outcomes to the broadest range of individuals, the DPC must look to deploy its resources in a targeted way.

Thirdly, we operate in an environment in which, as things stand, there is no agreed standard by which to measure the impact and success (or otherwise) of our regulatory interventions.

In that sort of vacuum, a narrative has emerged in which the number of cases, and the quantity and size of the administrative fines levied, are treated as the sole measure of success, informed by assumptions¹ as to the effectiveness of financial penalties, in particular, as drivers of real changes in behaviour, capable of delivering identifiable and meaningful improvements for data subjects. In that regard, a recent (2022) survey² citing Luxembourg and Ireland as top of a league table for fines in the EU tells us little about how effective regulation under the GDPR has been. (To be fair, the survey's authors do not suggest otherwise). Likewise, figures representing the number of cross-border cases provide little by way of meaningful insight. The decisions delivered in such cases vary widely both in the complexity of the subject matter and in the investigative procedures applied. For example a decision of the DPC, running to several hundred pages and touching on the complex operating processes of large multinational organisations, impacting on millions of people, is measured side by side with a two-line treatment of a comparatively simple issue that has minimal ramifications for data subjects in general. This is clearly not an informative means of measuring the success (or otherwise) of the GDPR.

Against the backdrop of these sorts of considerations, the DPC put its own regulatory strategy for the next 5 years out to public consultation, engaging with a range of stakeholders as we sought to develop our approach to the identification of the priorities we would bring to bear in our work, and setting out the reasons underpinning our strategic choices. As set out in more detail below, the consultation process was completed in 2021, and a finalised strategy document was adopted.³

Separately, the DPC is continuing to work alongside other EU DPAs to agree on a set of metrics to be used to measure regulatory outputs across the EU on a like-for-like basis, all with a view to addressing questions relating to the effectiveness of our interventions. On that score, both lawmakers and regulatory authorities (the DPC included) must be prepared to learn honestly from their legislative and regulatory efforts to date.

1 There is a body of evidence that indicates that such assumptions are not well founded. See for example <https://academic.oup.com/jeclap/article/12/4/301/5909388>

2 <https://www.dlapiper.com/en/us/insights/publications/2022/1/dla-piper-gdpr-fines-and-data-breach-survey-2022/>

3 <https://dataprotection.ie/en/news-media/latest-news/dpc-publishes-regulatory-strategy-2022-2027>

Regulation of large-scale platforms generally

Much of the public commentary around the effectiveness (or not) of data protection regulation across the EU is set against concerns about the level of control exercised by large-scale social media platforms. One recent feature of such discussions is the extent to which it is acknowledged that the control enjoyed by the platforms (in contexts extending beyond those with which data protection is directly concerned) may not be capable of being addressed in an effective way within a single regulatory discipline, whether that be data protection, competition law or content regulation.


Already in the United States, that discussion has moved a step further, with some commentators pointing out (in the context of the debate around the merits of introducing a federal data protection law) that there are many ways in which the activities of platforms can fall between cracks in regimes designed to regulate content, competition and data protection.

The same commentators have also raised questions as to whether concepts considered central to the data protection regimes that have developed in Europe (to include the concept of “individual control” as a means to protect individual users) can provide meaningful protection for platform users against some or all of the harms associated with particular aspects of the internet.

From a European perspective, there is no question but that, even allowing for its imperfections, the GDPR provides (and will continue to provide) the best-available framework within which the data protection rights of individuals can most effectively be vindicated in these parts.

For present purposes, however, a key consideration in these sorts of discussions is this: if the effectiveness of the GDPR’s enforcement regime as applied by national supervisory authorities is to be measured (and it must be measured), then we need to identify, with precision, the particular harms and risks we are looking to reduce and/or eliminate, and it must be acknowledged that, whilst the effective enforcement of data protection rules against platforms may serve to constrain the platforms’ power in certain respects, it is not the role of the DPC, or of any data protection supervisory authority, to target all manifestations of such power in respect of which concerns have been expressed.

It is against this particular backdrop that we need to find ways to measure performance by data protection supervisory authorities. As flagged above, there are several elements to that. As one step, the DPC has fixed upon – and declared – its regulatory priorities for the next 5 years. The work that remains ongoing with our colleagues throughout the EEA to identify a set of metrics by which performance can be assessed in an objective way – across all of the member states – is another such step. Such metrics must, however, move past both superficial totting exercises and assumptions to the effect that the bigger the fine, the greater the change of behaviour it will herald.



What is required is a system in which the effectiveness of our interventions (in whatever form they take) are assessed by asking whether they have delivered (measurable) changes in behaviour on the part of controllers and real-life (and measurable) benefits for data subjects.

DPC 5-Year Regulatory Strategy

As noted, 2021 saw the completion of the DPC's work on its **regulatory strategy for the next 5 years**, aimed at harnessing three years of reflection by the DPC and our many stakeholders on the application of GDPR in practice. One consistent demand from stakeholders was for more and more guidance and direction to allow more certainty about what is required to comply with the law and demonstrate accountability. The DPC as outlined in the Strategy intends to publish more guidance including more regular case studies of issues it has decided and work to support Data Protection Officers in their critical on-the-ground roles within organisations

Targeted actions aimed at ensuring children and more vulnerable internet users are protected in personal data terms - without shutting off their access - is a key strategic goal of the DPC and is already being given effect in a draft decision recently submitted by the DPC to our EU counterparts dealing with aspects of a particular internet platform's processing of children's data.

Our stated intention to more actively prioritise those complaints, the outcome of which will have the greatest impact, gave rise to a good deal of public commentary with certain commentators appearing to cast it as some sort of decision by the DPC to try to side-step its obligation to handle all individual complaints. The opposite is of course the case, reflecting our desire to ensure that complaints raising issues of substance, the resolution of which will achieve most for data subjects, are prioritised in terms of resources. The (now former) Advocate General Bobek of the CJEU highlighted this very issue in opinions issued before he departed his role in the autumn of 2021 where he sounded a note of caution about the risks of turning every exchange between individuals into a "GDPR issue"⁴. Ultimately, the DPC must fulfil its role and deploy its resources in such a way as to ensure it is giving effect to the GDPR in practical and meaningful ways that serve to protect individuals' rights where those rights are identified as being truly at risk.

Large-scale inquiries

This year's annual report features accounts of the outcomes delivered in a number of significant inquiries recently concluded by the DPC; it also details progress to date in a broad range of other inquiries to which the DPC has committed resources. One case that has attracted particular attention is the decision containing findings against WhatsApp which gave rise to a fine of €225m for a range of compliance failures relating to issues of transparency, and which also provided for an order directing remediation of the information provided to the public through WhatsApp's privacy policy. Whilst the decision is the subject of litigation, WhatsApp has agreed to make significant changes to its privacy policy in the meantime (reserving its position in relation to the litigation just referenced). Domestically, a significant outcome was delivered in an inquiry involving Limerick City and County Council in which a number of failures in terms of compliance with the GDPR and the Law Enforcement Directive were identified in the context of the deployment of CCTV and other surveillance technologies. (Details of this case can be found on page 69 of this report). A settlement was also reached in December 2021 in relation to an appeal brought by the Department of Social Protection against an enforcement notice issued by the DPC concerning personal data processing in the context of the Public Services Card. Inquiries into other areas of processing connected with the card remain ongoing. Whilst it is a policy matter for Government to fashion schemes to verify the identity of persons accessing public services, the DPC's position, based on the express terms of the GDPR and the EU Charter of Fundamental Rights, is that the processing of personal data in the context of any scheme of such scale must be grounded on an appropriate legal basis, must satisfy proportionality requirements, and must allow foreseeability on the part of the public in terms of the purposes for which their data will be processed and the uses to which such data will be put. These sorts of considerations are a recurring theme of the DPC's regulatory interactions with a whole range of public sector bodies in Ireland.

4 <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3a62020CC0245&from=EN>



In terms of those inquiries that remain ongoing, the DPC's large-scale inquiry into Facebook's transfers of personal data to the USA is of note.

In particular, it is our experience that insufficient consideration is given by such bodies to the requirement to demonstrate that a given processing operation is grounded on one or more of the legal bases expressly provided for by the GDPR and the LED. Such gaps are especially likely to be found in those cases where special category data is being processed or where data is being processed for law enforcement purposes.

In terms of those inquiries that remain ongoing, the DPC's large-scale inquiry into **Facebook's transfers of personal data to the USA** is of note. A stay imposed by the High Court on the DPC advancing its inquiry was lifted in May 2021 when the High Court rejected all of the grounds on which Facebook had sought judicial review of the DPC's decision to commence this investigation in August 2020. Following the resumption of the inquiry in the summer of 2021, submissions were received from relevant parties, the contents of which are presently under examination by the DPC. Ultimately, the DPC will be required to bring a draft decision to its fellow EU supervisory authorities as part of the cooperation and consistency mechanisms laid down by the GDPR.

The One-Stop-Shop

The GDPR's one-stop-shop has very laudable aims: to ensure a harmonised interpretation of key principles of the GDPR across all EU member-states; to ensure a consistent and level-playing field across the EU in terms of the application of the GDPR's rules; and to provide a "sole interlocutor" for multinationals operating across the EU with a view to streamlining the regulatory

and administrative challenges such entities would face if required to engage with different supervisory authorities in each member state in which they have a presence.

The one-stop-shop is doing well on the third of these three aims, one consequence of which has been to transfer a significant co-ordination function from the platforms onto the DPC, as we now engage with our colleagues across Europe on draft decisions and on projects proposed by multinationals involving cross-border processing.

As far as the first and second aims are concerned, the concept is doing less well. In part, this is because, under the arrangements legislated for by means of the GDPR, not all multinational activity in fact falls within the scope of the one-stop-shop arrangements. On the contrary, the platforms and other economic operators may choose whether they avail of one-stop-shop, or not, with significant consequences attaching to such choices. Already we have seen decisions that are difficult to reconcile being made about the same cross-border processing operations of one particular platform but by different EU supervisory authorities where neither process engaged the co-decision making procedures central to the operation of the one-stop-shop. That so much cross-border activity can sit outside the one-stop-shop brings into question the effectiveness of the coordination efforts that were intended to be a feature of the regulation of cross-border processing operations. It may also be said to undermine the idea, central to the GDPR, that a level playing field could be created across Europe (and fragmentation eliminated), by means of the implementation of a single legal framework.

New data regulation regimes

Amongst other pending pieces of legislation at an EU level, the NIS2 Directive, the Digital Markets Act, the Digital Services Act, the E-Privacy Regulation, the Artificial intelligence Act, and the Data Governance Act, demonstrate that the GDPR was never going to resolve all data issues in one single legislative instrument. Equally, the tug-of-war between “privacy” and competition rules triggered by Apple’s ATT initiative, and Google’s plans to phase out third party cookies show that for regulatory action in the “privacy” sphere, there can be an equal and opposite reaction in terms of competition regulation.

Critical, as this new suite of interlocking laws comes down the tracks, is the question of coordination at both EU and cross-regulatory levels. Structures are going to be important, particularly given the challenges that have surfaced in the operation of the one-stop-shop structures associated with the GDPR. What is clear, if hardly surprising, is that not everyone is seeing things in the same way.

Equally unsurprisingly, there are no obvious or easy answers to so many of the big issues on which political debate still rages: whether and in what ways targeted advertising could and/or should be banned; whether anonymity should be preserved in the online sphere; whether derogations should be allowed from the strict application of the rules on the confidentiality of communications in order to identify the transmission of child sexual abuse material; and how to secure global data flows while still protecting personal data, and whilst also allowing proportionate access consistent with national security requirements.

Conclusion

The DPC looks forward to continued engagement with the EU Commission, its fellow regulators across the EEA, and others, to try to reach a measure of consensus around how we measure the effectiveness of regulation and enforcement in the context of the GDPR. There are many aspects of this data era which the world hasn’t fully figured out. Equally, much progress has been made under the GDPR to better protect people’s personal data through the efforts and focus of all types of data controllers and data protection officers and through the engagement of the public with their rights. For its part, the DPC commits to progress and to roll out delivery of its 5-year Strategy grounded in the desire to do more for more people. Ar aghaidh linn!



Helen Dixon
Commissioner for Data Protection



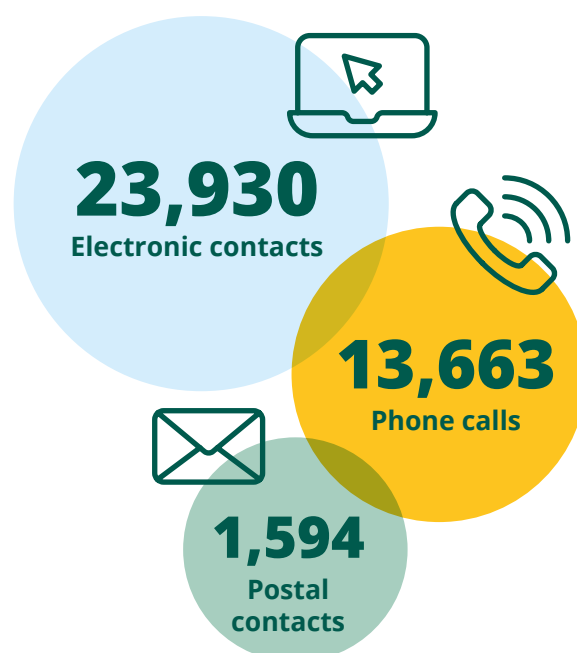
2

Executive Summary

Supporting Individuals

From 1 January 2021 to 31 December 2021:

- ▶ The DPC received in excess of **23,930** electronic contacts⁵, **13,663** phone calls and **1,594** postal contacts;
- ▶ The DPC received **10,888** queries and complaints from individuals in 2021 (an **increase of 7%** on 2020 figures) of which 8,017 had been concluded to by year end;
- ▶ The DPC received **3,419** complaints last year and concluded **3,564** complaints, including 1,884 complaints received prior to 2021;
- ▶ In total **10,645** cases - 7,081 queries and 3,564 complaints - were concluded by the DPC in 2021;
- ▶ Of the **7,499 queries** that were sent to the DPC in 2021, 6,255 had been dealt with by year-end;
- ▶ Overall the DPC **concluded 7,081 queries** last year, including 826 received prior to 2021;
- ▶ Just under **52% (1,771)** of complaints lodged with the DPC in 2021 were concluded within the same calendar year; and
- ▶ On foot of a concerted effort to bring aged access request complaints to resolution in 2021, the DPC **concluded 170% more access complaints than it received** – reversing a trend that had been in place since the GDPR came into application in 2018.



⁵ Electronic communications comprise both emails to the DPC's info@ account and webforms submitted through the DPC website.

In 2021, the most frequent GDPR topics for queries and complaints continued to be: Access Requests; Fair-processing; Disclosure; Direct Marketing and Right to be Forgotten (delisting and/or removal requests).

Supporting Industry

- ▶ Total valid breach notifications received in 2021 was **6,549**.
- ▶ Breach notifications down 2% on 2020 figures.
- ▶ Of the total recorded breach cases, **95% were concluded** in 2021 (6,274 cases).

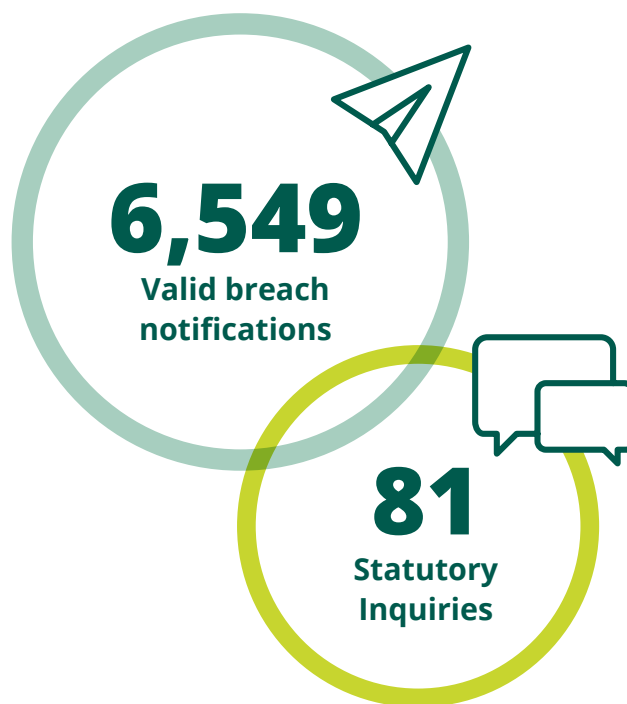
The most frequent cause of breaches reported to the DPC was unauthorised disclosure at **71%** of the overall total. This is down from 86% for the previous year.

The DPC launched a revised Breach Notification webform in 2021, increasing the ease and accuracy for stakeholders reporting breaches to the DPC.

In 2021, the DPC published its finalised **Fundamentals for a Child-Oriented Approach to Data Processing**, giving much-needed direction to organisations involved in the processing of children's data.

Also in December 2021, the DPC published its Five-Year **Regulatory Strategy for 2022-2027**, providing clarity to stakeholders as to the direction of travel for the regulatory priorities of the DPC going forward.

The DPC continued its partnership with the Croatian Data Protection Authority, AZOP, and Vrije University in Brussels on an EU-Funded project (**The ARC Project**) to provide practical supports to SMEs, with a series of **workshops** now planned for early 2022.



Regulating

As of 31 December 2021, the DPC had **81 Statutory Inquiries** on-hand, including **30** Cross-Border Inquiries.

In September, the DPC announced a conclusion to a GDPR investigation it conducted into WhatsApp Ireland Ltd. The decision was subject to an Article 65 Dispute Resolution Process, after which the **DPC imposed a fine of €225 million on WhatsApp**, in addition to an order for WhatsApp to bring its processing into compliance.

In December 2021 the DPC published its **Data Protection Audit of Political Parties in Ireland**. The report was compiled following data protection audits conducted in 2021 by the DPC in twenty-six registered political parties in Ireland.

In December 2021, the DPC settled legal proceedings with the Department of Social Protection (D/SP) on the D/SP's processing of personal data when issuing **Public Service Cards**.

Also in December 2021, the DPC sent an Article 60 Draft Decision to Concerned Supervisory Authorities. This Draft Decision concerned Instagram and was ongoing at year-end.

The DPC appeared **7** times before Oireachtas Committees and provided input and observations on over **40** pieces of proposed legislation.

In 2021 there were **9 judgments** delivered and/or final orders made in proceedings to which the DPC was a party.

Through **Supervision** action, the DPC has brought about the **postponement or revision** of **7** scheduled big tech projects with implications for the rights and freedoms of individuals.

In 2021 the DPC concluded **5** large-scale inquiries; sent forward **4** draft decisions to the Article 60 co-decision making process; referred **1** case to Article 65 on foot of which the DPC issued a finalised decision; issued a further **9** preliminary drafts of decisions for submissions to regulated entities and complainants in advance of finalisation, and sought submissions on statements of issues or inquiry reports from relevant parties in a further **17** inquiries.

Cases involving significant sanctions or corrective measures

The DPC **imposed fines and corrective measures in the following finalised cases** under the GDPR in 2021. Fines and orders were proposed in a range of other cases detailed in the Inquiries chapter, but which cannot be finalised until a consensus position is reached with other EU authorities:

Organisations	Decision Issued
Irish Credit Bureau DAC	23-Mar-21
WhatsApp Ireland Ltd	28-Jul-21
MOVE Ireland	20-Aug-21
The Teaching Council of Ireland	02-Dec-21
Limerick City and County Council	09-Dec-21

Engaging with Civil Society

In 2021, the DPC concluded an extensive consultation on its draft guidance on the rights of **children as data subjects**. The finalised guidance document - **Fundamentals for a Child-Oriented Approach to Data Processing** – was published in December 2021.

In December 2021, the DPC published its **Regulatory Strategy for 2022-2027**, which will be the roadmap for the DPC through a period of transformative change. The DPC has set out an ambitious vision for what it believes will be five crucial years in the evolution of data protection law, regulation and culture.

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

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

Engaging with Peers

Since 1 January 2021, the DPC:

- ▶ Responded to **over 600** Article 61 Mutual and Voluntary Mutual Requests for assistance from other European Regulators;
- ▶ Attended over **200** EDPB meetings, most of which were conducted virtually due to pandemic-related travel restrictions;
- ▶ Continued to have representatives on all European Data Protection Board (EDPB) subgroups; and
- ▶ Regularly met with senior regulators from the Broadcasting Authority of Ireland, ComReg and the Competition and Consumer Protection Commission to **drive regulatory coherence** and foster greater understanding of the respective regulatory roles.

Mainstreaming Data Protection

Staff of the DPC presented at over **90** speaking events in 2021. As Covid restrictions came into effect, the majority of staff participation was conducted online, except where public health guidance permitted.

The DPC remains committed to driving awareness of data protection rights and responsibilities, producing **10** substantive pieces of guidance, including the very significant Fundamentals for a Child-Oriented Approach to Data Processing, which was very well received by stakeholders.

Other Activity

In 2021 the DPC:

- ▶ Concluded **138 electronic direct marketing** investigations;
- ▶ **Prosecuted two telco companies** for persistently contacting customers who had opted out of correspondence;
- ▶ Implemented the first release of the new DPC **case management system**;
- ▶ Worked to finalise the inter-agency agreement between the DPC and Irish National Accreditation Board on accreditation of **certification schemes** under GDPR Articles 42 and 43;
- ▶ Worked closely with EU colleagues on the first approvals of a proposed **EU Seal** and a member state based certification scheme, in accordance with Articles 43 and 43 of the GDPR;
- ▶ Produced a new **ICT strategy** for the DPC; and
- ▶ Handled **49 Law Enforcement Directive** complaints.





3

Mission, Vision and Values at the DPC



Mission

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

The 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**

4

Regulatory Strategy

In December 2021, the DPC published its Regulatory Strategy for 2022-2027, which will be the roadmap for the DPC through a period of transformative change. The DPC has set out an ambitious vision for what it believes will be five crucial years in the evolution of data protection law, regulation and culture.

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

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

In developing this Regulatory Strategy for 2022-2027, the DPC has been careful to give conscientious thought to the needs and insights of its stakeholders, the legislation under which it must regulate, the context in which it currently operates and the various future states for which it must prepare. In addition to iterative rounds of broad public consultation, the DPC has also taken account of the academic theories that are emerging in respect of effective regulation and behavioural economics. This research has then been balanced against the recognition that the DPC's resources are finite and must be put where they can do the most good, which means that discerning regulatory choices must be made.

The breadth of the DPC's regulatory remit cuts across all areas of personal and public life; both at national and international level. In order to develop a Regulatory Strategy that will provide effective direction for such a vast operational remit, the DPC has been careful to take account of the wider context in which it regulates, the needs of its diverse stakeholders and the evolving nature of the fast-paced and non-traditional sectors it regulates.

This Regulatory Strategy is being implemented in the very early years of radically reformed data protection legislation – in the form of the GDPR and ancillary Law Enforcement Directive – along with all the attendant interpretative challenges that such immense regulatory change usually produces. These challenges, against a backdrop of hugely increased public consciousness of data protection, have given rise to ambiguities of interpretation and application of the law that the DPC – along with its peer data protection authorities – must work to clarify.

No action or approach outlined in this Regulatory Strategy – from the handling of complaints to the emphasis on strategic engagement – has arisen from a desire to do 'less' for stakeholders. The opposite is the case, and all strategic goals have been proposed as a means of doing more, for more.

The Strategy is arranged according to fundamental goals, underpinned by the DPC's mission, vision and values, which collectively contribute to the delivery of its strategic priorities. The DPC recognises that it cannot achieve its ambitions alone – new partnerships and new ways of engaging will be necessary as we look towards a future of closer convergence. The work to underpin this regulatory convergence is already underway, with regular meetings in 2021 between the senior regulators from DPC, the Broadcasting Authority of Ireland, ComReg and the Competition and Consumer Protection Commission to drive regulatory coherence and foster greater understanding of the respective regulatory roles.

In order to prepare this Regulatory Strategy, the DPC has engaged in a period of iterative consultation with a broad range of stakeholders, both internal and external, gathering insights and experiences of how the application of the General Data Protection Regulation (GDPR) has impacted the lives of individuals and organisations operating across a wide range of sectors. In late June 2021, the DPC closed its final open call for submissions to its regulatory consultation on the Draft Strategy itself. The breadth of the DPC's stakeholder body was reflected in the submissions received.

It is clear from the depth of thought given to these submissions that the GDPR is a matter of vital interest for many people. As is the case with any far-reaching legislation, the various interpretations from stakeholders of how best to apply the GDPR are not always in sympathy with each other. Nonetheless, the DPC is tasked with extracting the commonalities from these disparate points of view, and identifying an agenda of regulatory priorities which will drive compliance and promote better data protection outcomes for EU individuals. That overarching objective – to do more, for more – has underpinned the strategic choices made in this Strategy, as the DPC navigates a regulatory future replete with competing priorities.

5

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.

The SMC comprises:



Helen Dixon
*Commissioner for
Data Protection*



Anna Morgan
*Deputy Commissioner
- Head of Legal*



Colum Walsh
*Deputy Commissioner
- Head of Regulatory
Activity*



Dale Sunderland
*Deputy Commissioner
- Head of Regulatory
Activity*



Graham Doyle
*Deputy Commissioner
- Head of Corporate
Affairs, Media and
Communications*



John O'Dwyer
*Deputy Commissioner
- Head of Regulatory
Activity*



Tony Delaney
*Deputy Commissioner
- Head of Regulatory
Activity*



Ultan O'Carroll
*Deputy Commissioner
- Head of Technology,
Operational and
Performance*

DPC's Senior Team

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

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. As a Vote body, the Accounting Officer must prepare the Appropriation Account for the DPC's Vote for submission to the Comptroller and Auditor General. As required, this includes the Accounting Officer's statement on the DPC's systems of internal financial control. During 2021, the Office of the Comptroller and Auditor General completed an audit of the DPC Appropriation Accounts for 2020. The DPC is pleased to confirm that no matters gave rise to any adverse comments being included in the report.

The 2021 gross estimate provision for Vote 44 — Data Protection Commission was €19.128m (2020: €16.916m) of which €12.764m (2020: €10.552m) was allocated for pay-related expenditure, and €6.364m (2020: €6.364m) of which was allocated to non-pay expenditure. The funding for 2021 represented an increase of €2.2m on the 2020 allocation. The DPC is currently preparing the Appropriation Account for 2021 and this statement will be published on the DPC's website following the conduct of an audit by the Office of the Comptroller and Auditor General.



6



Contacts, Queries and Complaints

Contacts

Stakeholders contact the DPC in a variety of ways, including the DPC Helpdesk phone lines, online webforms, email and post. In 2021 DPC staff worked remotely, in keeping with the public health advice from Government. Despite this, full phone line services were maintained and arrangements put in place to collect and redirect any post arriving to the DPC offices in a timely manner.

In 2021 the DPC received **23,930** electronic contacts⁶, **13,663** phone calls and **1,594** postal contacts.

Despite the challenges that full remote-working posed, DPC productivity in frontline services was maintained throughout the year. No negative effect on response times or service levels was incurred, and productivity was consistent with pre-Covid rates.

The DPC **received 10,888 queries and complaints** from individuals in 2021 (an increase of 7% on 2020 figures) of which 8,017 had been concluded to by year-end. In total **10,645** cases - 7,081 queries and 3,564 complaints - **were concluded** by the DPC in 2021.

Of the 7,499 queries that were sent to the DPC in 2021, 6,255 had been dealt with by year-end. Overall **the DPC concluded 7,081 queries last year**, including 826 received prior to 2021.

The DPC **received 3,419 complaints** last year and **concluded 3,564 complaints**, including 1,884 complaints received prior to 2021. Just under 52% (1,771) of complaints lodged with the DPC in 2021 were concluded within the same calendar year.

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

Complaints

The DPC processes complaints under two main legal frameworks:

- ▶ Complaints received from 25 May 2018 onwards (and which relate to matters which occurred on or after 25 May 2018) are dealt with under the GDPR, Law Enforcement Directive, and the Data Protection Act 2018; and
- ▶ Complaints and infringements occurring before 25 May 2018 are dealt with under the Data Protection Acts 1988 and 2003, even where they are notified to the DPC on or after 25 May 2018.

To constitute a complaint – and therefore trigger the DPC’s statutory complaint-handling obligations – the matter must fall under one of the following headings:

- ▶ A complaint from an individual relating to the processing of their own personal data;

- ▶ A legally authorised person or entity complaining *on behalf of an individual* (e.g. a solicitor on behalf of a client or a parent/guardian on behalf of their child); or
- ▶ Advocacy groups which meet the requirements to act *on behalf of one or more individuals* under the GDPR, LED and the Data Protection Act 2018.

Between 1 January 2021 and 31 December 2021:

- ▶ The DPC received 3,389 complaints from individuals under the GDPR and 30 complaints under the Data Protection Acts 1988 and 2003.
- ▶ Overall, the DPC concluded 3,665 complaints, including 1,884 complaints received prior to 2021.
- ▶ Almost 52% of complaints lodged with the DPC in 2021 were concluded within the same calendar year.

Complaints Received under the GDPR - Top 5 Issues in 2021	No	% of total
Access Request	1,232	42%
Fair Processing	560	19%
Disclosure	291	10%
Right to erasure	263	9%
Direct Marketing	128	4%

Complaints Received under the Data Protection Acts 1988 and 2003 – Top Five Issues in 2021	No	% of total
Access Request	11	37%
Fair Processing	11	37%
Disclosure	6	20%
Security	1	3%
Fair Obtaining	1	3%

Complaint Handling

Where possible, the DPC endeavours to resolve individual complaints amicably – as provided for in Section 109(2) of the Data Protection Act 2018. The option to have their issue dealt with by amicable means is afforded to individuals throughout the lifetime of their complaint, regardless of how far the issue may have progressed through escalated channels. Case studies illustrating these escalated channels in operation can be found at the end of this chapter.

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

“Fast-Track” Amicable Resolution

Amicable Resolution includes facilitating amicable resolution between an individual and a data controller, executing certain complaint handling powers to resolve complaints both efficiently and appropriately and transferring certain cases to other relevant complaint handling units where there is a need for more in-depth/complex activities to be carried out. In certain cases, where the DPC identifies the possibility of swift resolution, it proceeds down a “fast-track” basis. Of the 3,564 complaints concluded by the DPC in 2021, **463** of those complaints were concluded by fast-track amicable means. In excess of 3,100 further complaints were also resolved but required a higher number of iterative contacts between the parties to achieve.

The Data Protection Acts 2018, Section 109(2) states that the Commission (DPC), where it considers that there is a reasonable likelihood of the parties concerned reaching, within a reasonable time, an amicable resolution of the subject matter of the complaint, may take such steps as it considers appropriate to arrange or facilitate such an amicable resolution.

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

Access Rights Complaints

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

The right of access is one of the fundamental rights conferred on individuals by the GDPR. That said, an individual’s right of access is not absolute and may be subject to certain restrictions, including but not limited to those set out at Sections 60 of the Data Protection Act 2018

By the end of 2021, the DPC had received **331** new access complaints and concluded **562**. This represents a complete inversion of the access complaints received : complaints concluded ratio. Since the GDPR came into application in 2018, the DPC has, year-on-year, received more cases per annum than it concluded. The DPC successfully reversed this trend in 2021 and **concluded 170% more access cases than it received**.

In addition, the DPC is still investigating access complaints under the old Data Protection Acts, 1988 and 2003, of which **8** were concluded in 2021. Access request related complaints remain the most frequent complaints received by the DPC.

Often the individual will have been in communication with the data controller but either did not receive an acknowledgement/response to their request or was dissatisfied with the response issued and as a result lodge a complaint with the DPC.

When the DPC investigates these complaints, it often transpires that the data controller has either (a) not performed an adequate search for the personal data (b) has not advised the individual they are withholding data and the exemption they are relying on for same, or (c) will not respond within the required timeframe to the access request.

The DPC uses the knowledge gained from handling these complaints to build a picture of how data controllers are applying the data protection principles within their organisation and through their policies and practices.

The DPC is concerned that it has identified a pattern where data controllers are not responding to subject access requests received from data subjects and/or not responding to complaint commencement correspondence by the DPC. In 2022 the DPC intends to increase its enforcement in this area and target non-responses and inadequate responses from data controllers.

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 **138** new complaints in relation to electronic direct marketing in 2021. These included some 84 complaints in relation to email messages, 43 complaints in relation to text messages, and 11 complaints concerning phone calls. A total of **150 electronic direct marketing investigations were concluded** in 2021.

This figure is made up of:

- ▶ 1 complaint from 2018;
- ▶ 5 complaints from 2019;
- ▶ 58 complaints from 2020; and
- ▶ 86 complaints from 2021.

On a matter of topical interest in relation to the current pandemic, it is interesting to note that during 2021 the DPC received three complaints against hotels where the complainants had provided their details for contact tracing purposes. In response to the DPC's investigation, the hotels in question confirmed that the mobile telephone numbers of the complainants were collected for contact tracing purposes and erroneously included in direct marketing contact lists. All three complaints were concluded with a warning against the hotels concerned.

Cookies Investigations

During 2021 the DPC continued to carry out cookies investigations, examining a significant number of websites to assess compliance with the relevant legislation, i.e. Regulations 5(3), 5(4) and 5(5) of the ePrivacy Regulations (S.I. 336/2011). That legislation provides that consent must be obtained for placing any information on a user's device, or accessing information already stored on their device, unless one of two limited exemptions are met. It is important to note that the law applies not only to websites, but also to mobile apps and other products that use cookies or similar tracking technologies that access a device.

It was notable during the year that the DPC continued to receive complaints and concerns from members of the public about the use of cookies and tracking technologies, and these complaints and concerns were examined and investigated where necessary. Issues targeted by the DPC this year have included the setting of tracking and advertising cookies without consent, the use of cookie banners that obscured the text of the cookies and privacy notices on websites, and the use of pre-ticked boxes or toggles to signal consent for cookies.

Investigations and enforcement in this area will continue to be a key element of the DPC's activities in 2022 and in the coming years. Of note is the fact that EU lawmakers have not yet concluded an updated e-privacy law for Europe. The DPC continues to regulate under the existing EU e-Privacy Directive as transposed under SI No. 336 of 2011 in Ireland. No fines can be imposed by DPC and violation of cookies requirements are not an offence under the SI. The DPC must therefore use a circuitous route of demonstrating to the website operator that the SI is not being complied with, then impose an Enforcement Notice if voluntary compliance has not been secured and only if that is not complied with, prosecute for failure to comply with a DPC Notice. The legislation urgently needs to be updated if more resource-efficient and effective enforcement is to be achieved.

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 requires that these organisations are 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. Since 2018, the DPC has received 1,150 valid cross-border processing complaints. The table below illustrates the proportional breakdown of those **1,150 OSS complaints** into 'Lead Supervisory' and 'Concerned Supervisory' roles for the DPC.

Of the 969 complaints where Ireland acted as Lead Supervisory Authority, **65% (634) have been concluded**.

As a Concerned Supervisory Authority the DPC reviewed **47** draft decisions from other European supervisory authorities in 2021. Of the 47 draft decisions circulated in 2021, only 12 were sent to all supervisory authorities, including four that were circulated by Ireland. Further information on these draft decisions can be found in the chapter on Inquiries. The DPC lodged no objections against any of the draft decisions it received.

Data-Breach Complaints

The DPC handled **187** complaints relating to both notified and non-notified data breaches in 2021. The majority of these complaints arose from a breach being communicated to the affected individual by the organisation. Where a breach has been notified to the individual by the data controller but not to the DPC, the DPC will ensure the breach is retrospectively reported and formally recorded, accompanied by a clarification from the data controller/processor as to why the DPC was not notified in the first instance.

When assessing the necessity of notifying breaches, the DPC advises data controllers that particular focus is given to the impact of a data breach on the rights and freedoms of an affected individual.

Most data breach complaints concerned the personal data of an individual inadvertently being issued to another third party in error. The DPC has found that when informing an individual that their personal information has been breached, the explanation provided by the data controller is often not sufficient to put the mind of the impacted individual(s) at ease. The DPC has found that organisations who take the time to properly update affected individuals ultimately resolve the matter sooner, sometimes negating the need for the DPC to become involved at all.

DPC Competency	No of complaints	%
DPC as Lead Supervisory Authority 1	969	84%
DPC as Concerned Supervisory Authority 2	181	16%
Total	1,150	100%

1 – Complaints lodged by individuals with other EU data protection authorities and passed to the DPC under the OSS, and complaints lodged directly with the DPC.

2 – Complaints lodged with the DPC and transferred to another EU data protection authority as the LSA for the organisations concerned.

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 2021, the DPC handled 49 LED complaints, the majority of which entailed 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.

A data controller may restrict data subject rights for one or more of the purposes set out in Section 94 of the Act. In some cases handled the DPC will approach the data controller in relation to the restrictions cited and, as a result of its intervention, the individual will be provided with additional personal data by the data controller. In many other cases, the DPC will agree with the restrictions imposed, following an examination of the legal basis for withholding the data in question.

Rapid Direct Intervention

Issues of concern from a data protection perspective may come to the attention of the DPC and give rise to rapid direct intervention by the DPC rather than the setting up of an inquiry targeted at enforcement action. This approach is taken to ensure a timely response in the interest of affected data subjects.

Matters examined by the DPC in 2021 included:

- ▶ CCTV in school toilets.
- ▶ CCTV in gyms.
- ▶ Security of files.
- ▶ Publication of photographs of minors on website.

- ▶ Auctioneers collecting excessive personal data from people wishing to view properties (see below).
- ▶ Hospitality sector- collection of personal data for Covid purposes on display in a public area.

Of particular concern to the DPC during 2021 were media reports regarding Savills Ireland and practices concerning the seeking of excessive personal data from persons wishing to view properties at a new housing development in Dublin. In order to view a property, Savills Ireland were requesting that prospective buyers submit their full proof of funds for the full purchase price for the property, including evidence of mortgage approval, bank statements, evidence of savings or gifts.

In response to concerns raised regarding this practice, Savills informed the DPC that the reasoning behind seeking such information was in the context of Covid-19 restrictions, whereby property viewings could only take place by appointment. According to Savills Ireland, the information requested was intended to help 'triage' applicants prior to scheduling sales appointments and ensure that prospective viewers attending the appointments could be designated as 'qualified buyers' who could realistically purchase a property in the development. Savills highlighted that such practices were introduced as a result of pandemic-related restrictions and that previously, open viewings would take place with no personal data required in advance of a viewing.

Savills referred the DPC to guidance issued to property services providers jointly by the Property Services Regulatory Authority (**PSRA**), the Society of Chartered Surveyors Ireland (**SCSI**) and the Institute of Auctioneers and Valuers (**IPAV**) with regard to viewings when Covid-19 restrictions were in force.

Having reviewed matters overall, the DPC did not consider there to be any justification (Covid-19 related restrictions included) for the extensive collection of personal data such as financial statements or proof of funds from prospective buyers at the initial stages of advertising or hosting viewings of a property. Following the intervention of the DPC, Savills immediately deactivated the online questionnaire.

In view of Savills Ireland response and the potential of other estate agents seeking similar and additional information such as utility bills and PPS numbers, the DPC published sectoral guidance.

Complaints under the Data Protection Acts 1988 & 2003

The DPC continues to receive and examine complaints that fall under the remit of the Data Protection Acts 1988 & 2003. The DPC received **30** cases in 2021 which were deemed to fall under the remit of the 1988 & 2003 Acts. Under both the 2018 Act and the 1988 & 2003 Acts, it is the statutory obligation of the DPC to strive to amicably resolve complaints that are received from members of the public. Throughout the last year, the vast majority of complaints falling under the 1988 & 2003 Acts were concluded amicably between the parties to the complaint without the necessity for issuing a formal decision under Section 10 of the 1988 & 2003 Acts. The Commissioner has issued **31** formal decisions under the Data Protection Acts 1988 & 2003 since January 2021 of which **16** fully upheld the complaint and **9** rejected the complaint.



Case Studies

Case Study 1

Content absent from an access request (Amicable Resolution)

The DPC received a complaint from an individual regarding a subject access request made by them to a data controller for a copy of all information relating to them. The data controller was involved in car park management and a dispute had arisen following the clamping of the individual's vehicle. The clamping incident was the subject of an appeal to the National Transport Authority. The individual did not receive any response from the data controller.

The individual was subsequently provided with their personal data but did not consider that the data provided to them was complete. Following the intervention of the DPC, further searches were undertaken and the data controller identified additional data which was released to the individual.

The individual remained unsatisfied as they had not been provided with a copy of a particular email which they had sent to the data controller. They stated that it was important for their appeal that they were able to prove that the data controller had received the email in question. The data controller subsequently provided this office with a report from the company which hosts its email services showing that the email in question was received but was quarantined as suspected spam and did not reach any of the intended mailboxes nor was it opened by any persons within the organisation.

This email was then automatically deleted from their servers after 14 days. The data controller also provided screenshots from searches conducted of each of the intended mailboxes, which did not return the email in question.

Article 12(3) of the GDPR states that "the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request."

Having examined the matter thoroughly, it was apparent to the DPC that the data controller did not comply with its obligations under article 12(3) of the GDPR as it had an obligation to provide a response to the individual's subject access request within the statutory timeframe, and the data provided to the individual in this case was provided outside of this timeframe. Regarding the email which was quarantined by the data controller's system, it was clear that this email was not in existence at the time the access request was made. When making decisions around the quarantine of emails, the controller must have due regard to security obligations in line with Article 32 but also ensure that it does not infringe on the rights of individuals. In this case, there was no apparent right interfered with through the initial quarantine and deletion of the email in question.

Case Study 2

Requests for identification when responding to access requests (Amicable Resolution)

A complaint was received from an individual who had submitted an access request to a hotel (the data controller) for a copy of all information relating to them. The hotel asked the requester to provide a copy of a utility bill and a copy of photo ID verified by An Garda Síochána. The DPC asked the data controller to set out the particular concerns it had regarding the identity of the requester in circumstances where the postal address and email address being used by the requester were the same as those provided by them during the booking and check-in process at the hotel. The data was subsequently released to the requester.

In relation to the general approach to requesting ID where data subjects seek to exercise their rights, controllers should only request the minimum amount of further information necessary and proportionate in order to prove the requester's identity. Seeking proof of identity would be less likely to be appropriate where there was no real doubt about identity; but where there are doubts, or the information sought is of a particularly sensitive nature, then it may be appropriate to request proof.

Bearing in mind the general principle of data minimisation, seeking more information than that already held as a means of proving identity is likely to be disproportionate. A request for official ID is only likely to be proportionate to validate identification where the category of information relating to that individual is sensitive in nature and where the information on the official ID can be corroborated with the personal data already held by the data controller such as a photo, address or date of birth.

The categories of personal data held and the likelihood of the risks associated with its release should be considered on a case-by-case basis to determine the minimum level of information required. Where no special category personal data is held, confirmation of address may be sufficient. In cases where there is in fact special category personal, additional information may be proportionate but only that which would be sufficient to confirm identity, having regard to the data already being processed.

Case Study 3

Processing of footage of funeral service by parish church

(Applicable Law – GDPR & Data Protection Act 2018)

An individual made a complaint against a parish church regarding the processing of the individual's personal data arising from the live streaming and recording of a family member's funeral service that the individual had attended. The individual also complained about a lack of transparency that the recording was taking place.

The individual complained to the DPC about the parish church's response to their concern around the use of live streaming and recording for funeral services. In our examination of the complaint, the DPC engaged with the parish church to ascertain their lawful basis for processing and for clarification on their response to the data complaint. The parish church informed the DPC that live streaming of funeral services was used during Covid-19 restrictions and that they record funeral services when requested to do so by family members, which did happen in this complaint, usually when one cannot attend the funeral. The parish church informed the DPC they use one camera in a fixed location to make these recordings and for live streaming. The parish church removes the recordings from their website at the end of 30 days. The parish church apologised to the individual for any distress caused and particularly for not informing the individual of the 30 days only retention period. The parish church informs attendees at the beginning of services that they will be

live streamed and have signs with this information at their entrance doors. The parish church implemented changes because of this complaint, including informing attendees during a service that it is being live streamed, including information on their live streaming and recording in parish newsletters and on their website, only responding to written requests for recordings and password protecting the recordings in future.

The DPC wrote to the individual and advised them under section 109(5)(c) of the 2018 Act that the parish church and those unable to attend a funeral service had a legitimate interest to view the service by live stream or recording. The DPC noted the 30-day retention period of the footage, the fixed restricted view of the camera and the changes the parish church had made arising from this complaint, including requiring a request for recording to be made in writing and password protecting these recordings. The DPC advised the individual that the response of the parish church was reasonable in the circumstances of this complaint and noted that the recording was requested by another family member of the deceased. Nevertheless, the DPC recommended under section 109(5)(f) of the 2018 Act that the parish church update the privacy policy available on its website with more information on the live streaming and recording of funeral services.

Case Study 4

Use of location data to verify expense claims

The complainant in this case study was a former employee of a statutory service provider, whose work involved driving to locations assigned by his employer. Where this gave rise to claims for overtime or subsistence, the complainant would complete forms provided by the employer, detailing items such as relevant dates and places, dispatch reference numbers, and the amounts claimed.

The employer made use of a dispatch system intended to ensure the most efficient use of drivers and vehicles, particularly as they provided response in emergency situations. This system logged the performance and completion of service calls, when vehicles were out on calls or back at base, and when drivers were on or off duty.

The complainant had made a claim for overtime and subsistence. The employer rejected this because of inconsistencies between the details on the complainant's claim form and those recorded on the employer's dispatch system. The complainant objected to the use of data from the dispatch system for this purpose and complained to the DPC.

The DPC considered whether the use of data from the dispatch system to verify overtime and subsistence claims was in line with fair processing requirements. The fairness of the processing was to be assessed by reference to whether the complainant and fellow employees had been made aware of the employer's use of the data for that purpose, whether that processing was compatible with the purpose for which the data was collected, and whether the employer had a legal basis for that processing.

The employer did not have a written policy on the use of the dispatch system. Instead, it relied on the "general awareness" of employees that the system was used for that purpose.

The employer pointed out that such use had been noted in an arrangement with its employees' trade unions some years previously. The DPC noted that overtime and subsistence claims required employees to include relevant dispatch reference numbers from the dispatch system.

The DPC took the view that the inclusion of relevant dispatch system reference numbers in overtime and subsistence claims indicated that employees were aware that the data was used not just for logistical processing but also to verify their claims. Even if the major purpose of the dispatch system was to aid logistics, its use to verify overtime claims was not incompatible with that purpose, as that data was the only means available to the employer to verify claims.

The DPC noted that applicable financial regulations required the employer to verify overtime and subsistence claims. The processing to verify overtime and subsistence claims was necessary not just to comply with that legal obligation, but to perform the complainant's employment contract and for reasons of legitimate interests of the employers.

This case is an example of when data collected for one legitimate purpose – in this case, logistical control – may be appropriately processed for another, in this case verifying overtime claims. However, controllers should bear in mind the overarching requirement to process personal data fairly and must ensure that data subjects are made aware of what data is collected, and the nature and purpose of the processing. Equally important is that the processing have a legal basis, which in most cases will require that the processing is necessary for the stated purpose.

Case Study 5

Unauthorised disclosure in a workplace setting (1)

The complainant alleged that insecure processing by his former employer had made his personal data accessible to unauthorised persons, including former colleagues and external third parties.

The complainant was in legal dispute with the company arising from his dismissal. In connection with that dispute, the company had prepared documents including an internal investigation report and a legal submission to the Workplace Relation Commission (WRC). While the WRC submission did not contain a great deal of the complainant's personal data, the internal investigation report did.

Approximately one month before the complainant first contacted the DPC, the company had notified the DPC of a data breach. The notification stated that the WRC submission had been inadvertently stored on a folder accessible by all employees, rather than on one that was accessible only by authorised HR staff. The error was noticed and corrected two days later, and the company notified the DPC shortly thereafter. The company's systems did not record whether, when or by whom the WRC submission might have been accessed, or whether it had been copied or printed.

In the complaint, the complainant alleged that the breach affected not just the WRC submission but also the internal investigation report, and that these had been accessible from all parts of the company's intranet, including on a device that could be used by both employees and visitors to the company's premises. The complainant submitted statements from former colleagues who described having access to documents relating to "the internal investigation." The company denied that the internal investigation report had ever been accessible by unauthorised persons.

It also maintained that, while the WRC submission had been inappropriately available for a short time on the company's intranet, it was not on a part of it accessible to non-employees.

The DPC addressed two main issues: what had been the content and extent of the breach, and whether the company's security measures had met the standard required by applicable data protection legislation.

The complainant's former colleagues had said that documents concerning "the internal investigation" had been accessible by them. However, these statements had not described in any detail the nature or contents of the documents, did not say when or by whom they had been seen, and did not say that the documents were accessible by non-employees. Against that, the company had consistently maintained that the WRC submission, but not the internal investigation report, had been inappropriately accessible to employees for a number of days. Significantly, the company had notified the DPC of that approximately one month before the complainant had first lodged his complaint. The DPC took the view that there was insufficient evidence to support the claim that the internal investigation report had been disclosed, or that the complainant's personal data had been accessible by non-employees as well as unauthorised employees.

Concerning the company's security measures, the DPC noted that the applicable standard had to reflect and mitigate the harm that could be caused by relevant risks including, as in this case, disclosure to unauthorised persons. The company was clearly aware of the risk of disclosure, as it had arranged for confidential documents to be stored in a way that gave access only to authorised HR staff.

Continued overleaf ►

However, the company had failed to properly anticipate and mitigate the risk of human error in storing such documents, as had happened to the WRC submission. The DPC also reminded the company of the need to ensure that relevant personnel are aware of the need to handle personal data in accordance with applicable security measures, and to respond to breaches accordingly.

This case illustrates how data controllers must consider all risks that can arise when they process personal data, including the risk of human error. The measures that they adopt to address those risks must reflect not just the possible causes of loss or harm, but also the consequences of a breach, and the ways in which those consequences can be minimised or remedied.

Case Study 6

Lack of appropriate security measures unauthorised disclosure in a workplace setting (2)

The DPC received a complaint against an employer, a manufacturing company, asserting that their private information including attendances with the company doctor, details of a personal injury claim being pursued against the company and details of a disciplinary procedure taken against the complainant had been placed on the company's shared 'C-Drive', available to be viewed by anyone within the company, and that a copy of the data on a CD-ROM was also left on the complainant's desk.

It became apparent during the examination of the complaint that a number of workplace computers had been used to access the data on the shared drive, which the company stated was downloaded, copied or sent to an external email address. The organisation advised that it had carried out an investigation of the incident resulting in two employees, identified as having a significant role in the incident, having their employment terminated and that An Garda Síochána had been notified about the incident. The company notified the DPC of the breach incident outlining that certain data was accessed and viewed by at least two of its employees.

It was stated that the data was being transferred internally from its Human Resources (HR) department to its Legal department due to the imminent departure of one of its HR employees. During the transfer a large volume of electronic files relating to legal cases involving a large number of individuals had the potential to be accessed and viewed by employees who would not ordinarily have access to these.

The implementation of measures to protect and secure personal data are foundational principles of data protection law particularly in terms of ensuring there is no unauthorised access to or destruction of personal data.

With regard to this specific complaint, the DPC observed firstly that the information in respect of the complainant which was disclosed as part of the data breach included very sensitive information, and which constituted "special category data", in circumstances where special category data includes information about "data concerning health or data concerning a natural person's sex life".

Continued overleaf ►

The information (examples of which were provided to this office) included details of attendances with the company doctor which revealed very personal and sensitive information about the complainant's physical health, mental health and their personal circumstances. It was noted that this information was being maintained by the company in the context of legal proceedings/claims being taken by the individual. Given the nature of the information, there was a particularly strong onus on the company to ensure that only those who needed access to such information were granted and so could access and process same.

The issue regarding this complaint was the placing of files to include the complainant's personal information on a shared drive accessible to all employees. The DPC considered that due regard was not given to the sensitivity of the information contained in the files and the risks entailed with making them available to any employee of the company, even if this was only for a very short period of time. It would seem that the decision to transfer the files to the shared drive was taken for pragmatic reasons, i.e. the company confirmed it was executed in this manner as the files were too large to be sent by email.

However, this did not justify the placing of the files somewhere where any employee of the company would be able to access them, particularly given the risk of harm to the data subject if colleagues of theirs were able to find out very personal and sensitive information which the complainant may, quite legitimately, not have expected or wanted other employees to know, save to the extent that it was strictly necessary for limited employees to know in relation to legal proceedings/claims between the data subject and their employer. Moreover, there were a number of alternative options in transferring the files to the Legal department which would not have presented the same risk to the security of the personal data, including placing the files on a folder, whether on the shared drive or otherwise, where access was restricted to limited individuals. That such alternative options might have been more time-consuming or difficult to implement were no justification for the placing of the files on the shared drive with unrestricted access to other employees.

The fall-out of the failure to protect personal data in this case was considerable giving rise to legal proceedings against the company by the affected individual, the loss of two long-term employees who were dismissed not to mention the impact on the individual whose data was disclosed.

Case Study 7

Delisting request made to internet search engine

(Applicable Law – GDPR & Data Protection Act 2018)

A data subject made a complaint against an internet search engine regarding the search engine's response to their delisting request. The complaint concerned two URLs that appeared as results to searches of the individual's name on the search engine. During the handling of this complaint, the individual included one further URL that they sought the search engine to delist.

The criteria to be applied by search engines is that delisting must occur if the results are irrelevant, inadequate or excessive. A case-by-base balancing exercise must be conducted by the search engine that balances rights of access and rights of those individuals affected by search results.

The individual had originally personally engaged with the search engine seeking delisting of the URLs because the individual argued the URLs contained defamatory content, making it unlawful to process them, and that the URLs were impacting on the individual's private and professional life given their content. The search engine operator refused to delist the URLs because they related to information about the individual's professional life and there was a public interest in accessing this information.

The DPC engaged with the search engine operator regarding their refusal to delist. The search engine operator relied on the legitimate interest of third parties to access the information in the URLs. No defamation proceedings had been pursued by the individual against the original publishers of the relevant content and so it was not possible to definitively decide the question of whether content in the URLs was defamatory or not.

That being said, during the course of the handling of this complaint by the DPC, the search engine operator delisted the URLs in Ireland alone based on the defamation arguments of the individual. The individual continued with their DPC complaint seeking delisting across Europe and not just Ireland. Further, the webpages underlying all of the three URLs were deactivated by the webmaster during the handling of this complaint.

Article 17(3)(a) of the GDPR states the right to be forgotten will not apply where the processing of personal data is necessary *"for exercising the right of freedom of expression and information"*. In examining this complaint, the DPC noted the information contained in the webpages - the subject of the individual's complaint - relates to previous business conduct by them relevant to their professional life. The individual continues to engage in the same professional sphere and activities. The individual accepted this by arguing the content was impacting their professional life. The individual argued the content was inaccurate because it was defamatory. The DPC noted that a significant majority of the content the individual said was inaccurate was a blog post and comments of third parties and related to their professional activities; appearing to be the opinions of third-party commentators. The DPC concluded if a third party were to consider the webpages the subject of this complaint it would be clear that the comments were made as user-generated content and represent third party opinions rather than appearing as verified fact. The role of the search engine in listing is not to challenge or censor the opinions of third parties unless to list results gives rise to personal data processing on the part of the search engine that is irrelevant, inadequate or excessive.

Continued overleaf ►

The DPC concluded that given the individual's business role and role in public life arising from their professional life, there is a public interest in accessing information regarding their professional life within the European Union.

The DPC wrote to the individual and under section 109(5)(b) of the 2018 Act dismissed the individual's complaint based on the above considerations.

Case Study 8

Department of Employment Affairs and Social Protection – Independence of the DPO

(Applicable Law – GDPR & Data Protection Act 2018)

The DPC commenced this Inquiry after receiving a complaint from Digital Rights Ireland alleging interference with the independence of the Data Protection Officer (DPO) in the Department of Employment Affairs and Social Protection (DEASP) (now the Department of Social Protection – D/SP) in the context of the D/SP's amendment to its Privacy Statement on 6 July 2018, in which it removed the only reference to its processing of biometric data from the Statement. The decision considered whether the Department's DPO was involved in the issue of amending the Privacy Statement in a proper and timely manner in accordance with Article 38(1) of the GDPR; and whether the DPO received instructions regarding the exercise of his tasks contrary to the requirements of Article 38(3) of the GDPR.

The scope of the inquiry did not concern whether the Department's amendment complied with its transparency obligations under the GDPR. Having regard to all of the relevant information, the DPC found that the Department involved their DPO, properly and in a timely manner, in the Department's amendment to its Privacy Statement as implemented on 6 July 2018. Therefore, the Department did not infringe Article 38(1) of the GDPR in the circumstances. The decision also found that the Department did not provide any instructions to the DPO regarding the exercise of the tasks referred to in Article 39 of the GDPR in respect of the Department's amendment to its Privacy Statement as implemented on 6 July 2018. Therefore, the Department did not infringe Article 38(3) of the GDPR in the circumstances.

Case Study 9

Data restrictions – absence of consent from all parties (Law Enforcement Directive)

In one case examined by the DPC, a parent applied to An Garda Síochána for copies of the personal data of his young children.

An Garda Síochána refused to supply the data. The DPC advised the parent that it agreed with the restriction imposed, as the controller

in this case had particular knowledge of all of the circumstances pertaining to a shared guardianship arrangement in place and considered that consent of all legal guardians would be required in order to release the data in this case.

Case Study 10

Data restrictions – third-party data; opinion given in confidence (Law Enforcement Directive)

The DPC examined a case where restrictions were imposed by An Garda Síochána to access on the basis of Sections 91(7) and (8) of the Data Protection Act 2018.

The matter related to an individual seeking copies of allegations of abuse made against him with regard to the welfare of his parents. Having examined this matter, it was clear to the DPC

that releasing the information would entail the release of third-party data and would reveal the identity of the person making the allegations. The DPC was satisfied on review that the information sought was provided in the strictest of confidence and considered the provisions of Section 91(9)(a) also applied.

Case Study 11

Data restrictions – prosecutions pending (Law Enforcement Directive)

The DPC frequently examines complaints in relation to restrictions imposed by An Garda Síochána and the Director of Public Prosecutions (DPP) due to criminal prosecutions pending. Complaints range from assault cases where documentation such as PULSE records, photographs and An Garda Síochána reports of the incidents are sought, to requests for CCTV footage from within An Garda Síochána stations themselves.

In some cases, An Garda Síochána may supply an individual with a copy of their statement provided by the individuals but will withhold other data on the basis of Section 94(3)(a) of the Act whereby a data controller may restrict

access, wholly or partly, for the purposes of “the prevention, detection or investigation of offences, the apprehension or prosecution of offenders or the effectiveness of lawful methods, systems, plans or procedures employed for the purposes of the matters aforesaid.”

Upon confirmation by a data controller that criminal prosecutions are pending, the DPC will advise an individual that once legal matters in relation to those cases are concluded, the individuals may re-apply for a copy of their data as set out in Section 91 of the Data Protection Act 2018.

Case Study 12

Access restrictions (Law Enforcement Directive)

The DPC received a complaint from an individual who alleged they were a victim of a crime. The individual requested to have their sensitive personal data processed by An Garda Síochána (AGS) according to their specific terms, namely they requested to have a full copy of the medical results of forensic tests undertaken by Forensic Science Ireland (FSI) made available to them immediately upon receipt of the results by AGS. The individual then sought to have the sample kit split, with this request subsequently amended to seeking the analysis of specific sample vials.

The DPC noted that the entire process of seeking the analysis of forensic samples, following the alleged crime, was initiated by the individual data subject. In order to proceed with the forensic tests, the individual was required to complete a form entitled *'Consent for Release of Stored Forensic and a Legal Report to the Custody of An Garda Síochána'*. The DPC determined that any personal data processed by AGS in the context outlined would fall under the Law Enforcement Directive (EU) 2016/680 as transposed in the Data Protection Act.

AGS advised the DPC that in cases where an individual submits their personal data to AGS and FSI for further testing, any related further processing by AGS and FSI is carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties.

Thus, a report issued by Forensic Science Ireland to AGS, is governed by the provisions of Section 94 of the Act, which sets out restrictions on access that may be imposed by a data controller, including a restriction to avoid prejudicing an investigation. Having examined the matters raised, the DPC advised the individual that the Law Enforcement Directive (EU) 2016/680 as transposed in Parts 5 and 6 of the Act does not provide for individuals to stipulate the conditions under which data subjects consent to have their personal data processed by a law enforcement authority.

In relation to the processing of forensic samples in a law enforcement context, the DPC was satisfied the processing of sensitive data was in compliance with sections 71 and 73(1)(b)(i) of the Act. The DPC noted the *'Consent for Release of Stored Forensic and a Legal Report to the Custody of An Garda Síochána'* form specified all the intended recipients of the data, as well as the fact that the findings of the laboratory tests and the legal report could also be released to the courts for use in evidence. The DPC recommended the addition of a Data Protection Notice to the form, to allow data subjects obtain detailed information on the legislative framework and procedures governing the conditions of processing in relation to forensic samples and AGS investigations.

Case Study 13

Prosecution of Three Ireland (Hutchison) Limited (ePrivacy)

In February 2021, the DPC received one complaint from an individual concerning unsolicited marketing electronic mail they had received from the telecommunications company Three Ireland (Hutchison) Limited. The complainant opted out of receiving marketing emails in mid-February 2021. In response to the DPC's investigation, Three Ireland (Hutchison) Limited explained that when it attempted to execute the opt-out request an issue arose from a scenario of two records getting sent simultaneously and losing sequence, resulting in its system not being updated correctly. As a result, three further marketing emails were sent to the complainant in the following weeks. Three Ireland (Hutchison) Limited stated that it remedied the matter by implementing a script to resolve differences between permissions data. It also set up an email alert to monitor the script and raise an alert should the script stop working.

The DPC had previously prosecuted Three Ireland (Hutchison) Limited in 2020 and 2012 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 6 September 2021, Three Ireland (Hutchison) Limited pleaded guilty to two charges under Regulation 13(1) of the ePrivacy Regulations. The District Court applied the Probation of Offenders Act 1907, on the basis of a charitable donation of €3,000 to Little Flower Penny Dinners. Three Ireland (Hutchison) Limited agreed to discharge the DPC's legal costs.



Case Study 14

Prosecution of Vodafone Ireland Limited (ePrivacy)

In August 2019, March and September 2020, the DPC received three complaints from individuals regarding unsolicited marketing telephone calls, text messages and emails they had received from Vodafone Ireland Limited. In response to the DPC's investigation of the first complaint, Vodafone Ireland Limited explained that the former customer had called Vodafone Ireland Limited on seven separate occasions to try to opt-out of receiving marketing phone calls to their mobile phone. On each occasion the agent they spoke to did not follow proper procedures and this resulted in the former customer not being opted out of marketing and receiving further marketing calls. The complainant closed his account with Vodafone Ireland Limited and switched to another operator due to the marketing phone calls he received.

In the other two cases, the complainants are existing customers of Vodafone Ireland Limited. In one case the customer received a marketing call to their mobile phone number in February 2019 and during that call the customer told the caller that they did not want to receive further marketing calls. Despite this request, Vodafone Ireland Limited subsequently made a further twelve marketing phone calls to the complainant's mobile phone as its agent did not take any action to change the complainant's marketing preferences.

In the other case, the complainant completed a transfer of ownership form on which they clearly set out their marketing preferences not to receive any marketing communications from Vodafone Ireland Limited. The agent handling the transaction failed to follow a process to input the customer's marketing preferences. As a result, the customer subsequently received a further fourteen unsolicited marketing messages – seven emails and seven text messages.

The DPC had previously prosecuted Vodafone Ireland Limited in 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 these complaint cases.

At Dublin Metropolitan District Court on 6 September 2021, Vodafone Ireland Limited pleaded guilty to seven charges under Regulation 13(1) and 13(6)(a) of the ePrivacy Regulations. The District Court convicted Vodafone Ireland Limited on seven charges and imposed fines totalling €1,400. Vodafone Ireland Limited agreed to discharge the DPC's legal costs.

Case Study 15

Request for footage from online meeting (Access Complaints)

An individual participated in a Zoom meeting that was recorded by the data controller. This was the sporting club's AGM. The individual made an access request for a copy of this recording. The data controller refused the request stating that it didn't fall within the remit of GDPR. The individual believed the data contained in the recording was their personal data. The data controller stated the video recordings of the AGM were no longer accessible due to corruption while saving and the inexperience of the data controller in employing this remote video hosting software. However they stated the minutes of the meeting would be available for viewing within a space of weeks.

At this time, the DPC proposed the conclusion of this case in light of the apparent inaccessibility of videos sought by the individual, but the individual did not agree with this approach, stating that video conferencing used during the AGM had been common practice for the data controller for some time and so it seemed unlikely to the individual that the difficulties described by the data controller would have occurred. Upon further questioning by the DPC, the data controller confirmed that video footage was in fact available, but advanced Article 15(4) of GDPR as a reason for its restriction. The data controller was now stating that the video footage of third parties visible in the recording could be considered third-party data and the individual was not entitled to this. However, they were willing to provide written transcripts of the footage to the individual. The DPC contested this, coming to the opinion that, in light of the public nature of the original recordings, as they were part of an AGM, they were made with the participant's understanding that they could be considered accessible at a later date.

Further issues arose when the individual received written transcripts of the video. The individual claimed that the transcripts were inaccurate and did not reflect the contents of the original video.

In light of this, the DPC contacted the data controller once again, both highlighting the DPC's opinion regarding the advancement of Article 15(4) and seeking sight of the video from which the transcript had been made. The data controller provided the audio of the video only. Upon assessment, it was clear that the transcript was an accurate reflection of the video's audio content. The DPC recommended that in order to facilitate an amicable resolution at this stage the data controller should release the same audio content, previously provided to the DPC, to the individual. The data controller complied, but the individual was still not satisfied, once again restating their request for sight of the video content. Upon further request by the DPC to state the exemption it relied on to restrict access to the video content, it was decided by the data controller to release the full video content to the individual. The DPC did not receive copy of the full video content, and so was unable to directly assess whether there was any disparity between it and the audio provided. However, upon confirmation of its receipt, the individual stated they were satisfied with its content and thus this matter was concluded amicably.

The above case involved extensive communication between the DPC, the data controller and the individual. This matter could have been resolved by the data controller if they had released the requested video footage on receipt of the access request. If the data controller was aware of its obligations under GDPR in the first instance then this case would not have been lodged with the DPC.

Case Study 16

Exemptions applied to CCTV footage (Access Complaints)

The DPC received a complaint from an individual regarding an access request made to the data controller, a retailer. The solicitors acting for the individual in relation to a personal injury claim had submitted the access request relating to a two-week period when the alleged incident had taken place. They were seeking records of the incident to include CCTV footage. Data was released but the individual identified that the CCTV footage, the accident report form and witness statements had not been released. In responding to the individual's query in relation to these items, the data controller advised they were restricting access to the items as it was necessary to avoid any obstruction or impairment of the legal proceedings and/or operation of legal privilege.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018, with both the complainant and data controller agreeing to work with the DPC to try to amicably resolve the matter.

The DPC advised the data controller to prepare a list which would document any items which the organisation was applying an exemption to, while also documenting the exemption on which they were relying. On receipt of the list, the DPC probed the exemptions being used and looked for the organisation to demonstrate how they had ensured the restriction was necessary and proportionate. The DPC also looked for samples of the documents to be released so we could examine how the exemptions were being applied.

Upon investigation the DPC identified that the documents did contain some personal data of the individual and requested the data controller to release them with relevant redactions. In relation to the CCTV footage, the DPC stated that the primary reason for capturing the data was for security purposes and not for the defence of litigation claim and therefore requested the footage be released to the individual with relevant redactions. The DPC accepted the remaining exemptions were being validly applied as provided by the legislation.



Case Study 17

Amicable resolution in cross-border complaints: access request to Airbnb

The DPC received a complaint in September 2020 relating to a request for access (under Article 15 of the GDPR), that the complainant had made to Airbnb Ireland UC ("Airbnb"). The complaint was made directly to the DPC, from an individual based in Malta. Upon assessment by the DPC, the complaint was deemed to be a cross border one because it related to Airbnb's general operational policies and, as Airbnb is available throughout the EU, the processing complained of was therefore deemed to be of a kind "...which substantially affects or is likely to substantially affect data subjects in more than one Member State" (as per the definition of cross-border processing under Article 4(23) of the GDPR).

The complainant submitted an access request to Airbnb. Airbnb facilitated this access request by providing the complainant with a link to an access file containing his personal data. However, when the complainant tried to use the link, it was not operational. In addition, the complainant was frustrated with the difficulty they faced in contacting Airbnb in relation to this matter. The complainant submitted their complaint to the DPC on this basis.

The DPC contacted Airbnb and asked that it facilitate the complainant's request. The DPC specified that Airbnb should ensure any links it sends to complainants are fully tested and operational.

In reply, Airbnb explained that once it was informed that the initial link it sent to the complainant was not operational, it sent a renewed link to the complainant and was unaware that the complainant had had any difficulty in accessing this second link. Nonetheless, in the interests of amicably resolving the complaint, Airbnb agreed to provide an additional link to an access file to the complainant and for an encrypted file to be sent to the complainant via secure email.

As a result, the matter was amicably resolved pursuant to section 109(3) of the Data Protection Act 2018 ("the Act"), and under section 109(3) of the Act the complaint was deemed to have been withdrawn. This case study demonstrates the benefits — to individual complainants — of the DPC's intervention by way of the amicable resolution process.

In this case, the DPC's involvement led to the complainant being able to access his data. This case study illustrates how often simple matters - such as links which do not operate properly - can become data protection complaints if the matter is not managed appropriately at the front end of data controllers' customer service and data protection teams.

Case Study 18

Amicable resolution in cross-border complaints: Google (YouTube)

The DPC received a complaint in September 2020, via its complaint webform, against Google Ireland Limited (YouTube). The complaint was made by a parent acting on behalf of their child and concerned a YouTube channel/account. The YouTube channel/account had been set up when the child was ten years old and at a time when they did not appreciate the consequences of posting videos online.

Although the complaint was made directly to the DPC by an Irish resident, upon assessment it was deemed to constitute a cross-border complaint because it related to YouTube's general operational policies and, as YouTube is available throughout the EU, the processing complained of was therefore deemed to be of a kind *"which substantially affects or is likely to substantially affect data subjects in more than one Member State"* (as per the definition of cross-border processing under Article 4(23) of the GDPR).

According to the complainant, the child no longer had control over the account as they had lost their passwords and the account was no longer in use. However, classmates of the child had discovered the videos, previously posted by the child which were now the subject of embarrassment to the child. The parent of the child had engaged in extensive correspondence with Google, seeking inter alia the erasure of the account from the YouTube platform. The parent had provided the URL for a specific video on the account and for the account itself. The parent was informed by Google, on a number of occasions, that it had taken action and removed the content from the platform. However, the parent repeatedly followed up to note that the content had not in fact been removed and was still available online. As she considered that the complaint had not been appropriately addressed she thus raised the matter with the DPC.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018, with both the individual and Data Controller agreeing to work with the DPC to try to amicably resolve the matter. The DPC investigated the background to the complaint and noted that it appeared that Google had removed a specific video from the account, for which the URL had been provided, but it had not removed the account in its entirety, with the result that further videos remained online.

The DPC communicated with Google on the matter and informed Google of the particular background of the complaint. Google immediately took action and removed the YouTube account in its entirety. Google confirmed that a misunderstanding had arisen as its support team had incorrectly assessed the URL for a specific video provided by the complainant, rather than the entire account.

The DPC informed the parent of the outcome and it proposed an amicable resolution to the complaint. The parent thereafter informed the DPC that she had recently become aware of another YouTube channel that her child had created, which again was no longer in use, and the child wanted deleted. The DPC thus corresponded further with Google and Google confirmed it had taken immediate action to remove the account and informed the parent of the actions it had taken.

This case highlights that the DPC can assist data subjects during the amicable resolution process in explaining their particular requests to a data controller, often at the appropriate level, when an individual has previously been unsuccessful in initial engagement with the data controller. This further allows the DPC to monitor the compliance of data controllers by taking note of any issues that may be repeated across other complaints.

Case Study 19

Amicable resolution in cross-border complaints: Yahoo EMEA Limited

The DPC received a complaint in March 2021 from the Bavarian data protection authority on behalf of a Bavarian complainant against Yahoo EMEA Limited. Under the One-Stop-Shop (OSS) mechanism created by the GDPR, the location of a company's main EU establishment dictates which EU authority will act as the lead supervisory authority (LSA) in relation to any complaints received. Once the lead authority is established, the authority that received the complaint acts as a concerned supervisory authority (CSA). The CSA is the intermediary between the LSA and the individual. In this case, the DPC is the LSA, as the company complained of has its main establishment in Ireland.

The complainant in this matter had lost access to his email account following an update on his computer. The complainant noted that he had engaged with Yahoo in order to regain access and was asked for information relating to the account in order to authenticate his ownership of it. The complainant asserted that he had provided this information. However, Yahoo informed the complainant that it could not verify his identity with the use of the information that it had been provided. The complainant was unclear which information he had provided was not correct and thus continued to give the same answers to the security questions. As Yahoo could not authenticate the complainant's ownership of the account, it recommended that he create a new email account.

The complainant was not satisfied with this solution and thus made a complaint to his local supervisory authority, who referred the complaint on the DPC in its role as Lead Supervisory Authority for Yahoo.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018, with both the individual and Data Controller agreeing to work with the DPC to try to amicably resolve the matter.

The DPC contacted Yahoo on the matter, and Yahoo took a proactive approach and immediately noted its desire to reach out to the complainant directly to seek to resolve the issue as soon as possible. Yahoo thereafter quickly confirmed to the DPC that its member services team made contact with the complainant, who provided alternative information that enabled Yahoo to successfully validate identity of the requester and subsequently restore their account access.

This case highlights that further direct engagement between the parties during the amicable resolution process can often achieve a swift resolution for data subjects. It further highlights that a proactive approach on the part of data controllers in the early stages of a complaint can often resolve matters and avoid the need to engage in a lengthy complaint handling process.

DPC Policy update: **Courts and Decision Making Bodies**

Under Article 55(3) of the GDPR, the DPC is precluded from supervising the data processing operations of the Court when it is acting in a judicial capacity. Section 157 of the Data Protection Act, 2018 provides for the assignment of a specific judge to act as the data protection supervisor in relation to the processing of personal data, which occurs when the Court is acting in their judicial capacity. Therefore, any data protection concerns that arise under such circumstances must be addressed to the Court.

Statutory bodies also engage in various forms of complaint handling, investigative and decision-making functions, such as the Workplace Relations Commission or the Residential Tenancies Board. Ultimately, the DPC remains the supervisory authority for such bodies. An individual who is concerned about the processing of their personal data by a statutory body should raise those data protection concerns with that statutory body in the first instance with recourse to the DPC thereafter, should the complainant remain dissatisfied. The DPC's general policy approach to cases such as these, is that it will not examine data protection issues relating to material that is before a statutory body while there is ongoing complaint handling, investigative and/or decision-making process. Such complaints may be handled by the DPC once the statutory process has concluded. Even if the DPC makes a finding of an infringement of the GDPR, it does not have jurisdiction to interfere with the ultimate findings of statutory bodies.

This policy approach is grounded in the DPC's Regulatory Strategy 2022 -2027 and reflects the DPC's assessment of the most appropriate way to handle complaints of this nature having regard to the risks posed to data subjects by the processing of their personal data by such statutory bodies, weighed against the public interest in ensuring the independence and proper functioning of such statutory bodies and the integrity of their processes.

DPC Policy update:

The DPC's approach to Domestic CCTV

The DPC receives a large volume of complaints each year and a significant proportion of these are from individuals in relation to their neighbours' domestic CCTV systems.

During the course of the examination it generally transpires that there are no data protection concerns, for the most part operators of Domestic CCTV are operating them in accordance with Article 2(2)(c) of the GDPR, as they are only being used to monitor the operator's property within their property perimeter, accordingly, they are being used for a purely personal or household activity (the personal/household exemption). In the remainder of cases, the DPC works with the operator to try to bring about a position where the CCTV operator comes within the personal/household exemption.

What the DPC has identified is that in the vast majority of Domestic CCTV complaints there is an ongoing dispute between both parties such as Right of Way access, alleged harassment, anti-social behaviour or criminal damage, which would be better addressed through mediation or the Courts. Although, the DPC recognises how stressful it is for individuals to live in an environment where there are ongoing issues with their neighbours, these are not issues that the DPC can examine or comment on. The DPC can only examine any alleged infringements of a natural person's data protection rights.

The DPC is obliged to operate a risk-based approach to complaints in accordance with the GDPR and in line with the DPC's Regulatory Strategy 2022 – 2027, to use its limited resources appropriately having regard to the needs of all complainants. The DPC's general approach to these complaints is:

- ▶ To assess the complaint to determine if there is evidence of the processing of personal data: where there is no such evidence or where the operator satisfies the DPC that the camera in question is either not operating or is operating within the personal or household exemption, GDPR does not apply and no further steps are required.
- ▶ Where the case involves disputed rights of way or land boundaries, the DPC cannot make finding of facts in relation to such matters so it is not possible to determine if the personal or household exemption applies. In those cases, no further action will be taken by the DPC until the legal dispute is determined by the appropriate authority and if processing continues after that point.
- ▶ Where there is evidence of personal data processing, the DPC will engage with the parties to try to resolve the matter by advising the operator to bring their devices into line with the domestic exemption.
- ▶ Where this is not successful and the circumstances of the case indicate a camera operating that is bound up in other issues between private individuals such as use and access to shared entrances and common areas, anti-social behaviour, allegations of harassment, nuisance, assault, threatened assault or damage to property, the DPC will usually attempt to identify the relevant data protection issue(s) for the parties and provide appropriate advice.
- ▶ It will be open to an individual to rely on this advice in the context of how they deal with the wider issues in dispute.

This is a general approach of the DPC and will be determined on the facts of any given case. However, since the introduction of this approach, the DPC anticipates a significant reduction in the number of repeat complaints from the same individuals, and a reduction in the resources utilised in examining these complaints, thus freeing up the DPC's resources to focus on complaints about more systemic data protection infringements.

7

Breaches

In 2021, the DPC received **6,616** personal data breach notifications under Article 33 of the GDPR. A total of **6,549** valid data breaches were recorded, representing a **2%** decrease (114) on the numbers reported in 2020. In line with what was reported in previous years since the introduction of GDPR, the highest category of data breaches notified in 2021 was in relation to unauthorised disclosures, accounting for **71%** of the total notifications.

Of the total 6,616 breach notifications that the DPC received in 2021, in terms of breakdown, 3,677 related to the private sector, 2,707 to the public sector and the remaining 232 came from the voluntary and charity sector.

It is noted that a disproportionately large chunk of breach notifications (2,707) originate in public sector organisations in Ireland. The ten organisations with the highest number of breach notifications recorded against them are public sector bodies and banks, with insurance and telecom companies falling among the top twenty.

Regarding the number relating to unauthorised disclosures, this is mostly due to poor operational practices and human error, such as inserting the wrong document in an envelope addressed to an unrelated third party, or sending email correspondence to multiple recipients using the 'To' or 'Cc' fields instead of the Bcc field. The DPC has also seen a vast increase in the number of breaches caused by email correspondence issuing to an incorrect recipient due to the message service employed which predicts the recipient's email address based on the first characters entered. As regards hard copy correspondence issuing to the wrong party, we are seeing this occurring particularly in the financial institutions and fundamentally it is down to a failure to update data in a timely fashion and customers' failure to notify the financial institution of a change of address.



Data Breach Notification by Category	Charity	Private	Public	Voluntary	Total
Disclosure (unauthorised)	32	2560	2012	124	4728
Unauthorised access - paper files/documents/ records	2	170	138	8	318
Processing error - (PD disclosed)	2	140	96	7	245
Paper lost or stolen	3	52	151	13	219
Online publication - Unintentional		166	28	6	200
Hacking - Other	1	107	18	4	130
Paper lost/stolen - Official documentation		7	108	1	116
Integrity - unintentional alteration (No PD disclosed)		96	5		101
Unauthorised access - Electronic Devices/Assets	2	36	36	6	80
Social engineering - Phishing		56	11	4	71
Hacking - Ransomware	1	54	11	1	67
Unauthorised access - Online Account		32	9	1	42

Notifications

2021 saw the introduction of a revised breach webform which was developed in light of feedback received from data controllers who have had a requirement to engage with the form process. Amongst other things, the form guides users through a number of questions in order to determine whether the breach relates to cross-border processing, as it is clear to the DPC that there is some confusion as to when an organisation meets the criteria to avail itself of the 'One-Stop-Shop' (OSS) mechanism.

For clarification, in order to avail of the one-stop-shop mechanism, a multinational organisation must have as a starting point its European headquarters established in one of the EU member states. Where this criteria is met, the organisation may be able to avail of the OSS and elect to deal directly with the supervisory authority of the country where its headquarters are based. This applies even in instances where a breach or complaint originates in a different member state.

The DPC has noted that organisations do not always understand when and how the OSS mechanism applies, resulting in organisations either incorrectly notifying personal data breaches to the DPC, or failing to separately notify breaches to another authority. In order to mitigate this, the new DPC form asks a number of questions aimed at identifying whether the breach relates to cross-border processing of personal data and, if so, whether the DPC is the appropriate supervisory authority to which the organisation must make the breach notification.

A noteworthy change is the requirement for the controller to outline what technical and/or organisational measures were in place before the breach occurred and what action was taken after the breach occurred in order to mitigate against any risk being realised. This information is vital to allow the DPC to undertake an immediate analysis on the breach which may direct what further mitigation steps, if any, are required to be taken. There is also the opportunity for the controller to upload any supporting documents that it may wish to bring to the attention of the DPC regarding the breach.

New strategic approach

Since the introduction of the GDPR, the DPC has taken a very hands-on approach to handling every single breach notified. The DPC would conduct its own risk and impact assessment and engage with the controller on mitigation actions and matters relating to notification of data subjects in high-risk cases. That practice will cease from the end of 2021. From January 2022, the DPC, regarding the notifications that data controllers are legally obliged to submit, will only provide an acknowledgement of receipt of the submission and will not be issuing recommendations or requesting further information in most cases. It should be noted that the absence of further immediate engagement by the DPC will not indicate satisfaction with the notification itself, nor the assessment contained therein. The DPC will continue to assess all notifications individually and, in cases where the DPC receives complaints or deems the issues to warrant further information or a formal statutory inquiry, the DPC will proceed in that way.

The DPC will no longer offer guidance to a controller when a breach arises, in recognition of the extensive guidance already in existence and the assistance already provided by the DPC to controllers in acclimatising to their breach notification responsibilities over the last three years. The focus will be on prioritising enforcement cases instead.

ePrivacy Breaches

The DPC received a total of **38** valid data-breach notifications under the ePrivacy Regulations (S.I. No. 336 of 2011), which accounted for just **under 1%** of total valid cases notified for the year.

The DPC expects the number of breaches notified under this regime to increase due to changes in ePrivacy legislation. Much of the existing Irish telecoms legal framework adopted in 2011, which supplemented the underlying Communications Regulation Acts 2002 to 2017, is due to be replaced upon Ireland's implementation of the new EU Electronic Communications Code (the Code). A significant change in relation to the Directive (EU) 2018/1972 (the "Recast European Electronic Communications Code") amended 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 that were required to notify personal data breaches to the DPC under Article 33 of the GDPR will have to notify the DPC of such breaches under the ePrivacy regime – i.e. SI 336 of 2011.

Law Enforcement Directive Breaches

The DPC also received **51** 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.

Case Studies

Case Study 20

Repeated similar breaches

Over a period of 12 months, the DPC received notifications of a series of similar breaches from a data controller involved in financial matters. The controller sold services through a nationwide retail network owned and operated by a third party, which acted as its processor. The breaches occurred when existing customers of the controller made purchases at the processor's outlets, but used an address different from the address they had previously registered with the controller. Recent changes to the controller's customer database systems had not been fully coordinated with those for sales, resulting in sales documents containing personal data being sent to customers' old addresses rather than their new ones. The controller had instructed the processor not to accept purchase requests until changes of address had been registered, but some counter staff did not consistently follow the correct procedures.

When the DPC flagged the pattern of breaches, the controller agreed that there was a systemic problem that required attention by its senior management.

While a technical solution was being designed and tested, the controller and processor adopted interim measures including re-training of staff, increased supervision, and a notice that appeared on screens used by processor staff when effecting sales, prompting them to confirm that the customer's current registered address was correct. The controller implemented the changes in its IT systems to prevent sales documents being sent to incorrect customer addresses, and the recurring breaches ceased.

This case demonstrates how the DPC monitors breaches notified under Article 33 of the GDPR to identify systemic problems, whether in individual controllers, industry types or economic sectors. It also shows how changes intended to improve information systems can have unforeseen side-effects that adversely affect data subjects and the controller. Lastly, it highlights that controllers must monitor the performance of processing agreements to ensure that processors clearly understand and follow procedures for processing personal data.

Case Study 21

Unauthorised disclosure arising from video conferencing

An educational institute utilised a video conferencing application to allow students to deliver presentations to lecturers while pandemic restrictions prevented in-person meetings. To enable sharing with external examiners, which is a requirement, the presentations were recorded. All participants were aware of this arrangement, though it was not intended that students would have access to recordings of their presentations.

Two groups of students made presentations to lecturers in separate sessions. After each session, the lecturers discussed the students' work among themselves. These discussions were also recorded, though the intention was to edit them out before sharing the recordings with external examiners. It was wrongly believed that saved recordings were accessible only to the lecturers. In fact, all invited participants, including the students who presented, had access to recordings of their sessions and were automatically emailed a link to the relevant file on the institution's server. As a result, students gained access to lecturers' discussion of other students' work, which included personal remarks about some of the students.

These were accessed by several students. In the following days, excerpts were circulated on messaging applications and social media.

The organisation reported the breach to the DPC, which confirmed that the recordings accessible to students had been deleted, and clarified the steps taken by the organisation to have the excerpts removed from the social media to which they had been posted. The DPC concluded its assessment of the breach with comprehensive recommendations on the use of IT equipment including video conferencing, and on measures to ensure that staff and students understood and complied with relevant data protection policies.

This case highlights the potential risks posed by the use of video conferencing and similar technologies. Data controllers should ensure that persons who operate these applications are familiar with how they work and ensure that they do so in compliance with data protection law. Controllers should ensure that data protection policies and procedures fully reflect the practices and technologies that they use when processing personal data.

Case Study 22

Disclosure due to misdirected email

A notification was received from a statutory body whose functions include the investigation of complaints concerning experts' professional conduct, training or competence. The personal data breach occurred when a letter concerning a complaint against a specialist was attached to an email and sent to an incorrect address. The attachment contained personal data of several persons, including health data, and was encrypted. However, the password for the encrypted letter was issued in a separate email to the same incorrect address.

The nature of the personal data and the context all indicated a high risk to data subjects. The DPC accordingly confirmed that all affected persons had been notified of the breach, the risks and measures being taken in response to them, as required by Article 34 of the GDPR.

The DPC reminded the organisation of its continuing obligation to secure personal data that was accidentally disclosed, and of the importance of ensuring security when emailing personal data. The statutory body has undertaken a review of all its data protection processes, policies and procedures.

Misaddressed emails are one of the most common causes of breaches reported to the DPC. Encryption is a valuable tool that can help to protect against accidental disclosures. However, it is advisable to use a separate medium – such as a telephone call or SMS message – to send the password, as a single mistake in an email address can negate the benefits.

Case Study 23

Inappropriate disposal of materials by an educational institution

A health science focused university notified the DPC of a breach arising from inappropriate disposal of materials containing personal data. Due to pandemic restrictions, an employee worked from home on a recruitment project. The employee worked on printed copies of a number of job applications and accompanying CVs. The organisation had instructed employees working from home to minimise printing and to destroy documents before disposal. However, the employee placed the recruitment documents intact into a domestic recycling bin. High winds caused contents of the bin, including the recruitment documents, to be dispersed.

In concluding its examination of the breach, the DPC made a number of recommendations. These focused not just on the work practices of employees, but most importantly on the technical and organisational measures of the controller.

While it is important for staff to understand and implement good data protection practices, it is the responsibility of the controller to ensure that they do so and have the means – including, where appropriate, devices such as shredders - of delivering the required standard of protection.

This case also illustrates how working from home can change people's work environment or habits in ways that can pose risks to personal data. Office facilities, such as confidential shredding, secure printing or even private rooms for discussions – are not always available or feasible at home. As the number of people working remotely increases, controllers must review and adapt their resources, policies and procedures to ensure that they are adequate for the risks posed and the environment in which they occur.

Case Study 24

Email addresses disclosed via group mail

The DPC received a breach notification from a charity that supports people with intellectual disabilities. The breach occurred when an email newsletter was addressed to recipients using the CC field rather than the BCC field. The result was that the email addresses of all recipients were disclosed to those who read the email. This is a common type of personal data breach that is often the result of simple human error and that usually poses low risks. While the risks posed in this instance may not have been significant, further inquiries and an analysis of previous submissions to the DPC indicated poor awareness of data protection issues and responsibilities among the charity's staff and volunteers.

Following engagement with the DPC, the organisation introduced training on data protection for staff and volunteers, and moved to create a new management role with responsibility for data protection compliance across the organisation.

Charities frequently process personal data of vulnerable persons, often including special category data such as information concerning health. Data protection is a fundamental right in the European Union and protecting the rights of vulnerable persons requires care, planning and careful organisational measures. The hard work and goodwill of staff and volunteers must be matched by appropriate management and compliance resources to ensure the protection of personal data rights.

Case Study 25

Social Engineering attack

A medium-sized law firm reported that it was the victim of a social engineering attack. A staff member opened an email from a malicious third party that secretly installed malware on their computer. The malware enabled monitoring email communications and permitted the bad actor to defraud a client of a sum of money. The firm reported the breach to the DPC.

Through its DPC engagement with the firm, the DPC established that the firm used a widely used cloud email service which was managed by a contractor. Basic security settings such as strong passwords were not properly enforced and multi-factor authentication was not implemented. Upon becoming aware of the incident, the firm immediately commissioned a full investigation to establish the root cause and the extent of the breach.

Based on the findings of the investigation, the firm responded promptly and implemented further technical security measures as well as additional cyber security and data protection training to all staff. The DPC requested that updates be provided on the implementation of appropriate organisational and technical security measures to prevent a reoccurrence of a similar breach.

This case demonstrates in stark terms that an organisation cannot assume that it has adequate measures in place simply because it uses an established service provider for functions such as email, or engages a third party to manage applications. Controllers and processors must still ensure that they have security measures that are appropriate to any risk that may be posed to the personal data for which they are responsible.

8

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; or**
- ▶ **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 facts as found to the provisions of the GDPR and/or 2018 Act as applicable 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 power⁷.

On 31 December 2021, the DPC had **81 statutory inquiries** on hand, including 30 cross-border inquiries.

⁷ 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.

Domestic Inquiries 2021

Inquiries where a significant sanction or corrective measure was applied in 2021

Irish Credit Bureau (March 2021): This decision concerned a personal data breach that occurred when the Irish Credit Bureau implemented a code change to its database which contained a technical error, resulting in the ICB database inaccurately updating the records of 15,120 closed accounts. The decision found that the ICB infringed Article 25(1) of the GDPR by failing to implement appropriate technical and organisational measures designed to implement the principle of accuracy in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. The decision also found that the ICB infringed Article 5(2) and 24(1) of the GDPR by failing to demonstrate compliance with its obligation, pursuant to Article 25(1) of the GDPR, to undertake appropriate testing of proposed changes to its database. The decision imposed an administrative fine on the ICB in the amount of €90,000 in respect of the infringements and issued the ICB with a reprimand in respect of the infringements.

MOVE Ireland (August 2021): In August 2021, the DPC issued a decision to MOVE Ireland (MOVE) regarding a personal data breach that MOVE notified to the DPC, which concerned the loss of eighteen SD Cards that may have contained recordings of group sessions of MOVE's programme where participants discuss their behaviour and attitudes with regard to domestic violence with a facilitator. The decision found that MOVE infringed Articles 5(1)(f) and 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 by means of recording group sessions on SD Cards containing participants' and facilitators' personal data and imposed an administrative fine on MOVE in the amount of €1,500 in respect of the infringements.

Limerick City and County Council (December 2021): The DPC issued a decision to Limerick City and County Council considering a broad range of issues pertaining to surveillance technologies deployed by the Council. The decision made findings on over 40 issues, including that certain CCTV systems operated by Limerick City and County Council were unlawful and that the Council infringed Article 15 of the GDPR by rejecting subject access requests in respect of CCTV cameras used for traffic management purposes. The decision imposed a temporary ban on the Council's processing of personal data in respect of certain CCTV cameras. The decision also ordered the Council to bring its processing into compliance by taking specified action and reprimanded the Council in respect of the infringements, and imposed an administrative fine in the amount of €110,000.

The Teaching Council (December 2021): The DPC issued a decision to the Teaching Council (the Council) regarding a personal data breach notified by the Council to the DPC on 9 March 2020. The personal data breach occurred when a phishing email was accessed by two staff members of the Council, allowing then for the creation of an auto-forward rule from their email accounts to a malicious email account. The decision found that the Council infringed Article 5(1) and Article 32(1) of the GDPR by failing to process personal data in a manner that ensured the appropriate security of the personal data using appropriate technical and organisational measures. The decision also found that the Council infringed Article 33(1) of the GDPR by failing to notify the DPC of the personal data breach when it ought to have been aware of them. The decision imposed an administrative fine on the Council in the amount of €60,000, reprimanded the Council and ordered the Council to bring its processing operations into compliance with Articles 5(1)(f) and 32(1) of the GDPR by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Inquires that have gone to draft decision in 2021

The Department of Health: The DPC commenced this Inquiry following RTE's Prime Time programme in March 2021 regarding the processing by the Department of Health of the personal data of children with autism who were involved in legal actions against the State. The DPC issued its Draft Decision in December 2021.

The Personal Injuries Assessment Board: This Inquiry examines the Personal Injuries Assessment Board's compliance with GDPR obligations in relation to a personal data breach notified which occurred through the loss of a USB storage device. This Inquiry is related to the below Inquiry concerning BEO Solutions. The DPC issued its Draft Decision in November 2021.

BEO Solutions: This Inquiry examines BEO Solution's compliance with GDPR obligations in relation to a personal data breach notified which occurred through the loss of a USB storage device. The DPC issued its Draft Decision in November 2021.

Bank of Ireland: This Inquiry commenced in response to the large number of data breaches notified to the DPC during the period since 25 May 2018 regarding information provided by Bank of Ireland to the Central Credit Register. The DPC issued its Draft Decision in January 2022.

Slane Credit Union: This Inquiry commenced in response to a breach notified to the DPC in relation to an unauthorised disclosure. The DPC issued its Draft Decision in December 2021.

Inquiries where submission on a statement of issues or inquiry report were invited from the relevant parties during 2021

Kildare County Council: This Inquiry considers a broad range of issues pertaining to surveillance technologies deployed the Council.

Bank of Ireland 365: This Inquiry examines a potential unauthorised disclosure of personal data in how BOI provisioned certain Banking 365 customers regarding potential incidents involving the bank misconfiguring a new customer's 365 profile such that a customer could inadvertently access the personal data and current account of a different customer.

Allianz: The DPC commenced this Inquiry following 49 personal data breaches notified by Allianz between 25 June 2020 and 31 December 2020. This Inquiry examines the appropriateness of Allianz's technical and organisational measures to ensure the security and accuracy of its personal data processing.

Centric Health: The DPC commenced this Inquiry following a ransomware attack potentially affecting patient data held on Centric's patient appointment system.

Virtue Eldercare: The DPC commenced this Inquiry following a personal data breach whereby an unknown actor potentially gained access to an email account and set up mail forwarding rules to an external account.

Cross-Border Inquiries 2021

Inquiries where a Final Decision issued in 2021

WhatsApp Ireland Limited (WhatsApp): Transparency for users and non-users

This inquiry concerned WhatsApp's compliance with its transparency obligations in respect of both users and non-users. In its final decision of 20 August 2021, the DPC imposed a fine of €225 million. In addition, the DPC also imposed a reprimand along with an order directing WhatsApp to bring its processing into compliance by taking a range of specified remedial actions. This final decision is now subject to litigation and a more detailed update in respect of these proceedings can be found at the end of the chapter on Significant Sanctions and Corrective Measures.

Inquiries where the co-decision making procedure under Article 60 GDPR commenced and remained ongoing in 2021

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): 12 data breaches

This inquiry concerns an examination of the extent to which Facebook complied with its obligations under Articles 5(1)(f), 5(2), 24 and 32 GDPR in the context of a series of 12 personal data breaches that it notified to the DPC on dates 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. In response, the supervisory authorities of Poland and Hamburg raised objections. As of the end of 2021, the DPC was engaging with those supervisory authorities in an endeavour to reach consensus on the issues arising in the context of their objections.

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

This inquiry concerns the processing of certain personal data of children by Facebook in the context of the Instagram social networking service, in particular relating to the operation by children of "business accounts" and also certain default settings which were applied to children's accounts. A draft decision in this Inquiry was sent to other concerned supervisory authorities on 3 December 2021 for the purpose of the co-decision-making process outlined in Article 60 GDPR. As of the end of 2021 the DPC was awaiting receipt of any comments or objections from other supervisory authorities (which are required to be raised within 1 month) in relation to the draft decision.

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

This complaint based inquiry concerns the legal basis on which Facebook 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. As of the end of 2021, the Article 60 process was underway at EDPB level, with a number of sets of objections having been received from other supervisory authorities.

Inquiries where submissions on a preliminary draft decision were invited from the relevant parties during 2021

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 Facebook 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. A final inquiry report was provided to the parties by the DPC investigator on 18 January 2021. Thereafter, the decision maker in the DPC issued a preliminary draft decision to the parties for their submissions on it in December 2021.

WhatsApp Ireland Limited (WhatsApp): complaint received from NOYB

This complaint based inquiry concerns the legal basis on which WhatsApp relies to process the personal data of users and certain issues related to transparency information which is provided to WhatsApp users. A final inquiry report was provided to the parties by the DPC investigator on 18 January 2021. Thereafter, the decision maker in the DPC issued a preliminary draft decision in December 2021 to the parties for their submissions.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): own volition inquiry and complaint based inquiry (complainant: Max Schrems) concerning the lawfulness of Facebook's data transfers to the United States

These inquiries are concerned with examining the lawfulness of data transfers from the EU to the US carried out by Facebook. The own volition inquiry relates to such data transfers generally as they apply to the personal data of Facebook users while the complaint based inquiry is concerned with a complaint made by Mr Max Schrems against Facebook.

A preliminary draft decision was issued to Facebook in August 2020 by way of the commencement of the own volition inquiry. A stay (suspension) was placed on that inquiry in September 2020 in the context of separate judicial review proceedings taken by each of Facebook and Mr Schrems against the DPC. Following the conclusion of both judicial review actions, the own volition inquiry resumed in May 2021 and a separate complaint-based inquiry concerning Mr Schrems' complaint was also commenced. The inquiries are proceeding in tandem with each other with voluminous submissions having been received in respect of each inquiry during the course of 2021.

(See also 'Judgments delivered in 2021' in the Litigation chapter for a summary of the two sets of proceedings and their outcomes; see also the detailed summary of the High Court judgment delivered in May 2021 in the judicial review action taken against the DPC by Facebook in Appendix 3 at the back of this report).

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 co-operation 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.

Inquiries where submission on a statement of issues or inquiry report were invited from the relevant parties during 2021

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. A Statement of Issues setting out the relevant factual matters and issues for determination was provided to Google for its submissions in December 2021.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): data scraping

In April 2021, multiple media reports highlighted that a collated dataset of Facebook user personal data had been made available online pertaining to the personal data of approximately 533 million Facebook users worldwide. On foot of this, an inquiry was commenced in April 2021 and is currently ongoing. A Statement of Issues was provided to Facebook in December 2021 for its submissions.

Quantcast Ireland Limited (Quantcast): adtech services

This inquiry concerns the processing of personal data by Quantcast in the context of services provided by it to advertising clients to enable the delivery of targeted advertising. The inquiry is examining the legal bases relied on by Quantcast for its processing of personal data for the purposes of profiling and targeted advertising activities, whether its retention of personal data complies with data minimisation and storage limitation obligations and whether it complies its transparency obligations towards data subjects. A Statement of Issues setting out the relevant factual matters and issues for determination was issued to Quantcast in December 2021 for its submissions.

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

This inquiry concerns a complaint made by La Quadrature du Net in relation to the lawfulness of the processing of personal data of users of the LinkedIn service carried out by LinkedIn for targeted advertising and/or behavioural analysis. A Statement of Issues setting out the relevant factual matters and issues for determination was provided to LinkedIn in July 2021 and submissions on that document were subsequently received. As of the end of 2021, preparation of the preliminary draft decision was underway.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): complaint by La Quadrature du Net

This inquiry concerns a complaint made by La Quadrature du Net in relation to the lawfulness of the processing of personal data of users of the Facebook service for targeted advertising and/or behavioural analysis. A draft inquiry report was provided to Facebook in August 2021 and submissions were subsequently received on that document. As of the end of 2021, the preparation of the finalised inquiry report was underway.

Facebook Ireland Limited (Facebook) (now known as Meta Platforms Ireland Limited): breach notification issues

This inquiry concerns Facebook’s compliance with the breach notification obligations arising under Article 33 of the GDPR in connection with the notification to the DPC of a data breach which occurred in September 2018 and affected Facebook user tokens. A draft inquiry report was provided to Facebook in May 2021 and submissions were subsequently received on that document. As of the end of 2021, the preparation of the finalised inquiry report was underway.

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

This inquiry concerns whether Facebook complied with its obligations under the GDPR, in particular in relation to security of processing, in connection with a security incident which occurred in early 2019 where user passwords were inadvertently stored in plaintext on Facebook’s internal systems.

A draft inquiry report was provided to Facebook in June 2021 and submissions were subsequently received on that document. As of the end of 2021, the preparation of the finalised inquiry report was underway.

Apple Distribution International (Apple): complaint by La Quadrature du Net

This inquiry concerns a complaint made by La Quadrature du Net in relation to the lawfulness of the processing of personal data of users of the Apple service for targeted advertising in connection with the unique Apple “Identifier for Advertising”. A draft inquiry report was provided to Apple for its submissions in August 2021 and submissions were subsequently received on that document. Thereafter a final inquiry report was completed and provided to Apple and to the DPC decision maker in December 2021. As of the end of 2021, the inquiry has progressed to the decision-making stage.

Twitter International Limited (Twitter): 5 breaches

This inquiry concerns an examination of the extent to which Twitter complied with its obligations under the GDPR with respect to a number of personal data breaches it notified to the DPC between August and October 2018. This inquiry is examining Twitter’s compliance with Articles 5, 24, 25, 32, and 33 in the context of the occurrence of those breaches. The Inquiry Report was completed and forwarded to the DPC decision maker in November 2021. As of the end of 2021, the inquiry has progressed to the decision-making stage.

Yahoo (formerly Oath EMEA Ltd/Verizon Media EMEA Ltd) (Yahoo): Transparency

This inquiry is concerned with examining Yahoo’s compliance with the requirements to provide transparent information to data subjects under the provisions of Articles 12-14 GDPR. The inquiry has involved extensive examination of the user-facing information provided on Yahoo’s online properties, and analysis of all the privacy disclosures, to establish whether there has been any infringement of those important transparency requirements.

A Statement of Issues setting out the relevant factual matters and issues for determination was provided to Yahoo for its submissions in September 2021 and submissions were subsequently received on that document. As of the end of 2021, the preparation of a preliminary draft decision was underway.

MTCH Technology Services Limited (MTCH): Tinder platform

The DPC commenced an own-volition inquiry, with respect to MTCH, following the receipt of a number of similar complaints from individuals both in Ireland and across the EU. The issues identified in the complaints related to MTCH’s processing of users’ personal data in connection with the Tinder platform, transparency information relating to that processing, and the company’s compliance with its obligations arising from the exercise of data subject rights. The inquiry is examining whether MTCH has a legal basis for the ongoing processing of its users’ personal data and whether it meets its obligations as a data controller with regard to transparency information and in responding to data subject rights requests. A Statement of Issues setting out the relevant factual matters and issues for determination was provided to MTCH for its submissions in October 2021 and submissions were subsequently received on that document. As of the end of 2021, a preliminary draft decision was under preparation.

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

This Inquiry concerns 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. An Inquiry report issued to the controller in November 2021 for submissions.

Inquiries commenced/at investigative stage during 2021

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 as of the end of 2021 the investigative stage of the inquiry was ongoing.

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

This inquiry concerns transfers by TikTok of the personal data of users of its platform from the EU to China and whether TikTok is complying with requirements under Part V of the GDPR in relation to international transfers of personal data to third countries. The inquiry is also examining whether TikTok is complying with its transparency obligations to users insofar as such data transfers are concerned. The inquiry was commenced in September 2021 and as of the end of 2021 the investigative stage of the inquiry was ongoing.

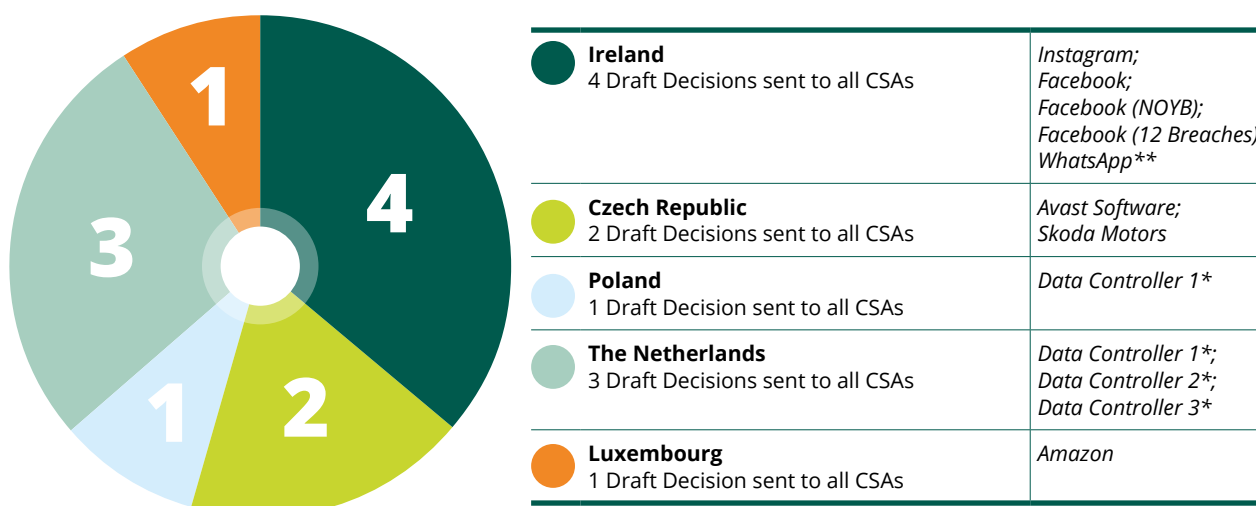
Decisions that have consequences for all European Supervisory Authorities

EDPB guidance on the one-stop-shop mechanism (OSS) is that only EU-based controllers may avail of it. A USA-based controller, for example, targeting services at all EU users may not avail of the OSS unless one of its establishments in the EU itself meets the criteria for main establishment; the USA-based entity cannot itself qualify as the main establishment. Such a controller must deal directly with the individual supervisory authorities for each of the EEA countries where the organisation offers its services. Very many large multi-nationals do not avail of the One-Stop-Shop and so decisions relating to their processing operations made by a supervisory authority are not subject to the cooperation and consistency mechanism of the GDPR.

Where the OSS is in operation, the draft decision of a Lead Supervisory Authority (LSA) must be shared with all other Concerned Supervisory Authorities (CSAs) where the subject of the draft decision operates, via the Article 60 process. In 2021, 11 draft decisions were shared where all 31 EU Supervisory Authorities were considered by the drafting LSA to meet the criteria of Concerned Supervisory Authority. In addition, in 2021, the DPC also shared the **finalised WhatsApp decision** with all EU Member States as CSAs.

The DPC has not raised objections in respect of any of the 7 draft decisions sent to it as CSA in 2021. The graph below illustrates how the draft decisions break down.

Article 60 Draft Decisions circulated by EU DPAs in 2021 where all DPAs were considered CSAs



* The National Laws in these member states may prohibit the naming of the data controllers involved.

** The DPC shared the **finalised WhatsApp decision** in 2021.

DPC Ireland Draft Decisions at Article 60

In 2021 the DPC sent forward **4 large-scale draft decisions** – relating to multinational organisations with operations in all EU member states – where all 31 European Supervisory Authorities met the threshold to constitute a Concerned Supervisory Authority. In addition, the DPC also shared the **finalised WhatsApp decision** with all member-states as CSAs.

As part of the Article 60 process, CSAs are afforded the opportunity to lodge relevant and reasoned objections against a draft decision. The LSA must then acquiesce to an objection or refuse to incorporate it on the basis that it is legally unworkable or runs contrary to an objection lodged by another CSA. Where the LSA is unable to incorporate an objection for these reasons – and the relevant CSA is not disposed to withdraw their objection – the draft decision must then be sent forward to Article 65 (Dispute Resolution).

25 May 2018 – 31 December 2021

Of the 8 EU-wide cross-border draft decisions sent forward by the DPC since May 2018 up to year-end 2021:

- ▶ two were resolved and concluded at Article 60 stage;
- ▶ two went forward to Article 65 Dispute Resolution; and
- ▶ the four remaining have had objections lodged against them

The DPC is presently assessing whether in the latter four cases these objections can be incorporated into the draft decision. Where the DPC is unable to incorporate an objection– and the relevant CSA is not disposed to withdraw their objection – the remaining draft decisions must also be sent forward to Article 65. The table below illustrates where objections were lodged in each case:

DPC Decisions as LSA								
	Twitter	WhatsApp	Instagram	Facebook	Facebook (NOYB)	Facebook (12 Breaches)	Ryanair	Groupon
Austria	✗	✓	✓	✓	✗	✓	✓	✓
Belgium	✓	✓	✓	✓	✓	✓	✓	✓
Bulgaria	✓	✓	✓	✓	✓	✓	✓	✓
Croatia	✓	✓	✓	✓	✓	✓	✓	✓
Cyprus	✓	✓	✓	✓	✓	✓	✓	✓
Czech Republic	✓	✓	✓	✓	✓	✓	✓	✓
Denmark	✗	✓	✓	✓	✓	✓	✓	✓
EDPS	✓	✓	✓	✓	✓	✓	✓	✓
Estonia	✓	✓	✓	✓	✓	✓	✓	✓
Finland	✓	✓	✗	✓	✗	✓	✓	✓
France	✗	✗	✗	✓	✗	✓	✓	✓
Germany*	✗	✗	✗	✓	✗	✗	✗	✗
Greece	✓	✓	✓	✓	✓	✓	✓	✓
Hungary	✗	✗	✓	✓	✓	✓	✓	✓
Iceland	✓	✓	✓	✓	✓	✓	✓	✓
Ireland	✓	✓	✓	✓	✓	✓	✓	✓
Italy	✗	✗	✗	✗	✗	✓	✓	✓
Latvia	✓	✓	✓	✓	✓	✓	✓	✓
Lichtenstein	✓	✓	✓	✓	✓	✓	✓	✓
Lithuania	✓	✓	✓	✓	✓	✓	✓	✓
Luxembourg	✓	✓	✓	✓	✓	✓	✓	✓
Malta	✓	✓	✓	✓	✓	✓	✓	✓
Netherlands	✗	✗	✗	✓	✗	✓	✓	✓
Norway	✓	✓	✗	✗	✗	✓	✓	✓
Poland	✓	✗	✓	✗	✗	✗	✗	✗
Portugal	✓	✗	✓	✗	✗	✓	✗	✓
Romania	✓	✓	✓	✓	✓	✓	✓	✓
Slovakia	✓	✓	✓	✓	✓	✓	✓	✓
Slovenia	✓	✓	✓	✓	✓	✓	✓	✓
Spain	✗	✓	✓	✓	✓	✓	✓	✓
Sweden	✓	✓	✓	✓	✗	✓	✓	✓

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



Objected



Agreed

9



Significant Sanctions and Corrective Measures

Decisions under the Data Protection Act 2018

The DPC decides, on foot of statutory inquiries, whether infringements of data protection legislation have occurred. These statutory inquiries include own volition inquiries and inquiries on foot of complaints. Where infringements are found, the decision-maker also makes a decision as to whether a corrective power should be exercised, and, if so, the corrective power(s) that are to be exercised.

Where the DPC decides to impose an administrative fine, and if there is no appeal against that decision, the DPC must make an application in a summary manner to the Circuit Court for confirmation of the decision to impose an administrative fine pursuant to Section 143(1) of the Data Protection Act 2018. Section 143(2) provides that the Circuit Court shall confirm the decision unless it sees good reason not to.

All DPC fines are remitted to the Exchequer on receipt in accordance with Section 141(7) of the Data Protection Act 2018.

The DPC imposed sanctions of fines and corrective measures in the following cases in 2021

Organisations	Decision Issued
Irish Credit Bureau DAC	23-Mar-21
WhatsApp Ireland Ltd	28-Jul-21
MOVE Ireland	20-Aug-21
The Teaching Council of Ireland	02-Dec-21
Limerick City and County Council	09-Dec-21

Sanctions imposed by the DPC in 2021

Irish Credit Bureau – March 2021

In March 2021, the DPC issued a decision in respect of the Irish Credit Bureau (ICB) regarding a personal data breach that the Irish Credit Bureau had notified to the DPC. The ICB is a credit reference agency that maintains a database on the performance of credit agreements between financial institutions and borrowers. The personal data breach in question occurred when the ICB implemented a code change to its database that contained a technical error. As a result, between 28 June 2018 and 30 August 2018, the ICB database inaccurately updated the records of 15,120 closed accounts. The ICB subsequently disclosed 1,062 inaccurate account records to financial institutions or data subjects before rectifying the issue. All of the inaccurate account records disclosed to the financial institutions stated that the accounts had been closed more recently than they actually had been, but none misstated that a balance was outstanding on the relevant account.

The DPC found in its decision that the ICB had infringed Article 25(1) of the GDPR by failing to implement appropriate technical and organisational measures designed to implement the principle of accuracy in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects. The DPC also found that the ICB infringed Article 5(2) and 24(1) of the GDPR by failing to demonstrate compliance with its obligation, pursuant to Article 25(1) of the GDPR, to undertake appropriate testing of proposed changes to its database.

In its decision, the DPC imposed an administrative fine on the ICB in the amount of €90,000 in respect of the infringements and also issued the ICB with a reprimand in respect of the infringements.

WhatsApp – August 2021

In August 2021, the DPC imposed a fine of €225 million on WhatsApp, arising out of an Inquiry into WhatsApp's provision of information, and the transparency of that information, to both users and non-users of WhatsApp's service.

In addition to the imposition of an administrative fine, the DPC also imposed a reprimand along with an order for WhatsApp to bring its processing into compliance by taking a range of specified remedial actions.

A more extensive update on the DPC's September 2021 decision in respect of WhatsApp can be found at the end of this chapter.

MOVE Ireland – August 2021

In August 2021, the DPC issued a decision in respect of MOVE Ireland (MOVE) regarding a personal data breach that MOVE had notified to the DPC. MOVE is a registered charity, which works in the area of domestic violence, with a primary aim of supporting the safety and wellbeing of women and their children who are experiencing, or have experienced violence/abuse in an intimate relationship. MOVE does this by facilitating male participants in weekly group sessions with a facilitator encouraging them to take responsibility for their violence and to change their attitude and behaviour. The personal data breach in question concerned the loss of eighteen SD Cards that may have contained recordings of group sessions of MOVE's programme where participants discuss their behaviour and attitudes with regard to domestic violence with a facilitator. Whilst the recording of group sessions focused on the delivery of sessions by the facilitators, and it could not be established definitively by MOVE, some of the participants may have been seen and heard in the recordings; furthermore the personal data on the SD Cards may have included participants' disclosure of behaviours, feelings and attitudes towards current or ex partners, other family members and friends, who may have been named by the participants. MOVE informed the DPC that 80 to 120 men may have been affected by this personal data breach and, at least, one facilitator per each recorded session.

In its decision, the DPC found that MOVE had infringed Articles 5(1)(f) and 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 by means of recording group sessions on SD Cards containing participants' and facilitators' personal data. The DPC imposed an administrative fine on MOVE in the amount of €1,500 in respect of the infringements.

Limerick City and County Council - December 2021

In December 2021, the DPC issued a decision in respect of Limerick City and County Council (the Council) in one of a number of own-volition inquiries it has undertaken concerning local authorities. These inquiries consider a broad range of issues pertaining to surveillance technologies deployed by State authorities. The inquiry in this case was conducted initially by means of an audit under Section 136 of the Data Protection Act 2018.

In its decision, the DPC found that certain CCTV systems operated by Limerick City and County Council were unlawful. In reaching this conclusion, the DPC carried out a detailed analysis of the legal bases put forward by the Council for personal data processing involving its use of CCTV cameras for traffic management purposes. The DPC found that these legal bases failed to meet the requirements of clarity, precision and foreseeability and that other certain CCTV systems for the purpose of the deterrence, prevention, detection and prosecution of offences were unlawful in the absence of authorisation from the Garda Commissioner under Section 38 of An Garda Síochána Act 2005.

In its decision, the DPC also made specific findings on over 40 issues, which included findings of infringement of the GDPR in relation to the Council's use of automatic number plate recognition technology and drones in public places which were used for the purposes of prosecuting crime or other purposes. In addition, the DPC found that the Council had infringed Article 15 of the GDPR by rejecting subject access requests in respect of CCTV cameras used for traffic management purposes, that it did not fulfil its transparency obligations under Article 13 by failing to erect signage in respect of its CCTV processing operations, and that it had infringed

Article 12 of the GDPR by failing to make its CCTV Policy more easily accessible and transparent.

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 the infringements, and an administrative fine in the amount of €110,000 was imposed.

The Teaching Council - December 2021

In December 2021, the DPC issued a decision in respect of the Teaching Council (the Council) regarding a personal data breach which had been notified by the Council to the DPC on 9 March 2020. The personal data breach in question had occurred when a phishing email was accessed by two staff members of the Council, which enabled the creation of an auto-forward rule from their email accounts to a malicious email account. As a result, between 17 February 2020 and 6 March 2020 when the auto-forward rule was discovered, 323 emails were forwarded to the unauthorised external email address. The emails contained the personal data of 9,735 data subjects and the sensitive personal data of one data subject.

In its decision, the DPC found that the Council had infringed Article 5(1) and Article 32(1) of the GDPR between 25 May 2018, when the GDPR came into application, and the dates of the personal data breaches, by failing to process personal data in a manner that ensured the appropriate security of the personal data in question, using appropriate technical and organisational measures. The DPC also found that the Council had infringed Article 33(1) of the GDPR by failing to notify the DPC of the personal data breach when it ought to have been aware of it.

The DPC in its decision imposed an administrative fine on the Council in the amount of €60,000, reprimanded the Council and ordered the Council to bring its processing operations into compliance with Articles 5(1)(f) and 32(1) of the GDPR by implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The confirmation and collection of administrative fines under the Data Protection Act 2018

The DPC decides, on foot of statutory inquiries conducted under the Data Protection Act 2018, whether or not infringements of the GDPR and/or the Data Protection Act 2018 have occurred. These statutory inquiries include own volition inquiries and inquiries in respect of complaints. Where infringements are found, the decision-maker also makes a decision as to whether a corrective power should be exercised, and, if so, the specific corrective power(s) that are to be exercised.

Where the DPC decides to impose an administrative fine, and if there is no appeal against that decision, the DPC must make an application in a summary manner to the Circuit Court for confirmation of its decision to impose an administrative fine, pursuant to Section 143(1) of the Data Protection Act 2018. Section 143(2) provides that the Circuit Court shall confirm the DPC's decision unless it sees good reason not to.

In circumstances where the Circuit Court has confirmed the DPC's decision, the DPC then issues the controller or processor concerned with a formal notice requiring payment pursuant to Section 141(5) of the Data Protection Act 2018. The controller or processor then has 28 days to make the payment. All DPC fines are required to be remitted to the Exchequer on receipt in accordance with Section 141(7) of the Data Protection Act 2018. Therefore, upon receipt of the monies in respect of a fine, the DPC remits the full amount to the Exchequer and notifies the Department of Public Expenditure and Reform.

In 2021, applications made by the DPC to confirm seven administrative fines imposed on organisations pursuant to DPC decisions were heard before the Circuit Court. In each case, the Court made an order confirming the decision to impose the fine. The DPC has collected each of those fines and has remitted them to the Exchequer. This total figure for 2021 was €800,000. The details of those confirmation applications are set out below.

Date of application to Court for confirmation of fine	Controller	Date of DPC decision imposing fine	Amount of the fine
23 April 2021	Tusla Child and Family Agency	12 August 2020	€50,000
23 April 2021	Tusla Child and Family Agency	12 August 2020	€35,000
26 April 2021	Tusla Child and Family Agency	21 May 2020	€40,000
26 April 2021	The Health Service Executive	18 August 2020	€65,000
18 October 2021	University College Dublin	17 December 2020	€70,000
18 October 2021	Twitter International Company	9 December 2020	€450,000
5 November 2021	The Irish Credit Bureau DAC	23 March 2021	€90,000

Litigation arising from the DPC's investigation into the processing of personal data in connection with the Public Services Card

December 2021 saw the resolution of legal proceedings commenced in December 2019 by the (now) Department of Social Protection (previously the Department of Employment Affairs and Social Protection, referred to here as the D/SP) in which the D/SP appealed against an Enforcement Notice issued by the DPC in relation to the D/SP's processing of personal data in connection with the issuing of Public Services Cards (PSCs). The background to the litigation, including the findings of the DPC arising from its investigation into processing of personal data in connection with the PSC, and the details of the resolution of the litigation are detailed below.

The DPC's report

On 15 August 2019, the DPC delivered its report in relation to the first part of its investigation into the processing of personal data carried out by the D/SP in connection with the PSC, to include the D/SP's "SAFE 2" registration (for identity authentication) process. The D/SP published the DPC's report on its website⁸ on 17 September 2019, along with its own response.⁹

This first part of the DPC's investigation focused on a defined and limited number of specific issues. In particular, it examined the **legal basis** on which personal data is processed by the D/SP in connection with the PSC, and whether the information provided to data subjects in relation to the processing of their personal data in that context satisfied applicable legal requirements in terms of **transparency**. (The DPC's investigation into certain other aspects of processing by D/SP in connection with the PSC is ongoing, as detailed below).

Legal framework for the DPC's investigation

Because the PSC scheme (and the DPC's investigation) pre-dated the coming into effect of the GDPR (the investigation was commenced in October 2017), the DPC's findings were made by reference to particular obligations imposed on controllers under the Data Protection Acts 1988 and 2003 rather than the GDPR. (This is specifically mandated by Section 8 of the Data Protection Act 2018). For completeness, it should be noted that the DPC's report also included some (non-binding) material addressing applicable provisions of the GDPR.

Findings

A total of **eight** findings were made in the DPC's report. **Three** of those related to the **legal basis** issue; the remaining **five** related to issues around transparency.

Seven of the **eight** findings were adverse to positions advanced by the D/SP insofar as the DPC found that there is, or has been, non-compliance with applicable provisions of data protection law.

In summary terms, the DPC found that:

- ▶ The processing of certain personal data by the D/SP in connection with the issuing of PSCs for the purpose of validating the identity of a person claiming, receiving or presenting for payment of a benefit, has a **legal basis** under applicable data protection law.
- ▶ The processing of personal data by the D/SP in connection with the issuing of PSCs for the purposes of transactions between individuals and other specified public bodies (i.e. bodies other than the D/SP itself) does **not** have a **legal basis** under applicable data protection laws; specifically, such processing contravenes Section 2A of the Data Protection Acts 1988 and 2003.

⁸ Available at <http://m.welfare.ie/en/pressoffice/Pages/pr170919.aspx>

⁹ Under applicable legislation, it was not open to the DPC to publish the report itself. A statement was issued by the DPC on its own website at the time, outlining the scope of the investigation and summarising the report's findings. However, as described further below, following the resolution of the litigation taken by the D/SP in December 2021, the DPC has published its report on its website alongside the details of the terms upon which the litigation taken by the D/SP against the DPC was resolved.

- ▶ The D/SP's **retention** of underlying documents and information provided by persons applying for a PSC on a blanket and indefinite basis contravenes Section 2(1)(c)(iv) of the Data Protection Acts, 1988 and 2003 because such data is being retained for periods longer than is necessary for the purposes for which it was collected.
- ▶ In terms of **transparency**, the scheme does not comply with Section 2D of the Data Protection Acts 1988 and 2003, in that the information provided by the D/SP to the public about the processing of their personal data in connection with the issuing of PSCs was not adequate.

(As per the DPC's statement of 16 August 2019 (referenced above), the DPC also determined that PSCs already issued by D/SP would not be treated as invalid and likewise, individuals who access benefits - including free travel - using their PSC remained free to do so.)

Requirements to address contraventions identified in the report

When delivering its report, the DPC notified the D/SP that enforcement action would be deferred to afford the D/SP an opportunity to identify the measures it would need to implement to bring the PSC scheme into compliance with data protection legislation and to remedy the contraventions identified in the report. The DPC called on the D/SP to develop and submit its implementation plan within a period of 6 weeks, and to ensure that the measures necessary to bring the scheme into compliance would be in place no later than 31 December 2019. Separately, however, the DPC called on the D/SP to take two specific steps within a period of 21 days:

- (1) Cease all processing of personal data carried out in connection with the issuing of PSCs, where a PSC is issued solely for the purpose of a transaction between a member of the public and a specified public body (i.e. a public body other than the D/SP itself).
- (2) Notify all public bodies who require production of a PSC as a pre-condition to entering into a transaction with (or providing a public service to) a member of the public that, going forward, the D/SP would not be in a position to issue PSCs to such persons.

The D/SP's response to the DPC's findings

The D/SP wrote to the DPC on 3 September 2019, noting that, having carefully considered the contents of the report, along with advices received from the Attorney General's office, the Minister for Employment Affairs and Social Protection was satisfied that, contrary to the position of the DPC, the processing of personal data in connection with the PSC had a strong legal basis. The letter also noted the Ministers' position that the information provided to users of the PSC scheme satisfied applicable statutory requirements relating to transparency. Against that backdrop, the letter noted that the Minister considered that it would be inappropriate and potentially unlawful to take the measures required by the DPC. Accordingly, the letter indicated that the Minister had determined that the D/SP would continue to operate the PSC scheme and the SAFE 2 registration process, without modification.

Notwithstanding its rejection of the report, and its refusal to formulate and implement measures to bring the scheme into compliance, the letter of 3 September 2019 proposed that the D/SP and the DPC should nonetheless meet to explore whether measures could be agreed that would obviate the requirement for enforcement proceedings. A statement was issued by the Minister (along with the Minister for Public Expenditure and Reform) on the same date, in terms that reflected the contents of the letter of 3 September 2019.

The DPC replied to the D/SP by letter dated 5 September 2019, explaining the reasons why the DPC considered that, in light of the rejection of the report's findings, and the Minister's stated determination to continue to operate the PSC scheme, without modification, there could be no basis for engagement between the parties in the manner – or for the purpose – suggested. The letter concluded by noting that, since the D/SP was refusing to accept the report's findings, and where it was clear that no implementation plan would be formulated or implemented by the D/SP to address the points of non-compliance identified within those findings, the basis on which the DPC had deferred enforcement action no longer applied. Accordingly, the letter indicated that the DPC would now proceed to enforcement.

Following a further exchange of correspondence between the parties in the intervening period, the D/SP published its response to the DPC's report on its website on 17 September 2019 together with a statement by the Minister. As well as restating that the Minister and the D/SP did not accept the findings contained in the DPC's report, the response and statement reiterated the stated views of the Minister and the D/SP to the effect that the PSC had a robust legal basis and that the D/SP would continue to issue PSCs for use by a number of public bodies across the public sector. The D/SP's response to the report also criticised various aspects of the report, the investigation process which had been followed by the DPC, as well as the process the DPC had called on the D/SP to engage with to identify measures to remedy the contraventions of data protection law identified in the report. The D/SP also reiterated, in categorical terms, its position that it would continue to operate the PSC and SAFE registration process as it had done to that point.

Enforcement action by the DPC and appeal taken by the D/SP

Ultimately an enforcement notice was issued under Section 10 of the Data Protection Acts 1988 and 2003 on 6 December 2019. That notice, which was addressed to the Minister (acting through the D/SP), directed the taking of a range of steps in order to remedy the contraventions identified in the DPC's report. The enforcement notice was appealed by the Minister to the Circuit Court in late December 2019.

Resolution of the appeal proceedings

The hearing of the appeal proceedings taken by the D/SP against the DPC's enforcement notice was due to take place before the Dublin Circuit Court in early December 2021. However a resolution of the litigation was reached between the DPC and the D/SP with the result that the hearing did not go ahead and the proceedings were struck out on 10 December 2021.

The details of the resolution of the litigation reached between the DPC and the D/SP were published on the websites of both the DPC and the D/SP¹⁰. The DPC also published the report on its own website, following agreement by the D/SP.

As part of the resolution of the litigation:

- ▶ it was agreed that further revisions would be made to the D/SP's updated Privacy Statement (which had previously been updated by the D/SP in order to seek to address the DPC's findings in its report concerning the inadequacy of information provided to the public about the processing of their personal data in connection with the issuing of PSCs). The revisions to be made to the Privacy Statement will include information to address: the circumstances in which personal data is shared with the D/SP by other public sector bodies and used to update a person's public service identity (as defined under the Social Welfare Consolidation Act, 2005); and the retention of personal data by the D/SP in connection with the issuing of PSCs;
- ▶ the D/SP acknowledged that, in the absence of legislation making specific provision for this, other public sector bodies cannot compel any individual to acquire a PSC as a precondition to the provision of access to public services. To that end, it was acknowledged by the D/SP that at least one other option must now be provided in any case where an individual is required to verify their identity before accessing other public services;
- ▶ significant adjustments will be made to the D/SP's approach to the retention of personal data submitted by individuals in connection with applications for PSCs, with the D/SP agreeing that, upon completion of a range of changes to be made to its data retention practices, it will not retain personal data submitted by an applicant for a PSC for more than 6 months, save to the extent that such information is held as part of a person's public service identity (as defined under the Social Welfare Consolidation Act, 2005); and

¹⁰ The DPC's report and a notice outlining the terms of the resolution of the litigation are available on the DPC's website at: <https://www.dataprotection.ie/en/news-media/latest-news/dpc-welcomes-resolution-proceedings-relating-public-services-card>

- ▶ The D/SP is to engage with the DPC in relation to the development and implementation of new systems which will give effect to certain terms of the resolution - namely concerning the retention of personal data of applicants for PSCs - including a project involving the deletion and redaction of certain personal data already collected in connection with identity authentication and the issuing of PSCs and currently held by the D/SP.

Continuation of investigation into other aspects of processing by the D/SP concerning the PSC

The DPC is continuing its ongoing (and separate) investigation into the D/SP's use of biometric facial templates in the application of its facial matching software which is used for the purposes of the SAFE 2 registration process when a person applies for a PSC.



Summary of DPC Decision in WhatsApp Transparency Inquiry

On 20 August 2021, the DPC adopted its decision in the WhatsApp Transparency Inquiry. The decision represented the conclusion of an inquiry that commenced on 10 December 2018, the purpose of which was to examine the extent to which WhatsApp Ireland Limited (“WhatsApp”) achieved compliance with its transparency obligations to both users and non-users of its consumer internet-based messaging and calling service.

Background

Following the entry into force of the GDPR on 25 May 2018, the DPC received a number of complaints from individual data subjects concerning the data processing activities of WhatsApp. These complaints were received from both users and non-users of WhatsApp’s service. In addition to this, the DPC also received a mutual assistance request, pursuant to Article 61 of the GDPR, from Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (the German Federal Data Protection Authority). That request touched upon the transparency obligations that are placed on data controllers by the GDPR in the context of the possible sharing of personal data between WhatsApp and a variety of Meta (formerly Facebook) companies.

Following a preliminary examination of the complaints, the DPC observed that, while the precise details of the complaints differed, concerns about transparency featured as a common theme throughout. Having considered the issues arising, the DPC decided to commence an own-volition inquiry pursuant to Section 110 of the Data Protection Act 2018 (“the **2018 Act**”) for the purpose of assessing the extent to which WhatsApp complies with its transparency obligations pursuant to Articles 12, 13 and 14 of the GDPR.

It is important to note that, while the decision to commence an own-volition inquiry was prompted by the common theme running across the various complaints and the above-referenced mutual assistance request, the inquiry did not concern any specific or individual complaint. The DPC has handled, and will continue to handle, any such individual complaints or concerns by way of separate processes under the 2018 Act, as might be required.

Article 60 and the Co-Decision-Making Process

Given that WhatsApp provides its service to individuals throughout Europe, the processing under examination was captured by the definition of “cross-border processing” set out in Article 4(23) GDPR. In the circumstances, Article 60 GDPR envisages a co-decision-making process whereby a draft decision is prepared by the lead supervisory authority for the purpose of enabling the other supervisory authorities concerned to express their views on same and, thereby, input into the decision-making process. WhatsApp’s single establishment in Europe is based in Dublin and, accordingly, the DPC was competent to act as lead supervisory authority for the purpose of the co-decision-making process. The extent of availability of WhatsApp’s service in Europe was such that all of the other data protection supervisory authorities were engaged as concerned supervisory authorities for the purpose of the co-decision-making process.

The Inquiry

The DPC’s inquiry examined the issues arising under three core headings, as follows:

1. Transparency in the context of non-users: this aspect of the inquiry examined the extent to which WhatsApp processes personal data in relation to non-users of its service and whether any such processing gives rise to a requirement for it to comply with the obligations set out in Articles 14 and 12(1) of the GDPR.
2. Transparency in the context of users: this aspect examined the extent to which WhatsApp complies with its obligations under Articles 13 and 12(1) of the GDPR, in the context of its processing of personal data relating to users of the service.
3. Transparency in the context of any sharing of personal data between WhatsApp and the Meta (formerly Facebook) group of companies: this aspect examined the extent to which WhatsApp complied with its obligations under Articles 13 and 12(1) of the GDPR, in the context of any sharing of personal data between it and the Meta (formerly Facebook) group of companies.

In the context of non-users, WhatsApp's position was that it did not, as a data controller, process personal data relating to non-users of the service. It stated that, while it processes the telephone numbers of non-users, it did so as a processor, acting on behalf of users who had activated the contact upload feature. The contact upload feature is a popular voluntary feature of the service that, when activated, allows WhatsApp to upload, to its servers, the mobile phone numbers that are stored in the address book on the user's device for the purpose of determining which of the user's contacts are already using the service. This enables WhatsApp to populate the user's contacts on the service, thereby enabling the user to easily communicate with fellow user contacts. In the case of a non-user, WhatsApp subjects the mobile phone number to a cryptographic hashing process that generates a hash value, following which the mobile phone number is deleted. The hash value is retained and stored by WhatsApp on its servers, in conjunction with details of the derivative user. According to WhatsApp, this enables it to efficiently connect new users with their existing user contacts in the event that they decide to sign up to the service in the future.

In order to determine whether or not the processing that takes place as a result of the activation of the contact upload feature involves the processing of non-user personal data, the DPC firstly examined the nature of a mobile phone number. Having considered the definition of "personal data" set out in Article 4(1) and the provisions of Recital 26 GDPR, the DPC concluded that a mobile phone number, in and of itself, constitutes personal data. The DPC reached this conclusion in light of the unique nature of a phone number, which provides a possible conduit to a particular individual; in other words, while an individual data subject is not necessarily identified by a phone number, he/she can be said to be *identifiable*. The DPC further concluded that, when processing the mobile phone numbers of non-users, WhatsApp did so as a data controller and not a data processor acting on behalf of individual users. This conclusion reflected the factual reality whereby it was WhatsApp, rather than an individual user, that was in a position to exercise control and make decisions concerning the means and purposes of the processing of the non-user data.

Following a consequent assessment of the information that WhatsApp provides to non-users, the DPC reached the view that WhatsApp to have infringed Articles 14 and 12(1).

The DPC then carried out an extensive assessment of the information that WhatsApp provided to users. This assessment identified a significant information deficit, in terms of the information that is required to be provided pursuant to Articles 12(1) and 13 GDPR. The issues identified by the DPC, in this regard, included concerns regarding the manner in which certain information had been presented which, in the view of the DPC, rendered it difficult for the users concerned to receive the information that WhatsApp was required to provide.

The Decision

Article 60 GDPR envisages a process whereby decisions are made by consensus; while the lead supervisory authority is responsible for the preparation of a draft decision, it must take due account of any views that might be expressed by any of the other supervisory authorities concerned. If a concerned supervisory authority decides to express a view by way of a formal objection, the lead supervisory authority is required to take account (or "follow") that objection, failing which, it must submit the matter to the European Data Protection Board ("the **EDPB**") for determination through the dispute resolution process under Article 65 GDPR.

Accordingly, having concluded its inquiry, the DPC prepared and circulated a draft decision to the concerned supervisory authorities on 24 December 2020. That draft decision proposed findings of infringement of Articles 12, 13 and 14. It further proposed the exercise of corrective powers, as follows:

1. A reprimand, to formally identify and recognise the fact of infringement;
2. An administrative fine of an amount between €30 million and €50 million; and
3. An order to bring processing into compliance, requiring WhatsApp to take a range of specified remedial actions to address the issues identified in the draft decision.

While there was a substantial level of agreement amongst the concerned supervisory authorities in relation to the DPC's analysis and proposed findings, a total of eight objections were raised by certain concerned supervisory authorities in response to the DPC's draft decision. Seven comments were also exchanged. The views underlying the comments and objections concerned a range of matters, including suggestions as to additional findings of infringement that might be added to the draft decision as well as the administrative fine that was proposed to be imposed in response to any concluded findings of infringement.

Having considered the matters raised, the DPC prepared and circulated a memorandum to the concerned supervisory authorities on 1 April 2021, addressing the concerns raised and setting out the compromise positions that it proposed to take, in order to try and reach consensus with the supervisory authorities concerned. Ultimately, consensus was not possible and, in the circumstances, the DPC formally confirmed that it was not in a position to follow the objections, as raised. Consequently, the DPC referred the matter to the EDPB on 3 June 2021 for determination pursuant to the Article 65 GDPR dispute resolution mechanism.

The EDPB adopted its Article 65 decision on 28 July 2021 and notified it to the DPC and the supervisory authorities concerned on 30 July 2021. The EDPB required the DPC to follow certain of the objections that had been raised, including those that proposed the amendment of the draft decision to include an additional finding of infringement of Article 5(1)(a) and the upward re-assessment of the proposed administrative fine. The EDPB further reached a determination of the divergent positions that had been taken by the DPC and concerned supervisory authorities in relation to the interpretation and application of Article 83(3) GDPR, which concerns the calculation of administrative fines in cases involving multiple infringements that arise from the same or linked processing operations.

The determination of this particular issue had a very significant impact on the fine that had previously been proposed by the DPC's draft decision in circumstances where the EDPB's decision required the DPC to take account of *each infringement* that was found to have occurred when calculating an administrative fine (as opposed to taking account of only the *gravest of the infringements* that were found to have occurred, as had previously been proposed by the DPC).

The DPC duly amended its decision to take account of the EDPB's decision and the final decision was adopted by the DPC on 20 August 2021.

Subsequent Events

WhatsApp has since exercised its statutory right of appeal against the DPC's decision. WhatsApp has additionally commenced judicial review proceedings concerning both the procedures followed by the DPC as well as the constitutionality of certain aspects of the 2018 Act such that both the DPC and the State are respondents to that action. Both sets of proceedings are currently pending before the Irish High Court. Separately, WhatsApp has also sought to challenge the EDPB's Article 65 decision by way of an annulment action before the General Court of the Court of Justice of the European Union. Matters are at a very early stage and it will likely be a number of years before these legal challenges have concluded.

In the interim, WhatsApp has amended its transparency information for users and non-users in pursuit of compliance with the terms of the order made by the DPC to bring processing into compliance. The order required remedial action to be taken by WhatsApp, to ensure that both users and non-users of WhatsApp's service receive the transparency information that they are entitled to receive pursuant to Articles 12 – 14 GDPR.

10

Litigation

Judgments Delivered and Final Orders made in 2021

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Outcome	Current Status of Case
1	2020/617 JR (2020/126 COM)	Facebook Ireland Limited v. Data Protection Commission [Notice party: Maximilian Schrems]	The High Court Judicial Review proceedings	14 May 2021 (Written Judgment of Barniville J.)	<p>These proceedings are related to the proceedings outlined at no. 2 below. Following the decision of the CJEU in Schrems II (C-311/18 <i>Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems</i>) the DPC commenced an own volition inquiry pursuant to Section 110 of the Data Protection Act, 2018. (That inquiry is examining the lawfulness of data transfers by Facebook Ireland Limited to its US-based parent company, Facebook Inc. via SCCs. The data transfers in question concern personal data of individuals based in the European Union/ European Economic Area. The inquiry is also examining whether and/or which corrective power should be exercised by the DPC pursuant to Article 58(2) of the GDPR, in the event that Facebook Ireland Limited is found to have acted unlawfully and in breach of Article 46 of the GDPR.)</p> <p>In order to commence the inquiry, the DPC issued a Preliminary Draft Decision (“PDD”) to Facebook Ireland Limited on 28 August 2020. The PDD was stated to have two purposes. The first was to notify Facebook Ireland Limited of the commencement of the inquiry. The second was to set out the background/ basis of the inquiry, to set out the DPC’s preliminary view on the issues raised and to invite submissions from Facebook Ireland Limited.</p> <p>In correspondence with Facebook Ireland Limited, the DPC noted that no final decision had been reached and that Facebook Ireland Limited could make submissions in relation to the PDD within 21 days.</p>	Proceedings concluded

Judgments Delivered and Final Orders made in 2021

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Outcome	Current Status of Case
					<p>Facebook Ireland Limited took issue with the DPC's decision to commence the inquiry in the manner it did. As a result, it issued judicial review proceedings against the DPC, which Mr Schrems joined as a notice party. Facebook Ireland Limited maintained that the DPC was not entitled to commence the inquiry by way of the PDD and that the PDD was in effect a premature judgment of the DPC. Facebook Ireland Limited also maintained that the DPC was not entitled to adopt the procedures it adopted, for various reasons.</p> <p>Ultimately, Mr Justice Barniville refused the application by Facebook Ireland Limited for judicial review and held that Facebook Ireland Limited had failed to identify any unfairness in the procedure adopted by the DPC in the PDD. He therefore held that the DPC was entitled to issue the PDD.</p> <p>In respect of costs, the Court ordered Facebook Ireland Limited to pay 90% of the DPC's costs and the costs of Mr Schrems, both to be adjudicated upon in default of agreement.</p> <p>A more extensive update on the DPC's September 2021 decision in respect of WhatsApp can be found in the chapter on Significant Sanctions and Corrective Measures.</p>	

Judgments Delivered and Final Orders made in 2021

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Outcome	Current Status of Case
2	2020/707 JR (2020/146 COM)	Maximilian Schrems v. Data Protection Commission [Notice Party: Facebook Ireland Limited]	The High Court Judicial Review proceedings	13 January 2021	<p>These proceedings also relate to the PDD (referred to in no. 1 above) issued by the DPC to Facebook Ireland Limited in the context of the DPC's own volition inquiry which is examining the lawfulness of data transfers by Facebook Ireland Limited to its US-based parent company, Facebook Inc., via SCCs.</p> <p>Mr Schrems issued Judicial Review proceedings in which he adopted the position that the DPC was bound to address issues relating to the lawfulness of Facebook Ireland Limited's transfers solely by means of the DPC's pre-existing investigation of a complaint previously lodged by Mr Schrems with the DPC. Mr Schrems also contended that the own-volition inquiry amounted to an attempt to exclude Mr Schrems from the procedure in which the substance of his complaint would be considered, in breach of Mr Schrems' right to fair procedures.</p> <p>The proceedings were settled on terms agreed between the parties, pursuant to which the own volition inquiry and complaint-based procedures are being pursued in tandem. Issues relating to costs have not yet been decided by the Court.</p>	Proceedings discontinued
3	2021/67MCA	Fingal County Council v Data Protection Commission	High Court proceedings	1 November 2021 (Final Order)	On consent of the parties, an order was made by the High Court striking out the proceedings, with no order as to costs.	Proceedings discontinued

Judgments Delivered and Final Orders made in 2021

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Outcome	Current Status of Case
4	2019/5964	Nowak v. Data Protection Commissioner and the Courts Service and Pricewaterhousecoopers	Statutory Appeal Dublin Circuit Court	23 November 2021 (Ex tempore Judgment)	<p>By ex tempore Judgment pronounced on 23 November 2021, the Circuit Court refused an appeal brought by Mr Nowak under section 26 of the Data Protection Acts 1988 and 2003. Mr Nowak had sought <i>inter alia</i> an Order setting aside the DPC's decision dated 5 September 2019 in relation to a complaint made by Mr Nowak against the Courts Service.</p> <p>Subsequent to the conclusion of High Court litigation between Mr Nowak and Pricewaterhousecoopers, in which Mr Nowak was unsuccessful, Mr Nowak complained to the DPC alleging that the Courts Service had contravened the Data Protection Acts 1988 and 2003 in its handling of his personal data in the course of legal proceedings between Pricewaterhousecoopers and Mr Nowak. Mr Nowak's complaint was not upheld by the DPC.</p> <p>The Circuit Court, in the appeal taken by Mr Nowak against the DPC's decision, held that Mr Nowak was attempting to circumvent the decision of the High Court and re-litigate the Pricewaterhousecoopers proceedings by complaining to the DPC.</p> <p>The Circuit Court held that the DPC had issued its decision after due consideration and further held that there was no basis upon which to substantiate any of Mr Nowak's grounds of appeal against that decision.</p> <p>In dismissing the appeal, the Circuit Court made an Order for costs in favour of the DPC, the Courts Service and Pricewaterhousecoopers. However, the Circuit Court put a stay of eight weeks on the Order.</p>	Mr Nowak has lodged an appeal with the High Court Central office.

Judgments Delivered and Final Orders made in 2021

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Outcome	Current Status of Case
5	2019/6940	Nowak v. Data Protection Commissioner and the Irish Auditing and Accounting Supervisory Authority	Statutory Appeal Dublin Circuit Court	23 November 2021 (Ex tempore Judgment)	<p>By ex tempore Judgment pronounced on 23 November 2021, the Circuit Court refused an appeal brought by Mr Nowak under section 26 of the Data Protection Acts 1988 and 2003. Mr Nowak sought <i>inter alia</i> an Order setting aside the DPC's decision dated 14 October 2019 in relation to a complaint made by Mr Nowak to the DPC against the Irish Auditing and Accounting Supervisory Authority (IAASA).</p> <p>Subsequent to the conclusion of High Court litigation between Mr Nowak and IAASA in which Mr Nowak was unsuccessful, Mr Nowak's complained to the DPC alleging <i>inter alia</i> that a complaint he had made to IAASA was processed unlawfully and seeking various declarations that the manner in which IAASA had dealt with Mr Nowak's complaint was unlawful. Mr Nowak's complaint was not upheld by the DPC.</p> <p>Having considered the submissions of the parties, the Circuit Court held that Mr Nowak was using the Data Protection Acts 1988 and 2003 in order to try to re-litigate a matter which had already been dealt with by the High Court. Accordingly, the Circuit Court refused Mr Nowak's appeal.</p> <p>In upholding the DPC's decision the Circuit Court held that the DPC had acted completely fairly and within her remit in coming to her decision. The Court made an Order for costs in favour of both the DPC and IAASA but stayed the Order for 8 weeks.</p>	Mr Nowak has lodged an appeal with the High Court

Judgments Delivered and Final Orders made in 2021

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Outcome	Current Status of Case
6	2019/8026	Nowak v. Data Protection Commissioner and the Residential Tenancies Board and the Minister for Housing, Planning and Local Government	Statutory Appeal Dublin Circuit Court	23 November 2021 (Ex tempore Judgment)	<p>By ex tempore Judgment pronounced on 23 November 2021, the Circuit Court refused an appeal brought by Mr Nowak under section 26 of the Data Protection Acts 1988 and 2003. Mr Nowak had sought <i>inter alia</i> an Order setting aside the DPC's decision dated 3 December 2019 in relation to a complaint made by Mr Nowak to the DPC against the Residential Tenancies Board (RTB).</p> <p>Following the conclusion of various High Court litigation between Mr Nowak and the RTB, in which Mr Nowak was unsuccessful in each instance, Mr Nowak complained to the DPC alleging <i>inter alia</i> that his various complaints to the RTB were processed unlawfully. He also sought various declarations that the manner in which the RTB had dealt with his complaints was unlawful. Mr Nowak's complaint was not upheld by the DPC.</p> <p>In refusing Mr Nowak's appeal, the Circuit Court was satisfied that Mr Nowak was seeking to re-litigate issues in relation to tenancy disputes which had already been decided and determined by the Courts. The Court held that the DPC had given fair and due consideration to the various issues involved in the complaint and held that none of the issues identified by Mr Nowak disclosed any valid ground of appeal.</p>	Mr Nowak has lodged an appeal with the High Court

Judgments Delivered and Final Orders made in 2021

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Outcome	Current Status of Case
7	2020/00712	Nowak v. Data Protection Commissioner and the Institute of Chartered Accountants in Ireland, the Irish Auditing and Accounting Supervisory Authority, the Minister for Justice and Equality, the Minister for Business, Enterprise & Innovation, the Commissioner of An Garda Síochána, the Director of Corporate Enforcement, the Attorney General and Ireland.	Statutory Appeal Dublin Circuit Court	23 November 2021 (Ex tempore Judgment)	<p>By ex tempore Judgment pronounced on 23 November 2021, the Circuit Court refused an appeal brought by Mr Nowak under section 26 of the Data Protection Acts 1988 and 2003. Mr Nowak sought <i>inter alia</i> an Order setting aside the DPC's decision dated 3 December 2019 in relation to a complaint made by Mr Nowak to the DPC against the Institute of Chartered Accountants in Ireland (ICAI).</p> <p>Subsequent to the conclusion of High Court litigation between Mr Nowak and the ICAI, in which Mr Nowak was unsuccessful, Mr Nowak complained to the DPC alleging <i>inter alia</i> that he had not consented to his personal data being processed by the ICAI and seeking various declarations including that his personal data was unlawfully processed and that the ICAI had operated unlawfully until 2012 and therefore could not be regarded as a legitimate data controller.</p> <p>In refusing Mr Nowak's appeal, the Circuit Court noted that Mr Nowak was again seeking to re-litigate a matter that had happened 8 years previously and that he was trying to use the Data Protection Acts 1988 and 2003 to circumvent the previous court decisions. The Court held that there was no evidence to justify the merits of Mr Nowak's appeal. The Court further confirmed that there was no lack of investigation by the DPC as alleged by Mr Nowak and that the Court was fully satisfied with the DPC's decision in this case.</p> <p>The Court dismissed the appeal and awarded costs to the DPC and ICAI, but placed a stay of eight weeks on the Order.</p>	Mr Nowak has lodged an appeal with the High Court
8	2019/8593	Department of Employment Affairs and Social Protection v. Data Protection Commission	Statutory Appeal Dublin Circuit Court	10 December 2021	<p>On consent, an appeal brought by the Department of Employment Affairs and Social Protection (as it was then known) against an Enforcement Notice issued by the DPC on 6 December 2019, in respect of the processing and retention of personal data relating to the Public Services Card (PSC), was struck out.</p> <p>An extensive update on the Public Service's Card appeal can be found in the chapter on Significant Sanctions and Corrective Measures.</p>	

Proceedings discontinued

No.	Record No.	Title	Type of action and venue	Date of Judgment/ Order	Outcome	Current Status of Case
9	2019/7318 P	Gerardine Scanlan v. Paul Gilligan and Ors	Plenary proceedings	21 December 2021 (Written judgment)	<p>By written judgment of 21 December 2021, the High Court struck out the proceedings against the nine remaining defendants including the DPC.</p> <p>By way of hearing on 13 and 14 May 2021, the various defendants sought to strike out the proceedings on the basis that they constituted an abuse of process.</p> <p>The Court agreed with the various defendants that the proceedings constituted an abuse of process and accordingly the proceedings were struck out pursuant to the inherent jurisdiction of the court.</p> <p>Further, the Court granted an Isaac Wunder preventing the plaintiff from issuing any further proceedings against the fourth to the seventh named defendants without first seeking the leave of the Court.</p> <p>The matter of costs has not yet been dealt with.</p>	Proceedings concluded save for the issue of costs.

A hand holding a smartphone with a stylized graphic overlay. The graphic consists of two large white numbers '11' on the left, and a series of white geometric shapes on the right, including a diamond, concentric circles, and a semi-circle, all set against a blurred background of a person's face and a smartphone screen.

11

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 **1,013 consultation requests** during 2021. The sectoral breakdown is as follows:

Sector	#	%
Private Sector	522	52
Public Sector	255	25
Multinational Tech Sector	105	10
Health Sector	91	9
Voluntary/Charity Sector	25	2
Law Enforcement Sector	15	2
Total	1,013	

Legislative Consultation

The DPC provided guidance and observations on **over 40** proposed legislative measures in 2021. 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 2021, some of the legislative measures that the DPC engaged in consultation on were:

- ▶ Birth Information and Tracing Bill
- ▶ Building Control (Construction Industry Register Ireland) Bill 2021
- ▶ Circular Economy Bill
- ▶ European Union (Interoperability of electronic road toll systems) Regulations
- ▶ Garda Síochána (Functions and Operational Areas) Bill
- ▶ Garda Síochána (Powers) Bill
- ▶ Garda Síochána (Digital Recording) Bill
- ▶ Health Amendment Act 2021 and secondary legislation relating to implementation of Covid-19 public health measures
- ▶ Judicial Appointments Commission Bill
- ▶ Maritime Area Planning Bill
- ▶ Official Languages (Amendment) Bill
- ▶ Policing and Community Safety Bill
- ▶ Protected Disclosures (Amendment) Bill

- ▶ Road Safety Authority (Commercial Vehicle Roadworthiness) Act 2012 (Use of Information) Regulations
- ▶ Sea Fisheries (Amendment) Bill
- ▶ Sex Offenders (Amendment) Bill
- ▶ Teaching Council (Information to be furnished by employer in case of dismissal or resignation) Regulations 2021
- ▶ Workplace Relations (Miscellaneous Provisions) Bill
- ▶ Inspection of Places of Detention Bill

The DPC also contributed at seven Oireachtas Joint Committee sessions in relation to Bills undergoing pre-legislative scrutiny by the Committees. Appearances before Oireachtas Joint Committees in 2021 have included:

- ▶ Birth Information and Tracing Bill
- ▶ Electoral Reform Bill
- ▶ Garda Síochána (Digital Recording) Bill
- ▶ Garda Síochána (Powers) Bill
- ▶ Online Safety and Media Regulation Bill

Throughout 2021, 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:

Health sector

2021 continued to be a busy year for the DPC in light of the ongoing pandemic. From January the DPC continued to oversee healthcare organisations and departments to ensure data controllers understand the data protection consequences of the processing required to minimise the spread of the Covid virus. The DPC also continued to produce and update guidance on a range of Covid related data protection issues including the Processing Covid-19 vaccination data in the context of employment, data protection implications of the Return to Work Safely Protocol, and the Vaccine Certificate check guidance.

Building on the work carried out in the previous year, the DPC continued to engage with Government Departments to ensure that data protection was given appropriate consideration in the development of public policy and legislation in the context of the pandemic. The DPC began its engagement with and oversight of the health sector on the Vaccine Information database before a single dose had arrived in Ireland and was pleased with the early involvement in the project, as the DPC's previous experience has demonstrated the positive outcomes associated with DPC involvement during project planning stages. A comprehensive Data Processing Impact Assessment (DPIA) on the project was reviewed and DPC feedback was integrated into the project on an ongoing basis, illustrating the value of DPIAs for this type of large scale processing for both citizens as data subjects and data controllers.

The DPC also engaged with the Department of Health in relation to legislation to implement various Covid public health measures, such as passenger locator forms for international travel and vaccination certs for access to hospitality services, to ensure that the principles of data protection were given due consideration in all cases.

2021 saw the signing into law of the Health Research Regulation Amendments. This important piece of legislation sought to improve patient outcomes through the use of health data whilst ensuring the rights of data subjects in terms of their health data are preserved through a range of measures, including clarification of standards required for retrospective chart reviews, pre-screening for the purpose of assessing eligibility/suitability for inclusion in health research, and data subjects' capacity to consent.

Anti-Money Laundering

There are substantive changes in the pipeline from the EU Commission regarding a new Regulation on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AML). Through the Financial Matters Subgroup of the EDPB, we have discussed these proposals with the EU Commission. These new changes to AML requirements and procedures will need to be proportionate and balanced with the GDPR. In that regard, substantive guidance will be needed for all obliged entities / data controllers who will have to comply with both the new AML rules and the GDPR. During 2021 the DPC raised these issues with the Department of Finance, the Central Bank of Ireland and the Revenue Commissioners, and has been involved in various working groups such as the Beneficial Ownership Working Group of the European Business Register Association (EBRA) organised by the Companies Registration Office, and the Financial Action Task Force (FATF) Project for Data Pooling and Data Protection for AML purposes. The work will continue in this area in 2022 to ensure that there is a balanced approach for the operation of AML in conjunction with the GDPR requirements.

Smart metering

Engagement with the Commission for Regulation of Utilities (CRU), ESB Networks and the Department of Environment, Climate and Communications continued in 2021 on the National Smart Meter Programme with a particular focus on the retention of smart meter data and the justification for the periods proposed took place. The DPC continues to engage with certain NGOs concerned on this point. The DPC also provided input to the development of the Smart Data Access Code which will define the rules for access to smart meter data, including the safeguards and procedures necessary to ensure the data is used in a data protection compliant manner.

Insurance

During 2021 the DPC provided detailed observations on Insurance Ireland's draft "Guidance on Data Protection Requirement for Insurers When Handling Personal Data". The guidance is intended to replace the outdated 2013 industry Code of Practice, providing a GDPR compliant document to guide the insurance sector's processing of personal data.



Case Study 26

Covid – 19 Vaccination Status and Schools

During 2021, a number of teachers contacted the DPC to raise concerns about, what they believed, was the processing of staff member's vaccination data by the Department of Education.

Schools across the country have required staff members to complete 'Self Declaration Forms,' if they have been advised to restrict their movements, and provide HSE/medical confirmation of this. One of the listed reasons a person could select to explain why they could not come into work was 'I am a close contact of a confirmed Covid – 19 case'. At the time the concern was raised with the DPC, public health advice indicated that if you were fully vaccinated and had no symptoms, you did not need to self-isolate if you were a close contact. The concern raised with the DPC was that the Department of Education was seeking vaccination status by proxy.

On foot of the concerns raised, the DPC engaged with the Department of Education on the Self-Declaration Form, the reasons for collecting personal data and the legal basis the Department was relying on to carry out the processing. We were informed by the Department that the Self-Declaration Form was required to determine the absence duration of a staff member and the length of contracts to be offered to a substitute teacher.

The Department also cited the lawful basis for the processing and that there was no intention, implied or otherwise, to collect information on the vaccination status of school staff.

Based on the wording of the form and its stated purpose, the DPC concluded that the requirement for employees to complete a Self-Declaration Form did not constitute the processing of special category (health) data by the Department of Education. The DPC's reason for coming to this conclusion was threefold:

- 1) The personal data recorded on the form did not constitute special category data.
- 2) The controllers (schools and Department of Education) were not systematically collecting or processing special category data for an identified purpose.
- 3) The controllers were not further processing the data collected in a manner that revealed or drew inferences about the health status of an individual (such as combining the data with other personal data).

Case Study 27

TikTok and cooperation with other EU data protection authorities

During 2021, GDPR Article 61 mutual assistance requests were received by the DPC from the Dutch and the French data protection authorities. Each of these requests sought the DPC to further investigate a number of concerns relating to TikTok's processing of its users' personal data, particularly child users.

The authorities concerned had been investigating TikTok prior to the company locating its main establishment (EU headquarters) in Ireland in July 2020, following which in December 2020 the DPC assumed the role of TikTok's lead supervisory authority once other EU supervisory authorities had satisfied themselves TikTok was main-established in Ireland.

As a result, the Dutch and French authorities concluded that they no longer had competence to investigate TikTok and accordingly transferred their investigation files, requesting the DPC to investigate further. These investigations coupled with the DPC's own identification of key concerns through active engagement with TikTok in 2021 led the DPC to commence two own-volition inquiries pursuant to Section 110 of the Data Protection Act 2018 in relation to TikTok compliance with requirements of the GDPR.

Case Study 28

Facebook Election Day Information feature

As reported in the DPC's Annual Report for 2020, Facebook suspended its Election Day Reminder feature following the DPC's request that Facebook implement a mechanism to ensure that information on how personal data is used be made available to users in an easily accessible form before a user decides whether or not to interact/engage with the feature. Of particular concern to the DPC was the lack of clarity from Facebook on whether any data generated by a user interacting with the feature would be used for targeted advertising and newsfeed personalisation.

In 2021, Facebook outlined to the DPC a number of changes made to the feature, renamed Election Day Information, to take account of the DPC's recommendations. The changes included the prominent positioning of the 'Learn More' link to the feature specific Help Centre article; and enhanced in-product transparency clarifying that Facebook does not use personal data collected through interactions with EDI for advertising purposes and that Facebook does not share such data with third parties.

Case Study 29

Facebook View (Ray-Ban stories)

During 2021, Facebook, in association with Ray-Ban, launched smart glasses known as 'Ray-Ban stories'. The glasses allow the wearer to take photos and videos of what they see, activated by a touch or voice command.

The images can then be relayed via a Facebook companion app for storage or sharing on social media. While it is acknowledged that many devices including smart phones can record third-party individuals, it is generally the case that the camera or the phone is visible as the device by which recording is happening, thereby putting those captured in the recordings on notice. Ray-Ban stories operate using a small indicator light which activates 'on' when taking a photo or recording.

The DPC engaged with Facebook, highlighting issues around the visibility and duration of this light, requesting that Facebook confirm and demonstrate that the LED indicator light is effective for its purpose. In response, Facebook has made software changes which increase the brightness of the external LED. Facebook also responded to the call from the DPC and the Italian Garante for Facebook to run an information campaign to alert the public as to how this new consumer product may give rise to less obvious recording of their images. Engagement with Facebook will continue into 2022. The DPC also continues to liaise with the Italian Garante in respect of any processing of personal data by Luxottica (the manufacturer of the glasses) whom the Garante is competent to supervise.

Case Study 30

Instagram user self-compromise

In May 2021, the DPC was made aware of incidents whereby users of Instagram were misled into providing their Instagram credentials to third-party apps leading to their accounts being compromised.

Although no EEA users were affected by this particular incident, in order to reduce the likelihood of users being misled in the EEA and similar incidents occurring, the DPC recommended that the data controller should supplement information to users with clear warnings as to the risks posed by these apps.

The controller subsequently updated the Instagram Help Centre articles to provide additional clarity to users about the consequences of allowing such apps to access their accounts and has consolidated all Help Centre articles into a single, dedicated Help Centre page.

Case Study 31

Facebook Viewpoints

During the course of 2021, the DPC engaged with Facebook on the planned launch of Viewpoints in the EU.

Facebook states that Viewpoints is a new market research platform that rewards users for participating in research programmes, the results of which Facebook uses to build and/or improve their products and evaluate new market opportunities. As part of the ongoing cooperation between the DPC and the other EU/EEA Supervisory Authorities, including the French, Italian, Hamburg, Norwegian and Dutch authorities, the DPC communicated to Facebook a number of concerns about the GDPR and ePrivacy compliance of the Viewpoints product.

In December 2021, the DPC accordingly requested Facebook to review the schedule for further rollout in the EU/EEA of the Viewpoint app and the associated programs/surveys so that the DPC and other data protection authorities could further assess and engage with Facebook on the concerns raised. Facebook in response has agreed to pause the EU/EEA rollout of the programme.

12



Children's Data Protection Rights

Public outreach work

Following the publication of extensive draft guidance on children's data protection issues at the end of 2020 (entitled "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing", referred to as the "Fundamentals" for short) and the subsequent launch in December 2020 of a final round of public consultation on this draft guidance which ran for the first quarter of 2021, the DPC spent the early months of 2021 meeting and engaging with representatives from industry as well as key stakeholders in the areas of children's rights and child online safety to discuss initial feedback in relation to various issues addressed in the draft guidance, as well as analysing and synthesising all written submissions received in the course of the public consultation.

Speaking engagements

In tandem, in order to keep industry and the wider public abreast of the DPC's activities in the field of children's policy, staff from the DPC also spoke at numerous external events over the course of 2021, such as the TTC Youth Summit's panel discussion on translating the best interests of the child into product design, a webinar hosted by law firm Lewis Silken entitled "Children's Data – A Global Perspective", and a conference hosted by the euCONSENT consortium entitled "Online Child's Rights, Age Verification and Parental Consent: Finding the Balance". The DPC also recorded a podcast interview for the Association of Compliance Officers of Ireland's Compliance Files series, and for Newstalk's Tech Talk series, in which the DPC's Fundamentals and key children's data protection issues and challenges were discussed at length.

The DPC also recorded a series of videos on children's data protection issues for the ISPPC's new Digital Hub, covering topics such as Protecting Your Children's Data Online, Data Protection and Social Media Platforms, Children's Rights and the Age of Digital Consent, and Targeted Advertising and Profiling.

Participation in external committees

Following an invitation, the DPC became a member of the Advisory Board of a new European Commission-funded project called euCONSENT, which aims to develop a European-wide infrastructure to facilitate interoperable age verification and parental consent mechanisms. The DPC also continued its participation as a member of the National Advisory Council for Online Safety, which this year published an extensive report on its National Survey of Children, their Parents and Adults regarding Online Safety.

Participation in external consultations

In early 2021, the DPC made a submission to the National Council for Curriculum and Assessment's public consultation on the Draft Primary Curriculum Framework, in which the DPC strongly advocated for the creation and inclusion of a free-standing and comprehensive programme for digital citizenship on the national primary school curriculum, a core part of which should be dedicated to educating children specifically about data protection issues. The DPC also submitted written comments to the Organisation for Economic Co-operation and Development's (OECD) stakeholder consultation on its draft recommendation on children in the digital environment and draft guidelines for digital service providers. Closer to home, the DPC also made detailed submissions, at the specific request of the Joint Committee on Media, Tourism, Arts, Culture, Sport and the Gaeltacht, on the General Scheme of the Online Safety and Media Regulation Bill. The DPC subsequently appeared as a witness during that Committee's pre-legislative scrutiny of the Bill in May 2021 to provide further testimony in relation to its submission.

Engagement with statutory bodies


Throughout the course of 2021, the DPC met with several statutory bodies to discuss developments in the area of children's data protection issues, including the Broadcasting Authority of Ireland (which is intended to become the new Media Commission (encompassing a dedicated Online Safety Commissioner) upon entry into force of the Online Safety and Media Regulation Bill), OfCom in the UK and the Federal Trade Commission (FTC) in the United States. The DPC also met with its French and UK counterparts, the CNIL and the ICO, on a number of occasions throughout 2021 to exchange views and discuss the latest developments in both DPA's work on children's data protection rights.

Report on public consultation on the draft "Fundamentals"

In November 2021, following careful analysis and consideration of issues raised in responses to the DPC's consultation on the draft Fundamentals, the DPC published a detailed report on the submissions received. The report focuses on the themes and sections of the draft guidance that attracted the most feedback and commentary, namely the scope of the Fundamentals, the "best interests of the child" principle, the exercise of children's rights, age verification, and profiling for targeted advertising purposes, and sets out the DPC's responses in relation to this feedback.

Publication of final "Fundamentals"

In December 2021, the DPC published the final version of the Fundamentals. This was the culmination of the DPC's intensive work in this area over three years involving three separate stakeholder consultation processes (including a direct consultation with children), engagement with experts in the area of children's rights, expansive research and a two-stage drafting process. The final version of the Fundamentals rests heavily on significant consultations and expert input and is an important step in terms of achieving the higher standards of protection for children's personal data required under the GDPR.



The DPC is determined to drive a transformation in how the personal data of children is handled and the Fundamentals represent an important stepping-stone in this evolution.

The Fundamentals have immediate application and operational effect, now forming the basis for the DPC's approach to supervision, regulation and enforcement in the area of processing of children's personal data.

European Data Protection Board (EDPB) Guidance on Children's Data Protection Issues

In late 2021, the DPC took on a lead role in the preparation at EDPB level of guidance on children's data protection issues alongside a team of co-rapporteurs from Germany, France, Greece and Denmark. The DPC is pleased to be involved in such an important piece of work that seeks to harmonise the approach at an EU level, to be taken to the critical area of the processing of children's data.



13

Data Protection Officers

The DPC continued its compliance work concerning obligations data controllers have regarding the designation and notification of a Data Protection Officer (DPO). In particular, the DPC successfully completed the most recent stage in its DPO enforcement programme, aimed at improving compliance with Article 37 of the GDPR.

The project, which was initiated in 2020, assessed the compliance of public bodies with their obligations under Article 37.7 of the GDPR, which mandates that public bodies are among the specific categories of data controller required to appoint a DPO and notify the DPO's details to the relevant Supervisory Authority.

This initial phase identified over 77 potentially non-compliant public bodies from a total of almost 250. Following the intervention of the DPC, over 70 organisations brought themselves into compliance, raising the sector's compliance rate from 69% to near 100%.

In 2021, the DPC expanded the project to include the private sector, acknowledging that there is no automatic requirement for non-public sector organisations to appoint a DPO. The appointment of DPOs in private sector organisations is determined by the scale and nature of the processing activities involved. With this in mind, the DPC identified several sectors likely to meet the threshold to appoint a DPO. These sectors included Private Hospitals and Out-of-Hours GP Services, Banking Entities, and Credit Unions. A summary of the findings is as follows:

Private Hospitals and Out-of-Hours GP Services

- ▶ 24 Private Hospitals and out-of-hours GP services were identified during the compliance review.
- ▶ Of these, 42% of identified services had appointed a DPO and notified the DPC in accordance with Article 37(7) GDPR.
- ▶ Following DPC intervention, 100% of identified services have brought themselves into compliance with the requirements.

Banking Entities

- ▶ 34 Banking entities were identified during the compliance review.
- ▶ On initial inspection, 74% of identified entities were compliant.
- ▶ Following engagement, 80% of identified entities are in compliance, three entities have given reasons for not appointing a DPO and the remainder are subject to ongoing engagement with the DPC.
- ▶ The DPC will be reviewing the reasons given for not appointing a DPO to ensure the correct application of Article 37(1)(b) and (c).

Credit Unions

Credit Unions were contacted separately to the other banking entities due to the number of credit unions in the country.

- ▶ **242** credit unions were identified during the review.
- ▶ On initial inspection, **29%** of credit unions were in compliance with Article 37(7) and **3%** were in partial compliance.
- ▶ Following first stage engagement, the rate of compliance has risen to **64%**, with **10%** in partial compliance.
- ▶ **13%** of credit unions identified have chosen not to designate a DPO.
- ▶ The credit unions engagement remains ongoing and the DPC will be reviewing the reasons given for not appointing a DPO to ensure the correct application of Article 37(1)(b) and (c).

In total, to date more than 170 additional organisations now comply with Article 37(7) as a result of the DPC's intervention, making DPOs more accessible to individuals seeking to exercise their data protection rights.

In cases of where the DPC identifies persistent non-compliance, further enforcement measures will be taken as proportionate and necessary to ensure compliance with the requirements of the GDPR.

Before extending compliance checks to other sectors, the DPC will consider whether further guidance is necessary to address any issues of concern.

DPO Network

The DPC remains committed to supporting DPOs and their teams; a commitment that has been reiterated among the priorities for the DPC's newly published Regulatory Strategy 2022-2027. This is in recognition of the key role played by DPOs in ensuring that GDPR programmes translate into lasting organisational culture and compliance. As part of the DPC's efforts to empower DPOs in the conduct of their duties, the DPC established a DPO Network in late 2019. The purpose of the Network is to foster peer-to-peer engagement and knowledge sharing between DPOs and data protection professionals.

DPC staff spoke at many virtual events for DPOs during the year, including engagements with sectoral DPO Networks. In recognition of the growing numbers of people who are acting in a data protection advisory capacity for organisations that don't meet the threshold to formally appoint a DPO, the DPC's DPO Network has expanded its scope to include non-designated DPOs.

In Quarter 1, 2022, the DPC will commence a series of online webinars aimed at supporting SMEs in their compliance efforts. Registrations are now open for those who wish to take part. To inquire about the DPC's DPO Network, or to register interest in the SME workshops, please email DPONetwork@dataprotection.ie.

14

International Activities

European Data Protection Supervisory Bodies

During 2021, the DPC continued to participate in the work programmes of the European supervisory bodies for large-scale EU IT systems such as Schengen, Europol, Eurodac, Eurojust, the Customs Information System (CIS) and the Internal Market Information (IMI) system.

Ireland connected to the Schengen Information System (SIS II) on 15 March 2021

The Schengen Information System (SIS) is the most widely used and largest information sharing system for security and border management in Europe. SIS provides Garda Members and Garda Staff who use PULSE with access to real time data on specific alerts; for example persons wanted for criminal purposes, missing persons and objects which have been stolen or are wanted as evidence for a judicial purpose.

In June 2021, a team of experts led by the European Commission carried out an on-site evaluation concerning the implementation of the Schengen Information System in Ireland. In advance of this evaluation, the DPC was required to complete a detailed questionnaire focusing on the DPC's supervision of SIS II and engagement with An Garda Síochána (AGS). As a consequence of Ireland's connection to SIS II, the DPC moved from its longstanding role as 'observer' to become a fully participating member of the data protection supervisory body of the Schengen Information Systems (SIS II). As part of its supervisory duties, the DPC engaged with AGS throughout 2021 on SIS II related matters including data subject information and access rights, Article 36 alerts and SIS II training.

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 applications from multi-national companies

Binding Corporate Rules

Binding Corporate Rules (BCR) were introduced in response to the need of organisations to have a global approach to data protection where many organisations consisted of several subsidiaries located around the globe, transferring data on a large scale. The inclusion of BCR in the GDPR further solidifies their use as an appropriate safeguard to legitimise transfers to Third Countries. During 2021, the DPC continued to act or commenced acting as **lead reviewer in relation to 33 BCR applications** from 19 different companies. The DPC also assisted other European Data Protection Agencies (DPAs) by acting as co-reviewer or on drafting teams for Article 64 Opinions on 13 BCRs in this period.

Furthermore, once the BCR is approved, the DPC continues to have an oversight role receiving annual updates on all BCRs. In 2021 **the DPC led on 23 BCRs** for 16 different companies which are already approved.

The EDPB issued Article 64 opinions on 18 BCR applications in 2021 and the DPC checked and offered feedback on these BCR applications.

Other International Transfer Issues

Staff from the DPC attended 11 meetings of the EDPB International Transfers expert sub-group (ITES) in 2021. This sub-group of the EDPB meets to consider, advise and prepare documentation on matters concerning International Transfers. In addition, staff from the DPC attended 15 other meetings with ITES colleagues for dedicated meetings on matters such as updating BCR documentation, BCR procedures and UK Adequacy.

The EDPB issued Opinions, Guidelines and Recommendations on many Transfers related issues throughout 2021. This included guidelines on the Interplay between Chapter V and Article 3 GDPR and Use of Codes of Conduct as tools for Transfers; recommendations on measures that supplement transfer tools; opinions on the European Commission's decisions on Adequacy of UK and South Korea and on the New EU Commission Standard Contractual Clauses. Staff from the DPC were involved at all stages of these various EDPB publications, participating in drafting teams, providing comments and feedback at the many meetings held to discuss them and actively contributing to the final discussions at Plenary level.

EU Cooperation

Despite ongoing travel restrictions preventing in-person meetings of the European Data Protection Board (EDPB) in 2021, the DPC continued to attend and actively participate at all virtual monthly plenary meetings, in addition to **over 200 expert subgroup meetings**. The EDPB successfully convened in November 2021 the first in-person plenary meeting since the beginning of the pandemic. This provided a valuable opportunity for the DPC to engage directly with EU data protection authority colleagues and plan future bi-lateral meetings and possible collaborations.

Cooperation with other EDPB supervisory authorities 2021

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.

- ▶ Article 61 Voluntary Mutual Assistance
Notifications sent to Ireland – 576
- ▶ Article 61 Voluntary Mutual Assistance
Notifications sent by Ireland – 828

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

- ▶ Article 61 Mutual Assistance requests sent to Ireland – 26
- ▶ Article 61 Mutual Assistance requests sent by Ireland – 94

International Activities

18-21 October Global Privacy Assembly

In October 2021 the DPC participated in the Global Privacy Assembly (GPA); the annual conference attended by over 130 international data protection and privacy authorities. The 2021 event took place fully online and was hosted by the Mexican supervisory authority. Mexico has also now taken over from the United Kingdom as the Chair of the GPA.

ARC Project

The DPC continued to contribute to the deliverables set out by the EU as part of its role within the ARC Awareness Raising Campaign aimed at SMEs, in conjunction with the Croatian Data Protection Agency AZOP, and Vrije University Brussels. Educational materials were drafted and uploaded to the ARC website, **a survey was conducted engaging with 300 SMEs**, and prep work for a number of workshops and a conference was conducted. Unfortunately, due to increasing restrictions towards the end of the year, both the conference and the workshops have been postponed until 2022.

15



Communications

Media Engagement

The DPC published a total of 14 press releases over the course of 2021, leading to significant coverage on international and national level media. Specific announcements included the launch of an inquiry into processing of personal data by the Department of Health, the achievements of the DPO enforcement programme – with an additional 170 organisations brought into compliance, and the confirmation of the €450,000 fine imposed on Twitter.

Direct Engagement

Despite the ongoing restrictions in place, direct engagement with stakeholders remained a high priority throughout 2021. The DPC continued to engage with a variety of both Irish and international stakeholders. The Commissioner and members of staff contributed to over 90 events in 2021. The majority of these events were virtual, but some were in-person events, in line with official health guidance in place at the relevant time.

Guidance and Educational Material

As part of the ongoing educational remit of the DPC, wide-ranging guidance on a variety of topics for both individuals and organisations was drafted and distributed throughout the year. Almost 10 items of guidance were produced in 2021, covering a wide range of issues ranging from the collection of personal data prior to viewing a property to vaccine certificate checks. Of particular note was the publication of the finalised Fundamentals for a Child-Oriented Approach to Data Processing in December, which received a warm reception from stakeholders across all channels.

Social media

The DPC's social media platforms continued to play an important role in the communications of the DPC in 2021. The growth of the DPC's social media presence across Twitter, Instagram and LinkedIn, was integral to the support of its awareness-raising and communications activities. The combined followers across the three platforms has **increased by over 6,000 during 2021, to over 35,000**. There was an organic reach of over 2.1 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 as an important resource for individuals and organisations throughout 2021. 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 2021.

16

Corporate

DPC Funding and Staffing

The funding of the DPC by government has increased year-on-year from €1.7 million in 2013 to **€19.1 million in 2021** (comprising €12.76 million in pay and €6.36 million in non-pay allocation). The funding for 2021 represented an increase of €2.2M on the 2020 allocation.

The DPC continued to progress the transfer of Corporate Functions from the Department of Justice in 2021. A Ministerial Order designating the Commissioner for Data Protection as the Appropriate Authority, under Section 20(2) of the Data Protection Act 2018, was signed in November 2021. Data Protection Commission employees, who were previously employed by the Department of Justice, are now employees of the DPC.

The DPC has established a new Strategic Human Resources function, People and Learning, in support of the Data Protection Commission's values, vision and mission, as outlined in our new Regulatory Strategy, 2022 – 2027.

It is the purpose of the new People and Learning function to support the whole organisation in meeting its goals through its most valuable resource, our people. In 2021, the new function continued to focus on an intensive recruitment programme, growing our headcount from 145 in 2020 to 190 at year-end. We will continue to drive recruitment during 2022, with a target headcount of 260, through a combination of open recruitment, and the promotion and development of our own people. We will be strengthening and expanding our senior management structure, with the appointment of two key positions at Director level.

Work began on a Learning & Development strategy in 2021, through a Skills Transformation lens. A new DPC Employee Engagement forum, together with the introduction of an Industrial Relations Framework, provides an employee voice mechanism which will contribute to enhancing trust, innovation, productivity and organisational improvement.

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 2021 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 members of the Committee are:

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

Eight meetings of the Audit and Risk Committee were held in 2021.

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.

During 2021, the DPC continued to meet its on-going business objectives despite the continuation of the Covid-19 pandemic and resulting challenges through the continuation of measures enacted via the business continuity plan at the outset of the crisis in 2020; increasing the capacity of the organisation to work remotely and ensuring the safety of staff. Senior management monitored this risk throughout 2021.

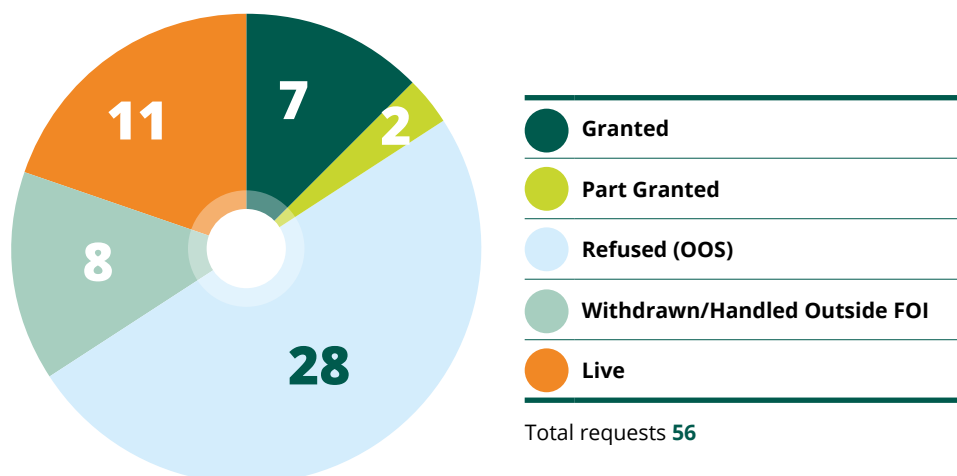
Building organisational capacity to meet the enhanced functions of the organisation under the GDPR and national legislation continued to be a key priority for the DPC in 2021 and the challenges around meeting this objective were reviewed regularly as part of risk management.

Official Languages Act 2003

The DPC's fifth Language Scheme under the Official Languages Act 2003 commenced with effect from 21 December 2020 and remained in effect for a period of three years.

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 Requests



Freedom of Information (FOI)

In 2021, the DPC received a total of 56 FOI requests.

Seven were granted, two were partially granted and 28 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. Granted 7 Part Granted 2 Refused (OOS) 28 Withdrawn/Handled Outside FOI 8 Live 11 Total requests 56

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.

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.

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.

A key achievement in 2021 was the publication of the DPC Regulatory Strategy 2022 – 2027 which 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.

For staff of the DPC, an Employee Engagement Forum was established following the transition of staff to the DPC as its own employer in 2021. The Forum is made up of DPC staff from all grades and was formed having regard for gender balance.

Staff of the DPC had the opportunity to avail of training in 2021 including data protection. Well-being of staff continued to be a key focus and measures are in place to raise awareness of the supports in place for staff.

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 published audio resources. The Duty is also embedded into the Corporate Governance Framework and the Customer Charter and Action plan, published in 2021.

During 2021, the DPC continued to review its service delivery and sought to ensure that it continued to be accessible to customers whilst DPC staff delivered this service remotely. 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

In 2021, the revised Customer Charter and accompanying Quality Customer Service Action Plan and Managing Unreasonable Behaviour and Contacts Policy for 2021 – 2023 were published on the DPC website.

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

Appendices

Appendix 1:

Report on Protected Disclosures received by the Data Protection Commission in 2021

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 internally genuine concerns about possible 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 2021:

- ▶ No internal protected disclosures (from staff of the DPC) were received.
- ▶ 16 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). Four of the disclosures were accepted as valid protected disclosures.

Reference Number	Type	Date Received	Status	Outcome
01/2021	Section 7 (external, to 'prescribed person')	01 February 2021	Open	Accepted and referred for potential investigation. Ongoing at year-end.
02/2021	Section 7 (external, to 'prescribed person')	05 February 2021	Closed	Accepted. The DPC engaged with the Data Controller on the issues raised.
03/2021	Section 7 (external, to 'prescribed person')	10 February 2021	Closed	Insufficient detail provided, complaint did not follow up when requested.
04/2021	Section 7 (external, to 'prescribed person')	30 March 2021	Closed	Not accepted as a valid protected disclosure.
05/2021	Section 7 (external, to 'prescribed person')	01 June 2021	Closed	Not accepted as a valid protected disclosure, referred as a potential complaint.
06/2021	Section 7 (external, to 'prescribed person')	12 June 2021	Closed	Insufficient detail and made anonymously.
07/2021	Section 7 (external, to 'prescribed person')	24 June 2021	Closed	Not a protected disclosure on follow up. Standard complaint made.
08/2021	Section 7 (external, to 'prescribed person')	14 July 2021	Closed	No information provided. Complaint did not follow up when requested.
09/2021	Section 7 (external, to 'prescribed person')	31 August 2021	Closed	No allegations made. Complainant did not follow up when requested.
10/2021	Section 7 (external, to 'prescribed person')	07 September 2021	Closed	Insufficient detail. Complainant did not provide information when requested.
11/2021	Section 7 (external, to 'prescribed person')	09 September 2021	Closed	No allegations made. Complainant did not follow up when requested.
12/2021	Section 7 (external, to 'prescribed person')	08 October 2021	Closed	Not a data protection matter, withdrawn by complainant.
13/2021	Section 7 (external, to 'prescribed person')	22 October 2021	Closed	No allegations made. Complainant did not make a disclosure when contacted.
14/2021	Section 7 (external, to 'prescribed person')	15 November 2021	Open	Accepted and referred for potential investigation. Ongoing at year-end.
15/2021	Section 7 (external, to 'prescribed person')	15 December 2021	Closed	Not accepted as a valid protected disclosure, referred as a potential complaint.
16/2021	Section 7 (external, to 'prescribed person')	17 December 2021	Open	Accepted and referred for potential investigation. Ongoing at year-end.

Appendix 2:

Report on Energy Usage at the Data Protection Commission

Overview of Energy Usage

General

During 2020 and 2021, the DPC operated remote working for its staff. However, all offices were open during this time to facilitate staff to access printing facilities, sign formal documents or arrange for registered post to be issued.

Staff were also on-site to ensure regular maintenance of equipment, issue equipment to new staff, process incoming post, implement Covid-related protocols and accept deliveries.

There has been a reduction in energy consumption in all buildings, with a 59% reduction recorded in the Fitzwilliam Square office for 2020.

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.

Portarlinton

The Portarlinton 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 2020 (last validated SEAI figures available) is as follows:

	Electrical	Natural Gas
Dublin		
Fitzwilliam Sq.	38,959KwH	
Satellite Office	62,545KwH	
Portarlinton	24,000KwH	39,566

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 Portarlinton office as units fail or require replacement bulbs
- ▶ Sensor lighting in use in one office (Satellite)
- ▶ Review of heating system in one office underway (Fitzwilliam Square)

- ▶ New Tender competition completed for bin collection services to include compost bin service for Portarlinton and Fitzwilliam Square. This was suspended for 2021 as there were too few staff in the offices to make this practical.

Reduction of Waste Generated

- ▶ DPC use a default printer setting to print documents double-sided.
- ▶ DPC has also introduced dual monitors for staff to reduce the need to print documents to review / compare against other documentation during casework.
- ▶ DPC provide 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:

Barniville Judgment: Facebook Ireland Limited v. Data Protection Commission and Maximilian Schrems

Facebook Ireland Limited v. Data Protection Commission and Maximilian Schrems (Notice Party)
[High Court Record No. 617/2020 JR]

Summary of the High Court Judgment of Mr. Justice Barniville delivered on 14 May 2021

1. Background

On 16 July 2020, the Court of Justice of the European Union ("CJEU") delivered its decision in proceedings titled *Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems*, Case No. C-311/18. In its judgment, the CJEU held that, where personal data is transferred from the EU to a third country, a level of protection equivalent to that provided by the EU must be provided by the third country. The CJEU found that such protection is not available in the United States and on that basis it struck down the EU-US Privacy Shield transfer mechanism.

Whilst noting that the Standard Contractual Clauses ("SCCs") may provide a basis for the lawful transfer of data to a third country which does not itself provide a level of protection equivalent to that available in the EU, the Court noted that a case by case assessment is required in respect of each such transfer to determine whether, on the particular facts of the transfer under scrutiny, the SCCs provide sufficient protection (in and of themselves) for the personal data being transferred to the third country, **or** whether safeguards need to be adopted supplemental to the SCCs, **or**, as may be the case in some instances, the SCCs do not offer a sufficient level of protection, even if supplemented with additional safeguards.

2. Facts

Following the delivery of the CJEU's judgment, the DPC wrote to Facebook Ireland Limited ("**Facebook Ireland**") on 28 August 2020 to notify it of the commencement of an "own volition" inquiry ("**the Transfers Inquiry**") pursuant to Section 110 of the Data Protection Act, 2018 (the "**2018 Act**"). The DPC's letter noted that, in its inquiry, it would examine (and determine the lawfulness of) data transfers made by Facebook Ireland to its US-based parent company, Facebook Inc. via SCCs. The data transfers in question concern the personal data of individuals based in the European Union/ European Economic Area. The letter also flagged that the DPC would determine whether (and, if so, which) corrective power should be exercised by the DPC pursuant to Article 58(2) of the GDPR in the event that the DPC found that Facebook Ireland was acting unlawfully and infringing Article 46(1) of the GDPR. (This article requires that there must be appropriate safeguards, and enforceable rights and legal remedies for data subjects, where data transfers are taking place to a location outside of the EU in respect of which there is no European Commission adequacy decision).

The DPC's letter also enclosed a Preliminary Draft Decision ("**PDD**"), the purpose of which was to identify the issues the subject of the Transfers Inquiry and to set out the DPC's preliminary views on those issues. As such, the document served as a preliminary draft of a draft decision which, having first considered such submissions as may be received from Facebook Ireland, the DPC would in due course submit to the co-decision-making procedure provided for at Article 60 of the GDPR.

Having noted that no action would be taken by the DPC pursuant to the PDD itself, Facebook Ireland was invited to submit a written response to the issues canvassed in the PDD within a period of 21 days.

Facebook Ireland objected to the DPC's decision to circulate the PDD at the commencement of the Transfers Inquiry. It issued judicial review proceedings against the DPC and obtained a stay (stop) on the inquiry until such time as its judicial review proceedings were heard and decided. Mr Schrems, sought to be, and was subsequently, added as a notice party to the proceedings as an interested party.

In its proceedings, Facebook Ireland relied on the following grounds of challenge (amongst others):

- (1) Even though the DPC had stated that no action would be taken on foot of the PDD, it claimed that the PDD and the DPC's procedures were nonetheless amenable to judicial review;
- (2) It claimed that the DPC had an obligation to conduct an investigation prior to issuing the PDD;
- (3) It claimed that the DPC had acted in breach of its legitimate expectations in terms of how the Transfers Inquiry would be conducted. This submission was two-fold:-
 - (a) Firstly, Facebook Ireland submitted that it had a legitimate expectation that the procedures set out in the DPC's 2018 Annual Report in respect of the progression of inquiries would be applied to the Transfers Inquiry. Asserting that the procedure adopted by the DPC differed significantly from its published procedures, Facebook Ireland claimed that the DPC was acting unlawfully.
 - (b) Secondly, Facebook Ireland submitted that the Transfers Inquiry should be conducted in a manner similar to other inquiries conducted by the DPC. Facebook Ireland maintained that this was the only inquiry in which the DPC had issued a PDD at the outset. Facebook Ireland also noted that the DPC did not provide reasons for departing from its previous practices.
- (4) Facebook Ireland claimed that its right to fair procedures was breached, e.g. because it was given just 21 days to make submissions in response to the PDD.
- (5) Facebook Ireland claimed that by issuing the PDD at the outset, the DPC had prematurely come to a judgment on the issues to be decided in the Transfers Inquiry.
- (6) It was claimed that the DPC had failed to take into account relevant considerations. In particular, the DPC had not awaited publication of the European Data Protection Board ("EDPB") guidelines/ recommendations to assist controllers and processors in relation to the use of what are called "supplementary measures" to ensure adequate protection for data subjects when transferring data to third countries.
- (7) Facebook Ireland claimed that the DPC had breached Facebook Ireland's right to equal treatment and non-discrimination.
- (8) It was claimed that the DPC had breached its obligation to act proportionately by subjecting Facebook Ireland to simultaneous inquiries. In other words, Facebook Ireland contended that it was disproportionate for Facebook Ireland to be subjected to two simultaneous inquiries in relation to substantially the same subject matter, namely, the Transfers Inquiry and its (separate) consideration of Mr. Schrems' complaint.
- (9) Facebook Ireland also claimed that the DPC breached its duty of candour in the way in which it defended the proceedings. In other words, Facebook Ireland believed that the DPC breached this duty by failing to answer questions raised by Facebook in correspondence between the parties.

The DPC opposed Facebook Ireland's case on all grounds as follows:

- (1) The DPC submitted that the issuing of decision the PDD was not amenable to judicial review.
- (2) The DPC also rejected Facebook Ireland's assertion that no investigation was conducted by the DPC before issuing the PDD.

- (3) The DPC disputed Facebook Ireland's allegation that Facebook Ireland had a legitimate expectation as to how inquiries would be conducted. In doing so, the DPC rejected Facebook Ireland's contention that the 2018 Annual Report or material published on the DPC's website created any legitimate expectation on the part of Facebook Ireland in this regard. The DPC also maintained that it did carry out an investigation prior to commencing the inquiry and that it would continue to carry out its investigation if the inquiry was permitted to continue. The DPC also referred to the express terms of the relevant section of the 2018 Annual Report (pages 28-29) which noted that the report was "not determinative of the precise steps which will be followed in each inquiry" and that those steps would depend on the "nature, circumstances, scope and subject matter of the inquiry". The DPC also emphasised that the "provisional sequencing" for inquiries (as it was described in the 2018 Annual Report) was expressly stated to be "subject to changes".
- (4) The DPC opposed Facebook Ireland's allegations of breaches of fair procedures and noted that no extension of time in which to respond to the PDD was sought by Facebook Ireland, nor was any extension of time refused by the DPC. The DPC maintained that, in proceeding as it did, it sought to give full and timely effect to the CJEU judgment of 16 July 2020. The DPC also rejected accusations of premature judgment and submitted that the views set out in the PDD were expressly provided to be preliminary only and were subject to any further submissions made by Facebook Ireland. The DPC emphasised that Facebook Ireland had been invited to submit any further information it felt was necessary in response to the DPC's preliminary views as set out in the PDD.
- (5) The DPC maintained that it was and is entitled and obliged to proceed as it did, notwithstanding the absence of guidelines or recommendations from the EDPB.
- (6) The DPC disputed the allegations of unequal treatment and discrimination.

- (7) The DPC also disagreed with Facebook Ireland's allegations of a breach of proportionality, by reason of the existence of the inquiry and the ongoing complaint by Mr Schrems. Therefore, it did not accept that being subjected to parallel processes gave rise to any disproportionality. The DPC noted that the GDPR and the 2018 Act envisaged that both forms of inquiry were available to the DPC.
- (8) The DPC also rejected any breach of the duty of candour in its defence of the proceedings.

As a notice party to the proceedings, Mr Schrems:-

- (1) Supported the quashing of the PDD, claiming that it infringed his legitimate expectation that his complaint would be determined by the DPC following the CJEU's judgment of 16 July 2020.
- (2) Also supported Facebook Ireland's submission in relation to the disproportionality of the DPC conducting simultaneous inquiries.
- (3) Opposed the allegation that the DPC had departed from its published procedures in issuing the PDD and commencing the own-violation inquiry. Mr. Schrems submitted that, in any event, the 2018 Annual Report did not give rise to any legitimate expectation that the particular procedures set out would be followed in all cases and noted that the procedures referred to were stated to be "illustrative".
- (4) Disagreed with Facebook Ireland's submission that the DPC was obliged to await publication of the EDPB guidelines before proceeding with its inquiry. Mr Schrems noted the DPC's obligation under the GDPR and the judgment in the CJEU judgment of 16 July 2020 to act expeditiously. On that basis, Mr Schrems also disputed Facebook Ireland's submission that it was afforded insufficient time to make submissions in response to the PDD.

It should be noted that the judicial review proceedings concerned the procedural rights and obligations of the DPC, Facebook Ireland and Mr Schrems in the context of the DPC's Transfers Inquiry. The proceedings were therefore not concerned with the merits of the preliminary views expressed by the DPC in its PDD.

3. Judgment of the High Court (Mr Justice Barniville)

In his judgment, Mr Justice Barniville considered the following points:-

- (1) Whether the DPC's decision to issue the PDD and the procedures which the DPC chose to adopt in respect of the inquiry are amendable to judicial review.
- (2) Whether the DPC had failed to carry out an investigation/inquiry prior to reaching a decision in breach of the 2018 Act, the GDPR and the judgment of the CJEU of 16 July 2020.
- (3) Whether the PDD and the procedure adopted by the DPC was a departure from the DPC's published procedures and in breach of Facebook Ireland's legitimate expectations.
- (4) Whether the DPC breached Facebook Ireland's right to fair procedures in the inquiry by affording Facebook Ireland a period of three weeks (21 days) to provide its submissions to the DPC.
- (5) Whether the DPC breached Facebook Ireland's right to fair procedures by reaching a premature judgment on the inquiry.
- (6) Whether the DPC breached Facebook Ireland's right to fair procedures by adopting a procedure in which the Commissioner for Data Protection was involved in the investigation and was also the sole decision-maker.
- (7) Whether the proposed adoption of a single decision to cover infringement and corrective measures was ultra vires to Section 111 of the 2018 Act.
- (8) Whether the DPC was required to await the recommendations/guidance from the EPDB before deciding to proceed with the own-volition inquiry and/or whether the DPC failed to take into account the timing of the EDPB recommendations/guidance as a relevant factor in its decision to proceed with the inquiry.
- (9) Whether, in deciding to commence an inquiry with respect to Facebook Ireland and not other persons or bodies involved in EU-US data transfers, the DPC unlawfully discriminated against Facebook Ireland and/or breached its right to equality under Irish and EU law.
- (10) Whether the DPC acted disproportionately in commencing the own-volition inquiry involving Facebook Ireland while its consideration of Mr Schrems' complaint was still ongoing.
- (11) Whether the DPC failed to set out adequate reasons for various decisions which it had taken in connection with the own-volition inquiry involving Facebook Ireland, including its decision to adopt the particular procedure which it decided to adopt notwithstanding its published procedures for inquiries.
- (12) Whether the DPC was in breach of its duty of candour and, if so, the consequences of such a breach.
- (13) Whether the proceedings by Facebook Ireland were an "abuse of process" as had originally been contended by the DPC. (It should be noted that during the course of the hearing, the DPC withdrew its allegations of abuse of process.)

Mr Justice Barniville concluded that the DPC's decision to issue the PDD and to adopt the procedures it did are amenable to judicial review on the basis that the commencement of the inquiry by the DPC had legal consequences for Facebook Ireland.

In considering Facebook Ireland's submission on whether the DPC had an obligation to conduct an investigation before issuing the PDD, Mr Justice Barniville referred to provisions of the 2018 Act and noted that the DPC has a wide discretion to regulate its own procedures. Noting that the PDD was used to commence the inquiry and to notify Facebook Ireland of the preliminary views of the DPC regarding the lawfulness of data transfers to its US-based parent, Mr Justice Barniville was satisfied that the DPC had not reached any final decision on the issues contained within the PDD.

On the question as to whether the legitimate expectations of Facebook Ireland had been breached by the procedure applied by the DPC, Mr Justice Barnville reviewed the relevant sections of the DPC's 2018 Annual Report (pages 28 - 29), together with information published on the DPC's website. Mr Justice Barnville held that this information did not give rise to any legitimate expectation on the part of Facebook Ireland, as claimed. In particular, Mr Justice Barnville highlighted the fact that the DPC had a wide discretion under the 2018 Act to regulate its own procedures. Mr Justice Barnville also referred to the wording contained in the DPC's 2018 Annual Report and noted that there were express "qualifications" to the effect that the procedures described could be altered by the DPC.

With regard to the 21-day period afforded to Facebook Ireland to make submissions to the DPC, Mr Justice Barnville had regard to the proceedings that gave rise to the CJEU judgment of 16 July 2020 and noted that, in that particular context, he was not satisfied that the 21-day time period provided for was inadequate, as contended for by Facebook Ireland.

In considering Facebook Ireland's submission that the PDD constituted a premature judgment by the DPC, Mr Justice Barnville held that the PDD was clearly a preliminary decision, and not a final decision. Mr Justice Barnville considered that there was nothing impermissible about placing an onus on Facebook Ireland to change the DPC's views based on the PDD and that it was fair for the DPC to adopt the procedure taken.

Mr Justice Barnville rejected Facebook Ireland's submission that it was treated unequally and discriminated against by the DPC. While Facebook Ireland had claimed that other organisations were not subject to the same investigations by the DPC, Mr Justice Barnville was satisfied that the particular focus on Facebook Ireland by the DPC was clear, given Mr Schrems' initial complaint against Facebook Ireland. Mr Justice Barnville also noted that the PDD provided clear reasoning as to why the DPC had initiated an inquiry against Facebook Ireland. On this basis, Mr Justice Barnville was satisfied that the DPC was not obliged to provide reasons for not pursuing similar inquiries against entities similar to Facebook Ireland.

Mr Justice Barnville further held that there was no breach of candour in the proceedings by the DPC.

4. Conclusion

Ultimately, Mr Justice Barnville refused Facebook Ireland's application for judicial review and held that Facebook Ireland had failed to identify any unfairness in the procedure adopted by the DPC in issuing the PDD. As such, Facebook Ireland's case was dismissed.

Facebook Ireland was ordered to pay 90% of the DPC's legal costs, and the costs of the Notice Party.

Appendix 4:

Audits of Political Parties

In 2021, the DPC decided to audit certain data processing activities by all twenty-six registered political parties in the State. The audits were conducted under Article 58.1(b) of the GDPR, which empowers each data protection supervisory authority to carry out investigations in the form of data protection audits. The decision to conduct the audits followed reports in the media concerned the alleged storing by one political party, Sinn Féin, of personal information of millions of voters on an internal party database and by further media articles that alleged that members of some political parties posed as market researchers in conducting opinion polls. The DPC audits of political parties examined the designation of data protection officers; the use of Registers of Electors and Marked Electoral Registers; Party Membership/Volunteers Databases; Databases of Electors/Voters; Data Protection Impact Assessments; and Market Research/Opinion Polling.

On 10 December 2021, the final audit reports were issued to all twenty-six political parties. Drawing from the contents of those twenty-six audit reports, the DPC published an overall report entitled “Data Protection Audit of Political Parties in Ireland” on 20 December 2021, which highlighted the main findings of its data protection audits and outlined the key recommendations made by the DPC to the political parties concerned.

Below is a brief synopsis of key points from within the overall report.

Designation of Data Protection Officer

Data controllers are obliged to designate a data protection officer where their core activities consist of processing on a large scale of special categories of personal data, such as data revealing political opinions.

During the course of the audits, the DPC considered the extent to which political parties process, on a large scale, personal data revealing political opinions. As data protection legislation does not prescribe a figure to quantify the term ‘on a large scale’ for such data processing, the DPC decided to guide where that figure should be set, with the benefit of information obtained from the political parties during the audits.

The DPC determined that the appropriate threshold that should be met in order for a political party to be considered to process personal data revealing political opinions on a large scale is 30,000 records of data subjects.

Arising from that guidance and based on the information supplied by the political parties to the DPC, it follows that only two political parties, namely Fianna Fáil and Sinn Féin, are required to designate data protection officers. Both have done so.

There is no requirement on the other political parties to designate data protection officers while the level of data processing revealing political opinions remains below the threshold but they may choose to voluntarily designate a data protection officer if they wish.

Party Membership/Volunteers Databases

The audits found that the dominant level of data processing by political parties occurs in respect of the personal data of party members and volunteers as most parties keep and process membership or volunteer records. Accordingly, the majority (approx. 60%) of the recommendations made in the audit reports related to the processing of those records.

Register of Electors and Marked Electoral Register

The use of data from the Register of Electors and the Marked Electoral Register, while not widespread across all political parties, attracted some attention in the audits with regard to the need to comply with transparency requirements by updating privacy policies to reflect this data processing activity and the need to set data retention periods to comply with the requirements of the principle of storage limitation.

Sinn Féin's Abú Database

Chapter Four of the overall report dealt exclusively with Sinn Féin's Abú database, it being the only political party in Ireland that maintains a database that encompasses electors/voters data from all constituencies. The audit of Sinn Féin considered in detail the matter of the legal basis for the Abú database and found it was not necessary to make recommendations in that regard. However, one of the main data protection concerns that arose related to transparency and a recommendation was made in particular with regard to drawing attention to the existence of the Abú database by means of canvassing and electioneering literature. The audit also found that certain data protection issues of concern that had emerged in the media earlier in the year were all remedied by the party before the commencement of the audit. These included the designation of a data protection officer, the carrying out of a data protection impact assessment in relation to the Abú database and the publication of a privacy notice on its website with regard to the Abú database.

Market Research/Opinion Polling

Only seven political parties were found to have conducted market research or opinion polling through the deployment of their own members, supporters or activists. The DPC was satisfied from the findings of the audits that no personal data was processed during those activities by the six of the political parties concerned and, on that basis, no data protection concerns arose for further consideration by the DPC.

In the case of the seventh party, Aontú, one recommendation was made by the DPC following its conduct of a survey in an overt manner which involved the processing of personal data of participants.

Social Media

No evidence was found during the audits that suggests that Sinn Féin has been using its social media presence, or its activities on social media platforms, to obtain or otherwise process personal data to enrich either the Abú database or its party membership database.

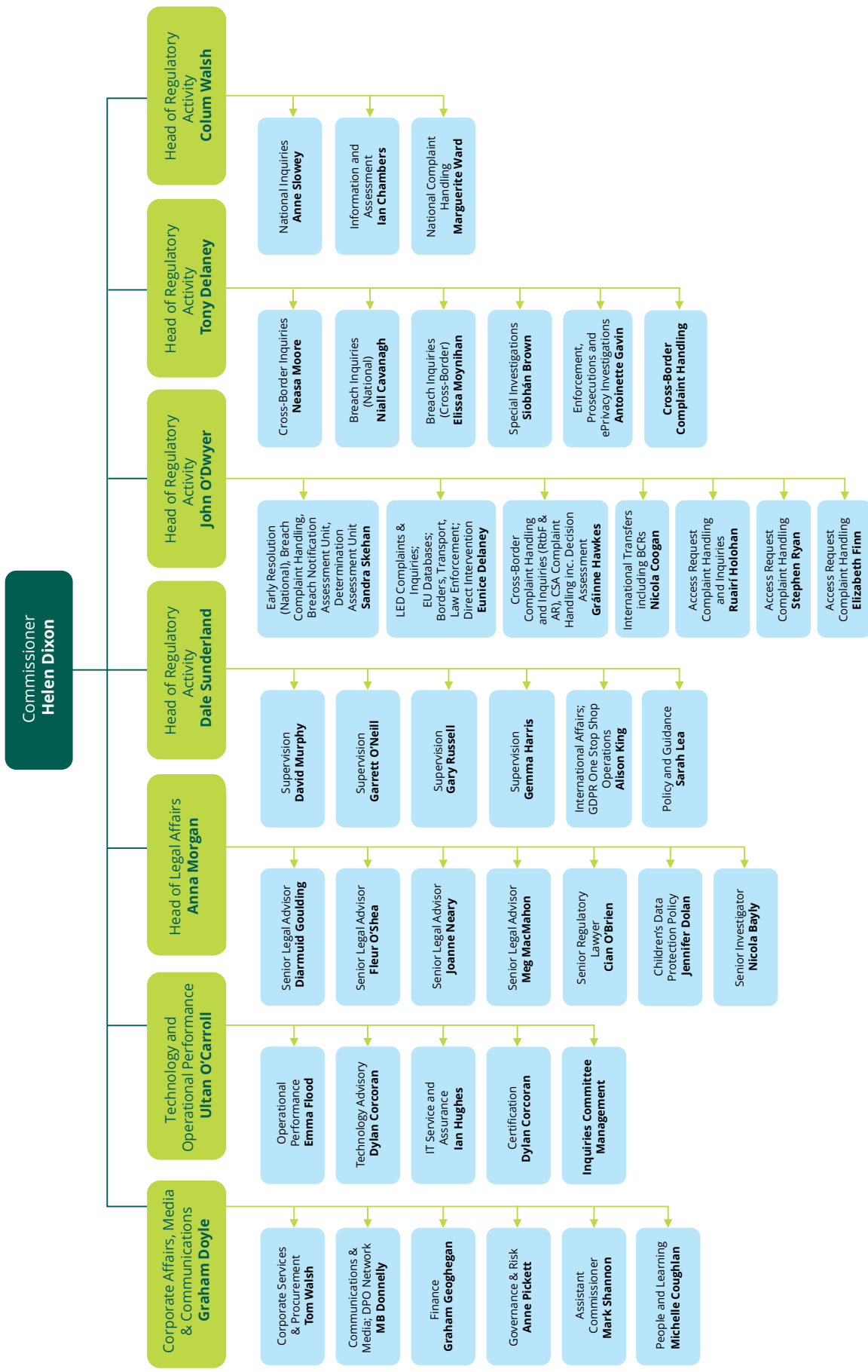
Conclusion

Over eighty recommendations were made by the DPC to political parties and some of those recommendations set down specific time limits for implementation. The DPC continues its oversight and supervision of the political parties concerned to ensure that the recommendations are fully implemented on time.

Appendix 5:

Financial Statement for the year 1 January 2021 to 31 December 2021 and the DPC's Statement of Internal Controls

The Financial Statement of the Data Protection Commission for the year 1 January 2021 to 31 December 2021 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 2021 by the Comptroller and Auditor General.



Data Protection Commission,
21 Fitzwilliam Square,
Dublin 2.

www.dataprotection.ie
Email: info@dataprotection.ie



**An Coimisiún um
Chosaint Sonraí**
Data Protection
Commission