DPC IRELAND 2018 - 2020

REGULATORY ACTIVITY UNDER GDPR

June 2020
Data Protection Commission
21 Fitzwilliam Square, Dublin 2

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Contents

Index of Case Studies

Introduction

Context

May 25, 2020 marked the end of two full years since the General Data Protection Regulation came into application across Europe. Since finalising the provisions of the Regulation in 2016 - and the subsequent readiness period leading to its implementation in May 2018 - data protection as a concept has grown exponentially; both in prominence and public awareness. Data protection is now a firmly fixed point of public consciousness.

Underpinning this increased awareness has been a range of important legal developments at an EU level, including judgments from the CJEU and the Advocate General's opinion on Standard Contractual Clauses and data transfers[1]. The attendant interest in these developments ensured that data protection has been the focus of growing media attention over the last two years, as a corollary of which the activities and outputs of the Data Protection Commission (DPC) have also been highly scrutinised.

Given its role as Lead Supervisory Authority to the various multinational organisations that are headquartered here, much attention is naturally given to Ireland's regulatory activities in the realm of 'big tech'. Since May 2018, the Data Protection Commission has commenced 24 Statutory Inquiries into multinational technology companies, in addition to Supervisory engagement which resulted in the postponement or revision of six planned big tech projects until such time as they could be reconciled with data protection requirements.

Separate to the foregrounding of its international remit, the Data Protection Commission also has responsibility for a significant body of work which takes place away from high-profile headlines. As data protection in general - and the GDPR in particular – have moved into mainstream public consciousness, the DPC has seen its caseload increase in all areas of the organisation. The diversity of concerns these cases present requires an equally considered approach to regulation. Though the same themes frequently reoccur – access issues, for example, being a consistent area of contention – there are nuances within each case that impact greatly on timescales and the resolution process. By reviewing and refining its approach to case handling over the last two years, the DPC has decreased wait times for individuals by over 54%.

The same is true of breach notifications, which the DPC also receives in consistently high numbers month-on-month. In the two years since the GDPR came into effect, the DPC has received almost 12,500 breach notifications, of which 93% were found to be in scope of the GDPR. The DPC has

[1] Summaries of both the Judgments and the Advocate General's opinion can be found in Appendices I and II of the DPC's **2019 Annual Report**.

processed and closed out almost 95% of these breach notifications. Despite the high volumes, the cases that have been assessed give no indication that organisations are over reporting. Rather, they suggest that many of the breaches that the DPC examines could have been prevented by more stringent technical and organisational measures at source, which is a learning that the DPC will look to reinforce going forward.

Arising from these learnings, the DPC has already instituted supports for both DPOs and SMEs, in order to drive improved data protection practices among its regulated entities. The DPC's Data Protection Officer Network was convened in 2019 in response to calls from that cohort for increased resources. Since the advent of the Coronavirus crisis, the DPC has transitioned to online supports in place of its planned conference. Also in 2019, an EU Commission stock-taking exercise identified the SME sector as one in need of focused supports. Subsequent to this, in late 2019, the DPC partnered with the Croatian Data Protection Authority and Vrije University on an EU-funded project to redress this gap. This project will run until 2022.

The DPC's remit is not limited to regulation of the GDPR. It encompasses all data protection legislation currently in force in Ireland, which includes a significant but declining volume of legacy work falling under the 1988 and 2003 Data Protection Acts. Since May 2018, the DPC has issued 59 Section 10 Decisions, of which 33 upheld the original complaint, 10 partially upheld the complaint and 16 rejected the complaint. The rate of old "act cases" that come before the DPC is diminishing, relative to the rates that were seen in May 2018, and the expectation is that this natural decline will continue in accordance with the passage of time. As the DPC moves forward, this will be taken into account in respect of the allocation of resources and internal processes.

In recognition of the volume of work the DPC currently processes, the two-year lens with which to analyse it and the expectation that overall volumes will only increase going forward, the DPC considers it timely to carry out an assessment of its activities to date under the GDPR. The second anniversary of the Regulation provides a valuable opportunity to take stock of the early years of its implementation and consider how this might influence the DPC's regulatory approach going forward.

Scope

This report is intended to assess the range of regulatory tasks of the Data Protection Commission for the period 25 May 2018 to 25 May 2020. It is distinguishable from the Commission's Annual Reports in that it does not focus on the administration of the office. Details of the DPC's administrative work are available in its annual reports, which can be found **here**; including its Financial Statements, Statements of Internal Control and Energy Usage.

This report takes stock of the DPC's experience of its mandated functions under the GDPR; its legal activities and the allocation of its resources in support of **Article 57.1 (b)(d).** To note, while the report refers in shorthand to "the GDPR", it is in fact intended to cover the substantive roles of the DPC under the three main pieces of data protection legislation – the GDPR, the e-Privacy Directive and the Law Enforcement Directive as transposed in the Data Protection Act 2018.

Purpose

The purpose of this two-year assessment is to provide a wider-angled lens through which to assess the work of the DPC since the implementation of the General Data Protection Regulation; in particular, to examine wider datasets and annual trends to see what patterns can be identified. While the DPC - as is the case for many other stakeholders - could already make some observations about aspects of the GDPR and the one-stop-shop procedures that work less well, the purpose of this document is not to offer a critique at this juncture but rather to showcase what has - and is - being delivered. The report and its findings will form part of the information upon which the DPC will base its regulatory approach for the next five years.

The report is additionally intended to give public insight into the work of the DPC and, through the inclusion of case studies, provide instructive examples which will give guidance to entities in similar situations.

Executive Summary

Supporting Individuals

From 25 May 2018 to 25 May 2020, the DPC:

- received in excess of 40,000 emails, 36,000 phone calls and 8,000 postal contacts;
- opened **15,025 cases** in support of individuals' rights;
- concluded 80% of cases opened (so far); and
- reduced conclusion times for cases (average days taken to conclude a case or query down by 53% over two years).

Since 25 May 2018, the **most frequent GDPR topics** for queries and complaints have consistently been: Access Requests; Fair processing; Disclosure; Right to be Forgotten (delisting and/or removal requests); Direct marketing and Data Security.

Figures indicate that the DPC is dealing with high volumes of cases that are potentially resolvable at a data controller/ Data Protection Officer level.

Supporting Industry

- Total **breach notifications** received between 25 May 2018 and 25 May 2020: 12,437.
- 93% classified as relating to GDPR (11,567 notifications).
- Of the 12,437 total recorded breach cases, 94.88% concluded (11,800 cases).

The most frequent cause of breaches reported to the DPC is unauthorised disclosure (80%).

Human error are at the root of far more reported breaches than phishing, hacking or lost devices (5.6% collectively).

Figures indicate that the DPC is dealing with breaches that could be mitigated by more robust technical and organisational measures.

The DPC launched a new website in December 2018 and webforms to make stakeholder access easier.

In the last two years, the DPC has published 40 guidance documents, 29 blogs and 10 podcasts to support stakeholder compliance.

In 2019, The DPC established a **Data Protection Officer Network** to facilitate knowledge sharing and peer-to-peer support.

In response to the Coronavirus crisis, the DPC has instead taken its supports online, including a dedicated section for DPOs on its website.

In 2019 the DPC partnered with the Croatian Data Protection Authority, AZOP, and Vrije University in Brussels on an **EU-Funded project** (The ARC Project) specifically targeting the needs of SMEs.

Regulating

Since May 2018, the DPC has opened 24 cross-border inquiries and 53 national **inquiries.**

In May 2020 the DPC issued its first **fines** under the GDPR, levying two separate fines against an Irish state agency.

Also in May 2020, the DPC issued a reprimand to the agency and ordered it to bring its processing into compliance.

In the same month, the DPC sent its first major-scale **Article 60 Draft Decision** to the EDPB.

The DPC has concluded **nine litigation cases** since GDPR came into effect.

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

Enforcing

- **An Garda Síochana** – reprimand and corrective powers applied in accordance with the Data Protection Act, 2018.
- **Tusla**; The Child and Family Agency – reprimand and fine applied in accordance with the Data Protection Act, 2018.
- **Tusla**; The Child and Family Agency – reprimand and fine applied in accordance with the Data Protection Act, 2018.
- **Twitter** – Inquiry completed and draft decision forwarded to EU concerned data protection authorities in accordance with Article 60 of the GDPR.
- **DEASP** - Enforcement notice issued regarding the use of the Public Services Card (currently under appeal). [2]
- 59 Section 10 decisions issued.
- **15,000** breach notifications assessed and concluded.
- 9 litigation cases concluded in the Irish Courts.

[2] DEASP is appealing the notice in the Circuit Court. Further details can be found in the DPC's **2019 Annual Report**.

- Hearing in CJEU Standard Contractual Clauses case brought by DPC to Irish High Court.
- **80%** of cases received under the GDPR have been concluded.

Engaging with Civil Society

In the past two years, the DPC has had 5 consultations open on:

- Targeting outcomes for regulatory planning (2);
- processing **children's data** (2); and
- the role of the data protection officer (1).

These open consultations have returned substantive insights from government departments, public bodies, social media platforms, technology companies, consultancies, trade associations and charities.

Through professionally facilitated focus groups and support from schools, the DPC has also taken steps to secure the input of individuals from across the country, as well as the views of approximately 1,200 children from demographically and geographically varied backgrounds.

Consultation reports (**Some Stuff You Just Want to Keep Private** and **Whose Rights Are They Anyway?**) have been made publically available.

Engaging with Peers

Since May 2018, the DPC has:

- received 746 complaints from peer DPAs in which the DPC has been identified as Lead Supervisory Authority.
- received 124 formal and voluntary mutual assistance requests (not complaint related).
- taken part in all meetings of the EDPB since 25 May 2018 and has representatives on all Subgroups.

Mainstreaming Data Protection

Staff of the DPC have presented at over 330 stakeholder events since May 25 2018.

Since the Coronavirus restrictions have been in effect, the DPC has continued to support stakeholder events through online participation.

The DPC has committed to driving awareness of data protection rights and responsibilities, including over **40 guidance notes** covering technological advice, GDPR compliance and direct marketing/electoral constraints.

Other Activity

Since May 2018:

- the DPC has opened **282 new direct marketing complaints** and concluded 247.
- the DPC has **successfully prosecuted 11 companies** for a combination of 42 offences under S.I. No. 336/2011.
- handled **66 Law Enforcement Directive complaints.**
- the DPC has successfully completed the EDPB consistency opinion process for both Code of Conduct monitoring bodies and for the additional requirements for INAB.
- established a **Data Protection Officer Network.**
- partnered with the Croatian Data Protection Authority and Vrije University on an **EU-Funded project** specifically targeting SMEs.

Cases, Queries and Complaints

Since the implementation of the GDPR on 25 May 2018, the DPC has seen an enormous increase in the number of communications it receives from individuals. In the two-year period from 25 May 2018 to 25 May 2020, the DPC received in excess of **40,000 emails, 36,000 phone calls and 8,000 postal contacts**.[3] For the most part, these communications fall into two categories[4]:

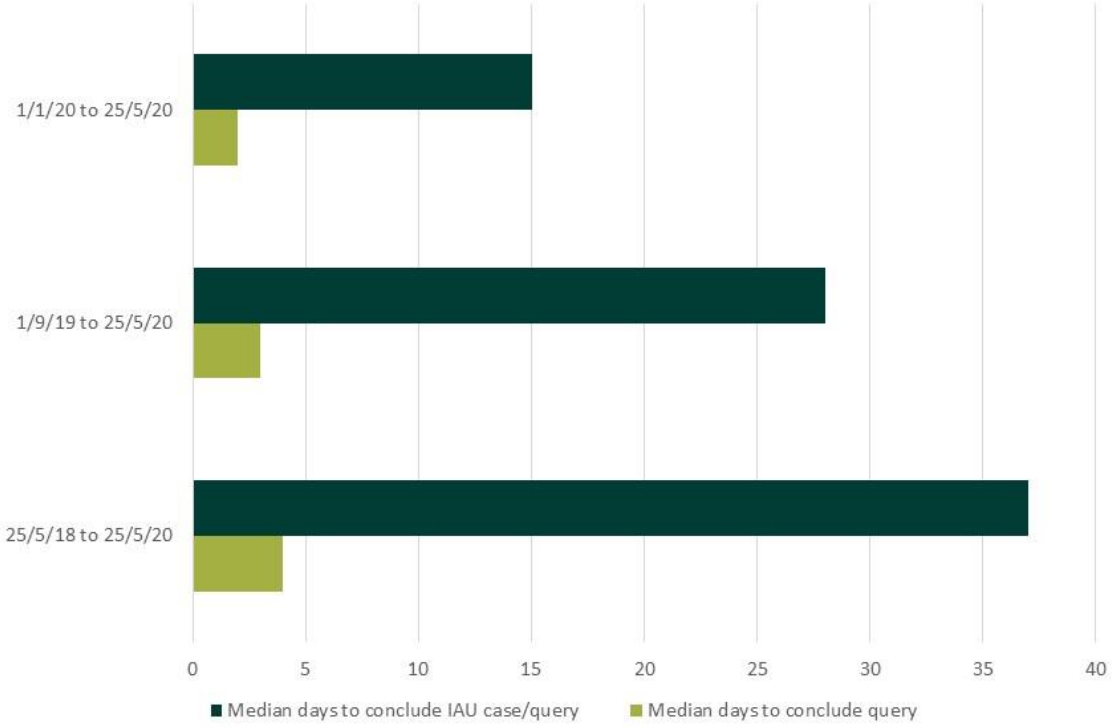
(i) requests for information/advice; and
(ii) further information in respect of ongoing cases.

In the period 25 May 2018 to 25 May 2020 the **total number of cases recorded as a result of these contacts was 15,025.**[5]

- % of which are concluded: **80%**
- % of which concluded as queries: **23.32%**
- % of all cases/queries closed due to information having been provisioned to the individual: **41.17%**
- Cases withdrawn by complainant: **6.60%**
- Amicably resolved: **7.96%**
- Not a DPC issue (issue outside of the regulatory remit of the DPC): **4.56% or 546 cases**
- DPC not the competent authority (issue appropriate to another DPA): **4.69% or 562 cases**
- Data Protection Issues: **22.62%** of all cases/queries logged concern Access Requests.

[3] The DPC facilitates a Monday-Friday Helpdesk phone line to assist stakeholders, in addition to services online and by post.
[4] Contact from the public includes a vast amount of spam contact. This is generally stopped at multiple stages throughout the digital network. However, the DPC filters through an average of 130 Spam items per day in addition to management of genuine queries, which must all be assessed before being discounted.
[5] Cases are defined as contacts that require further engagement beyond the initial query. Cases in this instance can therefore include complaints from individuals, but also encompasses requests for advice and guidance which do not have a complaint element. The figure does not include contacts from the media, speaking invitations, breach notifications or prior consultation.

Response Times



Responding to these contacts - and resolving or progressing them as appropriate - is a fundamental objective of the DPC and the high volume of communications received in the last two years has meant that the DPC has had to revise the way in which it counts its incoming contacts to accurately record to trends that emerge.[6]

- At the outset of the GDPR general queries were not recorded within a DPC database, only complaints. However, these metrics took no account of the high volume of general queries into the office, the trending issues amongst the public nor the corresponding staff time that such queries involve.
- Similarly, from 25 May 2018 to 31 December 2018, a query submitted to the DPC by an individual was counted as a single issue (e.g. Access Request) for the purposes of statistics, regardless of complexity or potential multi-faceted nature. This method of counting proved insufficient when determining the wide range of concerns and issues that a given

[6] Additional activity not recorded includes queries from 2018. 'One-touch' queries were not recorded prior to September 2019.

individual could present with, and so complex queries have been recorded as such since the start of 2019.[7]

- Since September 2019 all queries, regardless of complexity, are now recorded within the DPC database.

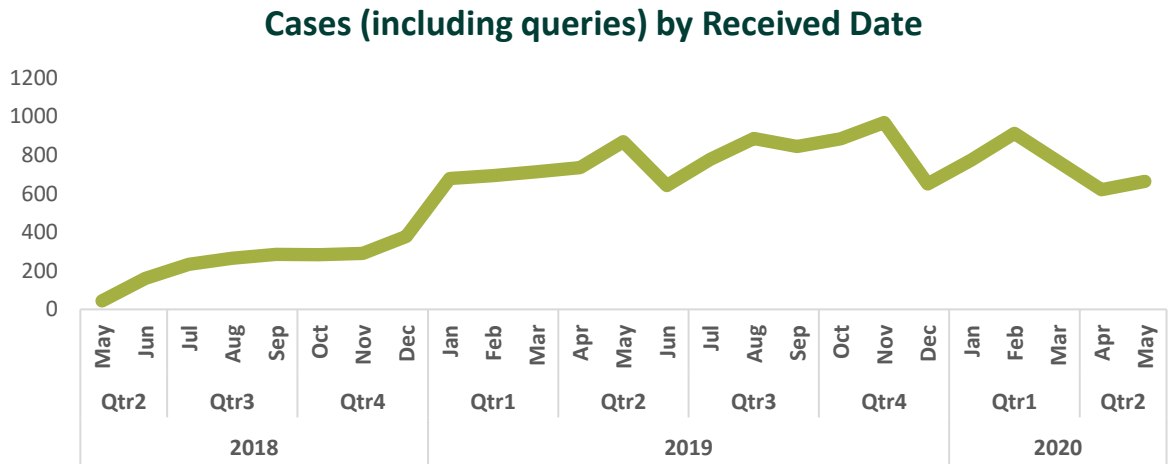
The response times for cases are not equal for all periods within the 24-month window of GDPR due to DPC organisational restructuring, staff allocation and evolving processes, but the impact of ongoing efficiency improvements are reflected in the table below showing the **downward trend of conclusion times for cases** (average days taken to conclude a case or query down 53% over the first 24 months of GDPR):

Statistic	25/5/2018 to 25/5/2020	1/9/2019 to 25/5/2020	1/1/2020 to 25/5/2020
Average days to conclude DPC case/query	49	35	26
Median days to conclude DPC case/query	37	28	15
Average days to conclude query	17.6	13.6	10.3
Median days to conclude query	4	3	2

The days to conclude listed above are calendar days and do not take in to account weekends or public/bank holidays.

It should be noted that the time required to close out an issue will vary greatly per case. Often a complaint will infer complexity, but complexity may be equally present within a query. The time to close a case will also be dependent on the timely supply of information from the individual. If an individual is non-responsive to a request for more information, a case will be closed after 30 days. However, *any case may be re-opened at any time* on receipt of further contact from the relevant parties. This goes some way to explain the outliers that skew the averages listed above. The median has been chosen for visualisation in the graph below, as it is more representative than the average.

[7] There has been an increase in multi-faceted cases where multiple aspects of GDPR legislation have validity within a single data subject complaint. New procedural means of capturing these were added in recent months, but already 61 live cases have been classified as such. Historical cases have not be reclassified as multifaceted.



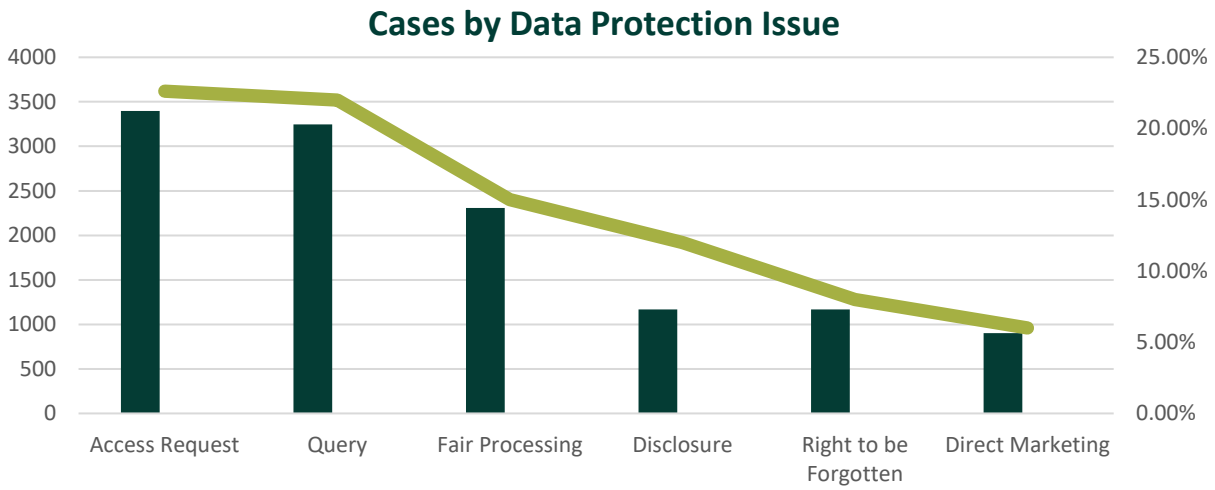
Most Frequently Queried GDPR Topics

Since 25 May 2018, the most frequently raised GDPR topics for queries and complaints have consistently been:

- Queries relating specifically to Access Requests;
- General queries (unclassified)[8];
- Fair processing (including fair obtaining and further processing);
- Disclosure (data shared with a third party);
- Right to be Forgotten (delisting and/or removal requests);
- Direct marketing; and
- Data Security.

There are 40 possible data protection categorisations under which cases can be recorded in the DPC. These categories have been added to, refined or reworded over the course of the two years of activity (e.g. an entry of 'multifaceted' was the most recent addition). These categorisations are scheduled to be reviewed again in the near future, to ensure that the DPC accurately captures the distinct aspects of individual concerns.

[8] The classification gap arises here due to older complaint logging modes. This will close out as the DPC's new case management system comes on stream.



DP Issue	Count	%
Access Request	3,398	22.62%
Query	3,245	22%
Fair Processing	2,309	15%
Disclosure	1,778	12%
Right to be Forgotten	1,168	8%
Direct Marketing	902	6%

Amicable Resolution

Of all of the cases that were active with the DPC on 25 May 2020, approximately 8% were being worked-out through Amicable Resolution.

Where feasible and appropriate, the DPC will always encourage resolution of cases through amicable means, as this can deliver a fair and efficacious solution for the affected individual in a timely manner. The option to have their issue dealt with by amicable means is afforded to individuals throughout the lifetime of their complaint with the DPC, regardless of how far the issue may have progressed through escalated channels.

Case Studies

Examples where issues have been resolved amicably through Early Resolution

Amicable resolution

Inadvertent disclosure of circumstances to third parties

The DPC received a complaint from an individual regarding the disclosure of his personal data by a hospital to a private debt collection agency. This occurred when the hospital informed the debt collection agency that they were cancelling the individual's debt, as he was a medical cardholder.

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

The data controller engaged with the DPC on the matter and accepted that it was not appropriate to share personal information in relation to health insurance status with a debt collection agency. It further advised that it had directed the Hospital Accounts Department to cease providing this information with immediate effect. The data controller advised that it had changed its process and ceased this practice. The data controller also made further changes, particularly in relation to transparency obligations, by informing patients that their personal details would be sent to third party providers in certain circumstances.

Through this interaction with the DPC, the hospital's practice of sharing extraneous information with debt collectors ceased.

Amicable resolution

Fair obtaining and retention

The DPC received a complaint from an individual who, when checking into a hotel with her guide dog, was asked for a copy of her guide dog identification. The individual presented her guide dog identification, which contains the owners name and photograph, as proof that her dog was indeed a service animal. The hotel proceeded to take a copy of this identification. The individual subsequently raised this with the hotel, who stated that they were merely trying to ascertain that the dog was a guide dog, as it was important that they ensure the safety of all their guests and they were aware that some guests may be afraid of dogs. The complainant was not satisfied that this response adequately explained why the hotel needed to take and retain a copy of the guide dog identification, which also contained her personal data.

This complaint was identified as potentially 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 hotel engaged with the DPC on the matter and agreed that they would change the practice of taking a copy of the guide dog identification, but would instead ask to view it and then note on the guest file that they had verified that the dog was a guide dog.

In accordance with Article 5(1)(c) of the GDPR (data minimisation), data controllers must identify the minimum amount of personal data required to fulfil the purposes of processing and should only request that information, but no more.

Observations and Emerging Patterns

As previously noted, general queries to the DPC were not initially recorded within DPC databases. Those queries that require more than 'one touch' engagement by the DPC have been recorded since early 2019. Over time, we can see that **a large proportion of contact from the public does not proceed to complaint stage**.

Early resolution of queries to the DPC often involves directing the individual to the appropriate information on either the DPC website or that of another regulatory body.

In a large number of these cases where relevant information is given to an individual or a data controller (41.17%) they pursue no further action through the DPC. In these instances, the information that has been provided proves sufficient to resolve the matter for the relevant party. However, the volume of correspondence to the DPC, charted against the most frequently queried topics, indicates that **the DPC still deals with a high volume of cases that may be resolvable at a data controller/ Data Protection Officer level going forward**.

Similarly, for the two-year period from 25 May 2018 to 25 May 2020, just under 10% (9.25%) of the cases the DPC received were deemed to be outside of its regulatory remit, either because the DPC was not the competent authority or because the matter did not relate to data protection.

This figure, combined with the 41.17% of cases that were resolved by the provision of information, supports the view that there are broadly high-levels of GDPR awareness amongst the DPC's stakeholder base, but as yet there is not the corresponding understanding of what can be managed at personal, data controller and DPO levels.[9]

[9] **Latest figures** from the EU Fundamental Rights Agency put the rate of DPA-awareness in Ireland at 84%, well above the EU average of 71%.

Complaint Handling and the Right of Access

Where a case cannot be amicably resolved, it is escalated as a complaint within the DPC. Complaints, by their very nature, imply a degree of complexity. Analogous to these complexities is the consequential fact that resolution times are non-linear, and vary from complaint to complaint.

The right of access to personal data is one of the fundamental pillars of the GDPR. While expansive in its reach, the right is not absolute and may be subject to certain restrictions, as provided for in **Article 23** of the GDPR and transposed into Irish Law by **Section 60** of the Data Protection Act, 2018. Any restrictions must respect the essence of the fundamental rights and freedoms.

In any examination undertaken by the DPC, much of the work focuses on examining the validity of the exemptions advanced by data controllers. In addition to addressing the complaint on behalf of the individual, this serves to provide data controllers with valuable information as to the criteria used by the DPC in accepting or rejecting cited exemptions. The DPC expects that increasing the knowledge of both data controllers and Data Protection Officers in this way will correspondingly increase efficiencies in future responses to access requests, ensuring that fewer and fewer such requests escalate to complaint status.

To assist data controllers in gaining an understanding of the criteria applicable when applying exemptions the DPC has published **guidance** on the application of exemptions.

Delisting and the Right to be Forgotten

The DPC also handles a number of Right to Be Forgotten – or 'delisting' - cases with respect to Google LLC. These delisting cases arise from complaints made by individuals, resident in Ireland, who have an objection or concern regarding the information that is returned when a search for their name is conducted on the Google LLC platform. Generally, the requests for delisting relate to personal circumstances of the individual, the details of which they do not want to be publicly available through search engines.

Given the often sensitive nature of these cases, delisting requests give rise to complex issues The DPC must ensure that balance is maintained with respect to the individual's rights and the public interest.

As a consequence of the rising number of delisting complaints the DPC was receiving, and conscious of the complexity involved in making such requests in the first instance, the DPC requested to review Google's Right to be Forgotten (RTBF) process. It was determined that, in order to ensure greater transparency for individuals making a delisting request on the platform, more information should be made available to affected users at the commencement of the process.

The DPC engaged with Google on this matter, as a result of which Google implemented changes to increase user transparency, including a link to the FAQs in its delisting communications. This FAQ clarifies, at the outset of the process, the reasons and instances in which Google will refuse a delisting request. This change was implemented at global level by Google, and it is envisaged this greater level of transparency will assist individuals in understanding the extent and applicability of the Right to be Forgotten and potentially reduce the number of complaints arising from this provision.

Trends Emerging

Of the complaints that have progressed though the DPC in the last two years, some common patterns are discernible. Typically, data subjects make access requests to organisations with whom they are already in dispute; the right of access is frequently invoked as an assist to independent issues of customer service, labour relations and custodial issues, among others.

Similarly, where a topic is the subject of widespread media reporting, the DPC will often see a spike in complaints that have likely been prompted by the coverage. An example of this is the recently contentious Cervical Screening Programme, which resulted in complaints to the DPC regarding outstanding personal data. The data controller cooperated with the DPC and further personal data was released.

Case Studies

Access request to retailer for CCTV

In August 2019, the DPC received a complaint from an individual in relation to an access request he had made to a mobile phone retail outlet, in which he sought a copy of his personal data which included CCTV footage.

The individual provided the DPC with correspondence from the company informing him that they would not be in a position to provide a copy of the CCTV footage as it contained images of other customers, including a child.

The complaint was handled under Section 109 of the Data Protection Act 2018.

The DPC began corresponding with the company in September 2019 and was dissatisfied with the responses received. The DPC provided further guidance on the use of CCTV and the threshold for exemptions to the right of access. The company subsequently provided the individual with the relevant footage, having first removed the images of all other customers in the store.

Access Request for personal correspondence with a state agency

In August 2018, the DPC received a complaint from an individual regarding an access request that he had submitted to an Irish state agency in June 2018, in which he sought a copy of all personal data held by the agency pertaining to him. At the time of contacting the DPC, the individual had received a response to his access request, wherein the majority of his information had been released to him with the exception of two particular letters, which in his view constituted his personal data.

The individual had previously been advised by the agency that they were in receipt of two letters, purportedly from him, containing allegations that a named third party was in unlawful receipt of benefits while also working. The complainant was adamant that he had not written the letters and was seeking access to same.

The DPC commenced its examination of the matter, contacting the agency and seeking copies of the two letters in their original format. The letters contained the name and address of the individual, which is considered personal data.

The agency considered that, as the complainant was denying authorship of the letters, he could not correspondingly claim them as his personal data.

The DPC directed the agency to release the letters. However, importantly, the DPC also found that the agency was entitled to withhold the details of the person about whom the allegation of fraud had been made.

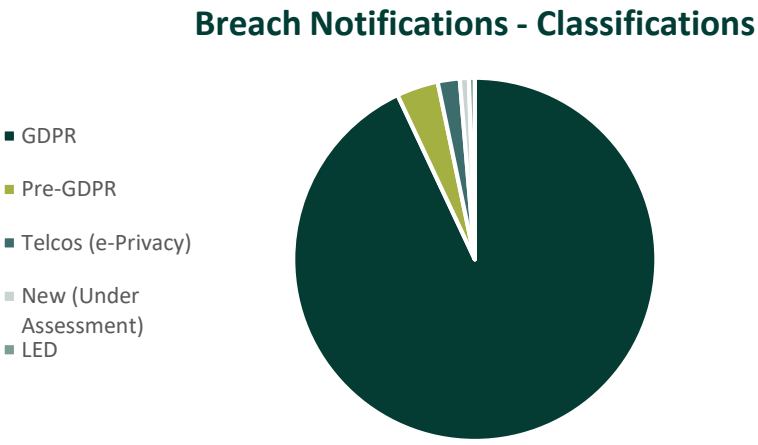
In response to this direction, the agency provided the individual with the two letters, in which third party/non-personal data had been redacted. To ensure that the redactions had been validly applied, the DPC subsequently sought copies of the letters from the complainant, confirming with them that the redactions were in order.

In view of the fact that the rationale for an access request is to enable an individual to determine what data is processed about them and seek the rectification where necessary, it was reasonable in the circumstances of this case for the individual to have sight of the personal data contained in the letters allegedly written by him.

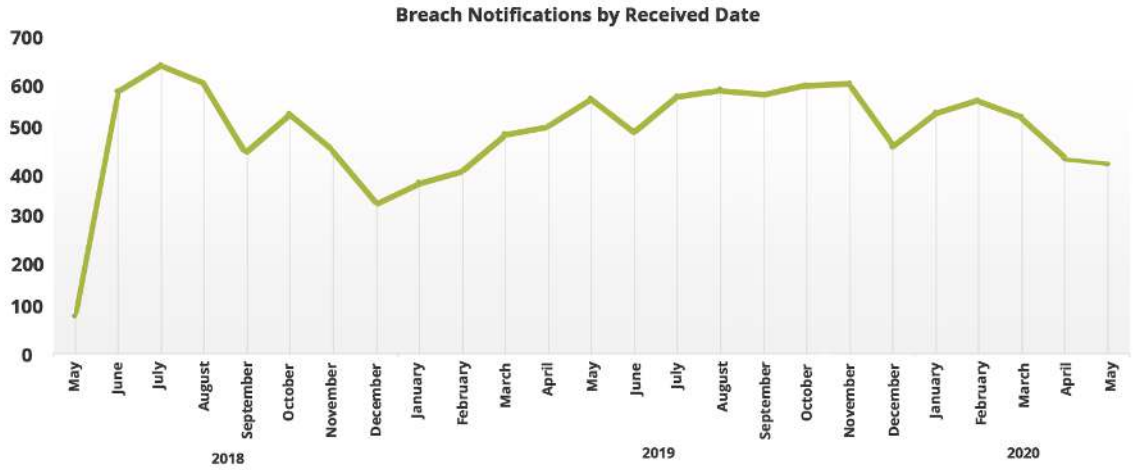
Breaches

Any organisation or body which makes use of personal data as part of its business – regardless of whether the data pertains to customers or staff – is deemed to be a data controller and ultimately accountable for the safeguarding of the personal information in its possession. **Article 33** of the GDPR introduced several obligatory actions for data controllers, including mandatory notification of breaches to the appropriate data protection authority within 72 hours. In the two years since the introduction of this provision, the DPC has seen an exponential increase in the breaches being notified to it.

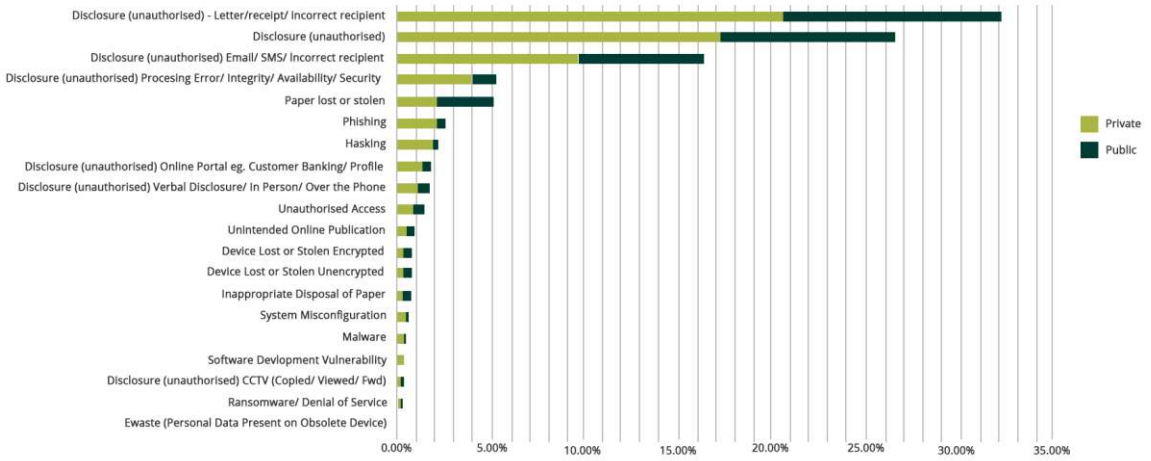
- Total breach notifications received between 25 May 2018 and 25 May 2020: **12,437**
- 93% have been classified as relating to GDPR (11,567 notifications).
- Of the 12,437 total recorded breach cases, **94.88% have been concluded (11,800 cases)** and 5.12% are currently active (637 cases).



The table below shows both the frequency and consistency of breach notifications to the Data Protection Commission. With the exception of a seasonal decline in December 2018, the number of breaches being reported to the DPC remained broadly consistent over the first 18 months of GDPR implementation. Q2 of 2020 shows an overall trend towards reduced breach notifications. It is not possible to attribute this decline to a particular cause, though it is likely that the number of breach notifications has been impacted by the Coronavirus crisis.



Breach Notifications – Breach Type by Sector



As the table above shows, by far the most frequent cause of breaches reported to the DPC is **unauthorised disclosure (80%)**; whether by digital, verbal or other manual means. Manual processing - and consequently an inferred lack of robust processing procedures - is at the root of far more reported breaches than phishing, hacking or lost devices **(5.6% collectively).**

As with the trends observed earlier in the queries and complaints that the DPC receives, the patterns within the recorded breach notifications indicate that there is also a significant volume of work that falls to the DPC, which could be mitigated by more robust technical and organisational measures being introduced by the data controller and the processes for testing, assessing and evaluating these measures being overseen by the data protection officer going forward.

At present, the DPC workload in the breach area is heavily influenced by the need to engage with organisations to address elementary processing liabilities, which are occurring at a very basic level. As we move forward in time, the DPC expects to see changed behaviours amongst its regulated entities, resulting in a reduction in the volume of breach notifications that can be attributed to a lack of due care and attention.

Case Studies

Insufficient organisational and technical measures in place to secure data

An organisation responsible for providing care to both children and adults with a range of support requirements notified the DPC of a breach in which it outlined that a wheelie bin containing the personal data of residents and staff of the facility had been removed from their premises and discarded on a neighbouring property.

The individual who discovered the contents of the wheelie bin fly tipped on their property contacted the organisation after first inspecting the records to establish their origin. Following contact from the individual, the organisation arranged to retrieve the records and disposed of them in an appropriate manner.

Based on the information provided by the organisation, the DPC raised a number of queries focusing on whether the organisation had policies and procedures for confidential disposal, and whether they were in place at the time of the incident. The organisation advised that it did not have a specific confidential disposal policy in place; however, it did advise that the premises had shredding facilities in place to assist with the confidential disposal of records. On this occasion, these facilities were not utilised.

The DPC highlighted that - as a data controller - it was the organisation's responsibility to ensure that both appropriate organisational and technical measures are employed to ensure that the processing of personal data is done in a secure manner. The DPC also highlighted that the processing of personal data also encompasses both its erasure and/or destruction.

The DPC recommended that the data controller undertake the following actions:

- Complete a GDPR self-assessment to identify areas where immediate remedial actions are required in order to ensure compliance with GDPR.
- Review their obligations as a data controller, in particular their obligation centring on the security of data.
- Undertake an exercise to produce adequate policies and procedures in relation to the appropriate disposal of personal/sensitive records both in hard and soft copy.

Based on the recommendations of the DPC the data controller has initiated a data protection compliance project to address the areas highlighted. The data controller committed to providing the DPC with updates in relation to the progress of this project and provide the necessary evidence of actions undertaken based on the recommendations provided. This is being monitored on an ongoing basis.

Ransomware attack on Leisure Company

A company, whose primary business is in the sports and leisure sector, notified the DPC of a breach in which they outlined that they had been the victim of a ransomware attack. Personal data, which they held in encrypted form, was consequently compromised.

Based on the breach notification, the DPC raised a number of queries with the company, requesting further information on:

- The chronology of events leading up to the incident;
- The description of the organisations IT system/environment and the software employed;
- The identified source of the incident and attack vector;
- The ransomware variant used to encrypt the data;
- Whether all relevant audit logs have been retained;
- The contents of any demand notice received;
- Whether backups of the encrypted data have been retained and could successfully be restored; and
- The organisational and technical measures which were employed at the time of the incident to mitigate against incidents of this nature occurring.

The data controller provided responses to all technical queries raised, based on which the DPC recommended that the data controller undertake the following actions:

- That an analysis of their ICT infrastructure be undertaken to ensure there was no further presence of unwanted programmes and to provide the DPC with evidence of the steps taken.
- That appropriate technical and organisational measures be implemented to ensure the ongoing confidentiality, integrity, availability and resilience of its processing systems, to include appropriate logging of all data processing, log file retention and log file analysis on a systematic basis.
- That it has adequate system monitoring in place to allow access to personal data in a timely manner in the event of a physical or technical incident and to provide a copy of the system monitoring policy to the DPC.
- That reasonable steps be put in place to ensure that both it and its processors fulfil their obligations set out in Article 24 and Article 28 of the GDPR. Appropriate guidance was provided by the DPC.
- Ensure that appropriate and regular refresher training is provided to staff to inform, educate and update them on security measures applied and the associated security risks, such as social engineering attacks: crypto ransomware, phishing etc., as they continue to evolve.
- That employees of the company have the minimum appropriate IT system permissions necessary to perform their duties. Appropriate guidance was provided by the DPC.
- That a review of DPC Guidance of Data Security for Microenterprises be undertaken.

Based on the recommendations of the DPC the data controller undertook a program to address the specific technical areas highlighted by the DPC. From the evidence provided the DPC was satisfied that the appropriate organisation and technical measures have been implemented to reduce the risk of incidents of this nature reoccurring.

Data processor accounts compromised

In October 2019, the DPC was notified by an Irish public sector body of a personal data breach, which had occurred as a result of a compromised email account which was being used by a data processor. This exposed the public sector body to the liability that personal data - including data subjects' names, addresses, dates of birth, details of family relationships and biometric data – could be accessed by a malicious third-party while being sent to, or held in, the compromised account. The data processor was located outside the European Union and was using a locally hosted email provider.

The DPC engaged with the public body in order to determine what measures it had in place at the time of the breach to ensure that the processor took all precautions required, pursuant to **Article 32** of the GDPR (security of processing). The DPC also sought to determine whether the arrangement between the public sector body and the processor was such as to require the processor to assist it in ensuring compliance with data security and personal data breach notification obligations, and to make available to the controller all information necessary to demonstrate compliance with data security obligations, as required by **Article 28** of the GDPR.

Following extensive engagement between the DPC and the public sector body in question, the DPC issued specific recommendations to the entity, including recommendations for technical measures to be implemented by third-party processors engaged by the public sector body.

In response to these recommendations, the public sector body informed the DPC that it is providing secure email addresses to relevant processors to replace locally hosted email accounts and is revising its conditions for the engagement of data processors, including specific requirements on data security and training. They have also provided the DPC with regular updates on the implementation of the DPC's recommendations, including providing copies of relevant documentation. The DPC continues to engage on a regular basis with the relevant public sector body in order to monitor its implementation of these recommendations.

Unsecured data storage highlighted through media reports

In November 2019, the DPC was made aware - via media reports - of a potential personal data breach occurring in an Irish university. The potential breach had arisen as a consequence of the manner in which the university was storing large volumes of personal data - including payroll data, bank account details and PPS numbers - in a location which was accessible to a potential large

number of persons. The DPC contacted the university directly in order to advise it of their data controller's obligations, pursuant to Article 33 of the GDPR, to notify personal data breaches to the DPC.

Following this initial contact, the university notified the breach to the DPC. The DPC engaged with the university in order to determine who may have had access to the stored personal data, the level (if any) of supervision of persons having access to the data, the nature and sensitivity of the exposed data and any actions taken by the data controller in response to the personal data breach. Based on the information provided, the DPC issued specific recommendations to the controller, in order to ensure that personal data is processed appropriately going forward. In particular, the DPC advised the data controller:

- To review the level of physical security applied in respect of personal data storage facilities;
- To ensure that adequate access controls are put in place with access to personal data being limited to a "need to know" basis and having regard to the nature and sensitivity of any personal data stored;
- To review its data retention policies to ensure that unnecessary data is not collected or retained and that the controller can record and track any personal data which is archived; and
- To provide regular and up-to-date training for staff on the requirements of data security.

In response to the DPC's recommendations, the data controller has now introduced mandatory data protection and data security training for all employees throughout the organisation, is undertaking a physical audit of all data storage locations and has reviewed its data retention schedule and provided guidance on data retention periods. The DPC continues to engage with the data controller on a periodic basis, in order to monitor its ongoing implementation of these recommendations.

Vulnerabilities in email application result in data breach

The DPC was notified of a breach by a medical testing company, which affected 750 patients whose medical diagnostic information was accessed via an email account which was itself the subject of an unauthorised disclosure, arising from a vulnerability in the cloud-based email application being used by the organisation.

The DPC assessed the information provided in the breach notification form and requested further information of a technical and organisational aspect. In response to which the organisation advised that, following a review of the Sign-In Logs, the breach was deemed to have occurred due to a brute force attack. The organisation was able to identify a number of failed initial access-attempts from the same IP address, followed by a successful access attempt, again from the same IP address.

The company acknowledged that it was working through recommendations it had received from the Irish Hospital Consultants Association (IHCA) of which it was a member and advised of the

processes already put in place to mitigate any risks. The company also welcomed engagement with the DPC.

Following an examination of the facts around the case and taking into consideration the steps the data controller had already taken, the DPC issued eight recommendations including:

- To conduct a Data Protection Impact Assessment (DPIA), where a high risk exists, to assess the impact of its processing operations on the protection of personal data;
- To ensure that access control and authentication contain appropriate measures for ongoing confidentiality and integrity of user account information including minimum appropriate permissions, strong password policies, ICT Infrastructure restricted to authorised users (especially where ICT infrastructure is accessed remotely) and removal of accounts no longer required;
- To review the security 'best practices' provided by the vendor for any ICT infrastructure and associated systems it avails of, ensuring compliance with Article 28 of the GDPR; and
- To consider the use of an expert third party (either on its own behalf, or on behalf of the data processor) to assist it periodically and independently in evaluating the effectiveness and appropriateness of the organisational and technical measures applied to public facing ICT infrastructure.

The DPC sought monthly updates and continued to engage with the data controller on its progress of implementing the recommendations. Within two months of issuing recommendations, the organisation provided the PDC with an update advising that it had implemented all the recommended actions. It also provided details regarding the measures now in place to improve its overall security and the safeguarding of the personal data it processes.

Third-party service provider breach indicates insufficient controller oversight

In 2019 an Irish hotel, part of a wider hotel franchise, notified the DPC of a breach which it had incurred as a result of a cyber-security breach relating to a third party service provider based outside of Ireland. The hotel utilises this third party software and service provider to monitor and manage the allocation and rates of its rooms across various sales channels, including booking.com and Expedia. The data processor had notified the hotel of the breach and published a number of security incident announcements.

The DPC assessed the information provided in the notification form and requested further information of a technical and organisational nature. In response to which, the hotel stated that the breach was ongoing for a period of fifteen months and had resulted in the unauthorised access and exfiltration of guests' credit card details. The DPC raised further questions with the hotel, which resulted in the third party service provider commissioning a forensic report. After a number of engagements and a direct request to the third party service provider, the DPC received a copy of the forensic report. Upon examination of the forensic report, the DPC issued five technical and organisational recommendations to the hotel, including:

- That it only utilise processors who provide sufficient guarantees that they will implement appropriate technical and organisational measures to ensure the protection of data subject rights, pursuant to **Article 28(1).**
- That it put steps in place to ensure that both the hotel and its processors fulfil their obligation as set out in **Article 24** and Article 28 of the GDPR.

The DPC further engaged with the hotel and reviewed the progress of its implementation of all the recommendations issued by the DPC. The hotel introduced new procedures for on-boarding processors, including securing guaranteed data processing standards before engaging processors and regularly auditing existing processors to ensure ongoing compliance with security of processing. The hotel also undertook an audit of its existing processors and provided the DPC with the results. Following a review of the documents provided - and confirmation from the hotel that it had implemented the remaining recommendations - the DPC concluded its examination of the case.

Inquiries

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 Data Protection Act has occurred:

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

A more detailed, narrative update on the ongoing inquiries is available in the DPC's **2019 Annual Report**.

Multinational Technology Company Statutory Inquiries Commenced since May 2018

	Company	Inquiry type	Issue being examined	Status
1	Apple Distribution International	Complaint-based inquiry	Lawful basis for processing. Examining whether Apple has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data in the context of behavioural analysis and targeted advertising on its platform.	Inquiry ongoing
2	Apple Distribution International	Complaint-based inquiry	Transparency. Examining whether Apple has discharged its GDPR transparency obligations in respect of the information contained in its privacy policy and online documents regarding the processing of personal data of users of its services.	Complaint withdrawn
3	Apple Distribution International	Complaint-based inquiry	Right of Access. Examining whether Apple has complied with the relevant provisions of the GDPR in relation to an access request.	Inquiry ongoing
4	Facebook Inc.	Own-volition inquiry	Facebook September 2018 token breach. Examining whether Facebook Inc. has discharged its GDPR obligations to implement organisational and technical measures to secure and safeguard the personal data of its users.	Inquiry ongoing
5	Facebook Ireland Limited	Complaint-based inquiry	Right of Access and Data Portability. Examining whether Facebook has discharged its GDPR obligations in respect of the right of access to personal data in the Facebook 'Hive' database and portability of "observed" personal data.	Inquiry ongoing
6	Facebook Ireland Limited	Complaint-based inquiry	Lawful basis for processing in relation to Facebook's Terms of Service and Data Policy. Examining whether Facebook has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data of individuals using the Facebook platform.	At decision making phase
7	Facebook Ireland Limited	Complaint-based inquiry	Lawful basis for processing. Examining whether Facebook has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data in the context of	Inquiry ongoing

			behavioural analysis and targeted advertising on its platform.	
8	Facebook Ireland Limited	Own-volition inquiry	Facebook September 2018 token breach. Examining whether Facebook Ireland has discharged its GDPR obligations to implement organisational and technical measures to secure and safeguard the personal data of its users.	Inquiry ongoing
9	Facebook Ireland Limited	Own-volition inquiry	Facebook September 2018 token breach. Examining Facebook's compliance with the GDPR's breach notification obligations.	Inquiry ongoing
10	Facebook Ireland Limited	Own-volition inquiry	Commenced in response to large number of breaches notified to the DPC during the period since 25 May 2018 (separate to the token breach). Examining whether Facebook has discharged its GDPR obligations to implement organisational and technical measures to secure and safeguard the personal data of its users.	Inquiry ongoing (submissions received from relevant parties on the draft investigation report, final report being prepared)
11	Facebook Ireland Limited	Own-volition inquiry	Facebook passwords stored in plain text format in its internal servers. Examining Facebook's compliance with its obligations under the relevant provisions of the GDPR.	Inquiry ongoing
12	Google Ireland Limited	Own-volition inquiry	Commenced in response to submissions received.Examining Google's compliance with the relevant provisions of the GDPR. The GDPR principles of transparency and data minimisation, as well as Google's retention practices, will also be examined.	Inquiry ongoing
13	Google Ireland Limited	Own-volition inquiry	The Inquiry will 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.	Inquiry ongoing
14	Instagram (Facebook Ireland Limited)	Complaint based inquiry	Lawful basis for processing in relation to Instagram's Terms of Use and Data Policy. Examining whether Instagram has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data of individuals using the Instagram platform	Inquiry ongoing (draft inquiry report provided to relevant parties)

15	LinkedIn Ireland Unlimited Company	Complaint-based inquiry	Lawful basis for processing. Examining whether LinkedIn has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data in the context of behavioural analysis and targeted advertising on its platform.	Inquiry ongoing
16	MTCH Technology Services Limited (Tinder)	Own-volition inquiry	The Inquiry of the DPC will set out to establish whether the company 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 and its compliance with data subject right's requests.	Inquiry ongoing
17	Quantcast International Limited	Own-volition inquiry	Commenced in response to a submission received. Examining Quantcast's compliance with the relevant provisions of the GDPR. The GDPR principle of transparency and retention practices will also be examined.	Inquiry ongoing
18	Twitter International Company	Complaint-based inquiry	Right of Access. Examining whether Twitter has discharged its obligations in respect of the right of access to links accessed on Twitter.	Inquiry ongoing
19	Twitter International Company	Own-volition inquiry	Commenced in response to the large number of breaches notified to the DPC during the period since 25 May 2018. Examining whether Twitter has discharged its GDPR obligations to implement organisational and technical measures to secure and safeguard the personal data of its users.	Inquiry ongoing
20	Twitter International Company	Own-volition inquiry	Commenced in response to a breach notification. Examining an issue relating to Twitter's compliance with Article 33 of the GDPR.	Draft decision circulated under Article 60 of the GDPR to concerned supervisory authorities.
21	Verizon Media/Oath	Own-volition inquiry	Transparency. Examining the company's compliance with the requirements to provide transparent information to data subjects under the provisions of Articles 12-14 GDPR.	Inquiry ongoing
22	WhatsApp Ireland Limited	Complaint-based inquiry	Lawful basis for processing in relation to WhatsApp's Terms of Service and Privacy Policy. Examining whether WhatsApp has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal	Inquiry ongoing (draft inquiry report provided to relevant parties)

			data of individuals using the WhatsApp platform.	
23	WhatsApp Ireland Limited	Own-volition inquiry	Transparency. Examining whether WhatsApp has discharged its GDPR transparency obligations with regard to the provision of information and the transparency of that information to both users and non-users of WhatsApp's services, including information provided to data subjects about the processing of information between WhatsApp and other Facebook companies.	At decision making phase
24	Yelp	Own-volition inquiry	Inquiry into Yelp's compliance with Articles 5, 6, 7 and 17 of GDPR following a number of complaints received by the DPC in relation to the processing of personal data by Yelp on its website.	Inquiry ongoing

National Statutory Inquiries Commenced Since May 2018

	Organisation	Inquiry type	Issue being examined	Status
1	An Garda Síochána	Own Volition	State Surveillance	Decision issued
2	An Garda Síochána	Own Volition	Disclosure Requests from An Garda Síochána to external data controllers	Inquiry ongoing
3	An Garda Síochána	Own Volition	Breach of security resulting in unauthorised disclosure of personal data held for LED processing	Inquiry ongoing
4	Bank of Ireland	Own Volition	Multiple breaches, resulting in an infringement of the rights and freedoms of a data subject. Data Accuracy, particularly where personal data is used in relation to the assessment of behavioural aspects such as reliability.	Inquiry ongoing
5	BEO Solutions	Own Volition	A personal data breach occurring through the loss of an unencrypted USB storage device. Related to inquiry into PIAB.	Inquiry ongoing
6	Catholic Church	Own Volition	Multiple complaints re right to rectification & right to be forgotten	Inquiry ongoing
7	DEASP	Own Volition	Article 38: Independence of the data protection officer	Inquiry ongoing
8	HSE Dublin and Mid Leinster (Tullamore Labs)	Own Volition	Ransomware Attack (Malware) Art 28 & 32.	Inquiry ongoing
9	HSE Our Lady of Lourdes	Own Volition	Own volition inquiry following media reports and review of breach notifications, personal data found by member of the public in a public place. Security of processing, appropriate organisational and technical measures following the loss of sensitive personal data.	At decision making phase
10	HSE South	Own Volition	Personal data breach, unauthorised disposal of personal data at a recycling facility in Cork	At decision making phase
11	Irish Credit Bureau	Own Volition	Data Integrity Breach. System change allowed invalid updates to be applied to loan accounts of members' customers.	Inquiry ongoing
12	Irish Prison Service	Own Volition	legal basis for Data Processing by OSG	Inquiry ongoing
13	Maynooth University	Own Volition	Email accounts compromised - financial fraud - Art 32, 33, 34	Inquiry ongoing
14	Personal Injuries Assessment Board	Own Volition	A personal data breach occurring through the loss of a USB storage device. Related to inquiry into BEO Solutions	Inquiry ongoing

15	Slane Credit Union	Own Volition	Unauthorised Disclosure of member data on website	Inquiry ongoing
16	SUSI	Own Volition	Data Integrity and Confidentiality Breach. Malware (WSO Shell, fake plugins on webserver, SEO manipulation code). Art 28, 30, 31, 32, 33 & 34.	Inquiry ongoing
17	Teaching Council	Own Volition	Inquiry concerning the breach of two email accounts held by staff of the Council, email redirection rules were set which caused the unauthorised processing of 332 emails containing personal data of a large number of data subjects.	Inquiry ongoing
18	TUSLA	Own Volition	Data Breach	Decision issued
19	TUSLA	Own Volition	Multiple breaches	Decision issued
20	TUSLA	Own Volition	Own volition from 72 breaches collated June 2018 - 6 Dec 18 Sensitive data disclosed in large variety of breaches.	At decision making phase
21	UCD	Own Volition	Multiple breaches	Inquiry ongoing
22	University of Limerick	Own Volition	Email account phished	Inquiry ongoing
23-53	31 local authorities	Own Volition	State Surveillance	25 inquiry ongoing, six in decision making phase

Decisions

Domestic Decisions Under the Data Protection Act 2018

An Garda Síochana and Kerry County Council

The first two decisions of the DPC under the Data Protection Act, 2018, concerning An Garda Síochána and Kerry County Council, are covered in detail in **Appendix 1**: Surveillance by the State Sector for Law Enforcement Purposes. These decisions were in respect of own-volition inquiries into surveillance of citizens by the state sector for law-enforcement purposes, through the use of technologies such as CCTV, body-worn cameras, drones and other technologies such as automatic number-plate recognition (ANPR) enabled systems.

The first decision was issued by the Commissioner in August 2019 and concerned An Garda Síochána. It made a number of findings into the use of ANPR cameras, access to CCTV monitoring rooms, governance issues, appropriate signage and general transparency, and the absence of written contracts with third party processors. The decision also exercised corrective powers.

The second decision was issued by the Commissioner in March 2020 and concerned Kerry County Council. It found that certain CCTV systems operated by Kerry County Council were unlawful in the absence of authorisation from the Garda Commissioner under Section 38 of An Garda Síochána Act 2005. Significantly in this regard, the Litter Pollution Act 1997, the Waste Management Act 1996 (as amended), and the Local Government Act 2001 were comprehensively considered and the decision found that those Acts do not provide a lawful basis for the use of CCTV for law enforcement purposes.

The decision also made findings on appropriate signage and general transparency, excessive data collection, the lack of written rules or guidelines governing staff access to the CCTV, the use of smartphones or other recording devices in the CCTV monitoring room, the practice of sharing login details for accessing CCTV footage, auditing the audit trails of CCTV footage, security for transferring CCTV footage to An Garda Síochána, record keeping for An Garda Síochána's access to the CCTV footage, and the requirement for Data Protection Impact Assessments. The decision also exercised corrective powers.

TUSLA

In April 2020, the Commissioner issued a decision in respect of an own-volition inquiry regarding three personal data breaches notified to the DPC by Tusla. These breaches occurred when Tusla failed to appropriately redact documents when sharing them with third parties.

The inquiry commenced on 24 October 2019 and examined whether or not Tusla had discharged its obligations in connection with the breaches, in order to determine whether or not any provision(s) of the GDPR and/or the 2018 Act had been contravened by Tusla. The office completed its final inquiry report on 24 February 2020 and submitted it to the decision-maker (the Commissioner).

The decision considered the appropriateness of the technical and organisational measures implemented by Tusla at the time of the breaches. Tusla was provided with the opportunity to make submissions at decision-making stage. The decision found that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate measures with regard to the redaction of documents. The decision also considered one of the notified personal data breaches with regard to the duty to notify the DPC without undue delay pursuant to Article 33(1) of the GDPR. Tulsa notified the DPC of this breach 5 days after becoming aware of it. The decision found that this constituted an undue delay in the circumstances and found that Tusla had infringed Article 33(1). The decision reprimanded Tusla, ordered it to bring its processing into compliance with Article 32(1) of the GDPR, and imposed an administrative fine of €75,000. An application to confirm the administrative fine is currently pending before the Circuit Court.

In May 2020, the Commissioner issued a decision regarding another own-volition inquiry concerning Tusla. This inquiry concerned one personal data breach that Tusla notified to the DPC on 4 November 2019. The inquiry commenced on 11 December 2019 and examined whether or not Tusla had discharged its obligations in connection with the subject matter of the breach to determine whether or not any provision(s) of the GDPR and/or the 2018 Act had been contravened by Tusla.

The breach concerned the disclosure, to a third party, of the identity of data subjects who had made allegations of abuse and the details of the allegations made. The letter disclosing the details was later shared on social media by the recipient of the letter. On 19 March 2020, the DPC completed the final inquiry report and submitted it to the decision-maker (the Commissioner). Tusla was provided with the opportunity to make submissions at decision-making stage.

The decision considered the appropriateness of the technical and organisational measures implemented by Tusla at the time of the breach in respect of its safeguarding letter process. It found that Tusla infringed Article 32(1) of the GDPR by failing to implement organisational measures appropriate to the risk. The decision also considered the breach with regard to the duty to notify the DPC without undue delay pursuant to Article 33(1) of the GDPR. This breach was notified to the DPC over 29 weeks after Tusla became aware of it.

The decision found that Tusla infringed Article 33(1) by failing to notify the DPC of the breach without undue delay. The decision reprimanded Tusla, ordered it to bring its processing into

compliance with Article 32(1) of the GDPR, and imposed an administrative fine. Tusla has 28 days from receipt of the decision to decide whether it wishes to appeal the decision.

Decisions Under the Data Protection Act 2018 to Which Article 60 Applies

In May 2020 the DPC submitted a draft decision to other concerned Supervisory Authorities, in accordance with **Article 60** of the GDPR, in relation to an inquiry it has completed into Twitter International Company, a data controller based in Ireland.

This own-volition inquiry was commenced by the DPC on 22 January 2019, following receipt of a data breach notification from the controller. The draft decision focusses on whether Twitter International Company has complied with Articles 33(1) and 33(5) of the GDPR.

Also in May 2020, the DPC sent a preliminary draft decision to WhatsApp Ireland Limited, seeking their final submissions, which will be taken in to account by the DPC before preparing its draft Article 60 decision regarding the DPC's inquiry into the company's compliance with Articles 12 to 14 of the GDPR in terms of transparency; including transparency around what information is shared with Facebook.

The DPC has also completed the investigation phase of a complaint-based inquiry which focuses on Facebook Ireland's obligations to establish a lawful basis for personal data processing. This inquiry is now in the decision-making phase at the DPC.

The DPC has also sent draft inquiry reports to the complainants and companies concerned in two further big tech inquiries – these inquiries concern the Instagram and WhatsApp platforms respectively. These draft inquiry reports mark a significant milestone in the inquiry process and all parties (both the controller and the complainants) will have an opportunity to make submissions, after which a final inquiry report will be prepared for the decision-maker.

Litigation

Since the GDPR came into effect in May 2018, the DPC has concluded nine litigation actions, the details of which are summarised in the table below.

Cases Concluded Since May 2018

No.	Record No.	Title	Type of action and Venue	Date of Judgment	Outcome of Judgment and link/copy	Current Status of Case
1.	2018/0040	Lavinia O'Shea v. DPC	Statutory appeal, Portlaoise Circuit Court	1 June 2018	Statutory appeal dismissed in favour of the DPC. The Circuit Court ruled that it had no jurisdiction in this matter, as no decision had in fact been issued by the Commissioner. The Court ruled also that the Appellant had issued her proceedings in the incorrect jurisdiction; and therefore dismissed the appeal.	Finalised – no appeal
2.	2018/54 CA	Agnieszka Nowak v. DPC	Appeal of Circuit Court statutory appeal decision, High Court	12 July 2018	The High Court found in favour of the DPC and dismissed the Appellant's appeal against the Order of the Circuit Court. The High Court held that there was no error of law, either by the Commissioner or by the Circuit Court in reaching their respective determinations.	The Appellant filed an appeal to the Court of Appeal, which is listed for hearing on 15 January 2021.

3.		DPC v. Clydaville Investment Group t/a Kilkenny Group	Direct marketing prosecution, Tralee District Court	16 October 2018	Clydaville convicted of two charges; the other two charges were dismissed.	Finalised – no appeal
4.	2018/0017	Young's Garage v. DPC (Notice Party: Bank of Ireland)	Statutory appeal, Nenagh Circuit Court	4 February 2019 (Oral judgment only)	The Court found in favour of the DPC and upheld the Commissioner's decision, noting that (1) the Commissioner's decision that the Appellant (Young's Garage) was a data controller was correct, (2) it was clear the Appellant was not a processor for the bank and (3) the Appellant had not provided evidence that it had obtained the complainant's unambiguous consent to the processing of his data.	The Appellant initially filed a Notice of Appeal in the High Court on 11 February 2019, but subsequently issued a Notice to Withdraw on 11 March 2019. Therefore, the case is now concluded.
5.	2018/5134 (Circuit Court) 2019/211 CA (High Court)	Cormac Doolin v. DPC (Notice Party: Our Lady's Hospice and Care Services ("OLHCS"))	Statutory appeal, Circuit Court and appeal to High Court	Circuit Court: 1 May 2019 (Ex-Tempore) High Court: 21 February 2020	The Circuit Court found in favour of the DPC and upheld the Commissioner's decision, noting that the Commissioner was correct in finding that (1) there was <u>one</u> investigation carried out by OLHCS, which was based on security concerns and (2) the disciplinary action taken against the Appellant by OLHCS was taken for security reasons. Therefore, there was no breach of Section 2 of the Acts by OLHCS. The High Court found against the DPC and set aside the Commissioner's decision insofar as it stated that no contravention of s.2(1)(c)(ii) of the Acts occurred.	The DPC filed an appeal with the Court of Appeal on 3 April 2020. Hearing date awaited.

6.	2018/68 (Supreme Court)	DPC v. Facebook Ireland Limited and Maximillian Schrems	Supreme Court	31 May 2019	Supreme Court dismissed Facebook's appeal and affirmed the order of the High Court referring questions to the CJEU.	Pending judgment of the CJEU – expected on 16 July 2020.
7.	2017/464 & 2017/459 (Court of Appeal)	Grant Thornton (plaintiff/respondent) v. Gerardine Scanlan (defendant/Appellant)	Appeal of High Court Decision – including refusal to join DPC as Notice Party, Court of Appeal	31 October 2019	The Court of Appeal upheld the orders of the High Court dated 27 July 2017, one of which related to its refusal of the Appellant's application to join the DPC as a Notice Party to the proceedings. The Court of Appeal dismissed the appeal in its entirety. In paragraphs 48 – 68 of the judgment, the Court held that no case had been made which would justify the joinder of the Commissioner to the proceedings, either as *amicus curiae* or otherwise. The Court also found that no cause of action had been asserted against the Commissioner and that the joinder of the Commissioner would be inappropriate. [NOTE: this is not the conclusion of these proceedings, as the main (High Court) case has yet to be heard, but it concludes the DPC's involvement and is the conclusion of the Court of Appeal case.]	No appeal taken to date
8.	2019/95 JR	Aimee Scott v. DPC	Judicial Review, High Court	5 December 2019	The High Court found in favour of the DPC and struck out the proceedings on grounds of mootness.	The Applicant has filed an appeal to the Court of Appeal, which is listed for hearing on

						21 October 2020.
9.	2018/4097	Courts Service v. DPC (Notice Party: P.M.)	Statutory appeal, Dublin Circuit Court	3 February 2020	The Circuit Court found in favour of the DPC on the main points, but against the DPC on other points. The Circuit Court refused to set aside the decision of the Commissioner and agreed with the DPC's finding that the Appellant (Courts Service) was a data controller. However, the Court set aside the Commissioner's finding that the Appellant breached Section 2(1)(d) of the Acts. The Court also ordered that the finding that the Appellant had breached section 2A and section 2B(1) of the Acts be limited to the period of 12–15 May 2014.	On 17 February 2020, the Appellant filed an appeal to the High Court. Currently adjourned generally.

CJEU

The Court of Justice of the European Union (CJEU) announced on 14 May that it will deliver its judgment in the case of Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems (Case C-311/18) on 16 July 2020. The case concerns proceedings initiated and pursued in the Irish High Court by the DPC, which raised a number of significant questions about the regulation of international data transfers under EU data protection law. The judgment from the CJEU - on foot of the reference made arising from these proceedings - is anticipated to bring much needed clarity to aspects of the law and to represent a milestone in the law on international transfers.

The detailed background to the Litigation concerning Standard Contractual Clauses can be read in the DPC's 2019 Annual Report; **Appendix II**.

Supervision

The 25 May 2018 brought immeasurable change to the remit of the Irish Data Protection Commission bringing, as it did, the numerous large-scale multinational companies who are headquartered in Ireland within the regulatory scope of the DPC.

Subsequent to the implementation of the GDPR, the DPC now acts as Lead Supervisory Authority for such entities as Facebook, WhatsApp, Twitter, MTCH, LinkedIn and Google; in accordance with the One Stop Shop mechanism of the Regulation. The manifestation of this regulatory responsibility is multifaceted, reflected both in the **inquiries** that the DPC undertakes and in its supervision actions, where the DPC proactively engages on issues that have the potential to prove problematic to the rights and freedoms of individuals.

In line with **Article 57** of the GDPR, the Supervision function of the DPC promotes regulatory stability by monitoring relevant developments in information technologies and commercial practice. This supervisory role further enables the DPC to understand the ways in which personal data are being processed by these entities and identify the processing concerns that may be implicit in proposed products and services. In this way, the DPC has in the past two years advocated for the rights of individuals by mitigating against potential infringements before they have occurred.

Supervisory activity is a key function of the DPC and is not limited to the multitech sector. Supervision extends to all entities within the DPC's regulatory sphere, but in particular those whose activities are likely to have consequences for large numbers of individuals. To this end, supervision extends to encompass the health, voluntary, public, financial and insurance sectors, among others.

Case Studies

Health and Voluntary

Commencing in 2019, the DPC has undertaken a series of outreach engagements under **Article 57(1)(d)** of the GDPR, to promote awareness and understanding of data protection responsibilities amongst the organisations in these two sectors.

Hospital Grand Rounds

Since November 2019, the DPC has attended 'Grand Rounds' in several of Dublin's major hospitals to deliver presentations on data processing in the hospital context. The primary purpose of these presentations is to provide focussed guidance on data processing operations in hospitals, following up on the recommendations made in the report of the **DPC's investigation into the Hospitals Sector** published in May 2018. However, an important secondary purpose of the presentations is to highlight awareness and understanding of the role of the Data Protection Officer within the hospital. This is part of the DPC's strategic goal of supporting DPOs in their critical role within their organisations.

Public Sector

Development of Section 40 Guidelines for Elected Representatives

Following DPC engagement with elected representatives and the Houses of the Oireachtas (Irish Parliament) on the implementation of both the GDPR and Data Protection Act 2018, the DPC undertook to develop and publish guidelines for elected representatives (including members of both houses of the Oireachtas, Local Authorities and the European Parliament) on data processing under **Section 40** of the Data Protection Act, 2018. Section 40 provides for the processing of personal data by elected representatives in their role as advocates on behalf of constituents and members of the public.

The **guidelines** were published in December, 2018 and were subsequently presented to members of the Oireachtas and their staff in a special briefing, as well as elected members of Local Authorities at the Association of Irish Local Government annual conference in 2019. These briefings also provided an opportunity to promote awareness and understanding among elected representatives of their general obligations as data controllers.

Financial Sector

Data minimisation and AML

The DPC received a query regarding an investment firm, which was selling properties and seeking to obtain AML identification or '*Know your Customer*' data (KYC) from the third party purchasers.

The DPC instructed that, pursuant to the Criminal Justice (Money laundering and terrorist financing) Act 2010 (as amended) the investment firm could not be considered a "Designated Person" (nor an "Obliged Entity" as defined in the AML Directives) to collect AML KYC documentation. This is a statutory public interest function only, proper to the purchaser's solicitors or the credit institution that is providing a mortgage or loan facility to the purchaser. Both the purchaser's solicitor and/or the lending institution are a "designated person" under the 2010 Act and as such, each should comply with the AML requirements when ascertaining the 'Customer due diligence', of their client(s) who are purchasing the property from the vendor.

From a data protection perspective, unless there is a proper legal justification for the collection of this KYC documentation of third party purchasers then the practice of seeking to collect these documents, should cease immediately. Otherwise it could potentially contravene the principles of **Article 5** of the GDPR.

The Law Society of Ireland committee on AML/Conveyancing also commented that such practices were not appropriate.

Following DPC representations, the companies agreed to cease this practice of seeking KYC AML documentation from third party purchasers and their representatives.

Insurance Sector

Excessive processing of personal data for insurance purposes

The DPC received a query from an individual who was concerned that an insurance company had processed excessive information about her in order to generate a quote for car insurance.

The insurance company had sought and obtained penalty point data pertaining to this individual spanning five years. [10] Significantly, under Irish law, penalty point demerits expire after three years. Having two additional years' data was deemed a beneficial advantage to the insurance company when assessing premiums. Some policy holders were charged an extra premium, which was calculated on the basis of this extraneous data.

[10] Penalty points are applied to Irish driving licences where a driver is deemed to have infringed motoring laws. They are directly associated with the individual licence holder. The number of points applied is governed by the severity of the infringement(s), potentially culminating in disqualification from driving.

The DPC contacted the DPO of the insurance company seeking clarification around the practice of obtaining extra data from consumers. The DPC further requested that the company:

- Change its websites to only seek 3 years of penalty point data.
- Ascertain how many account holders could have been impacted by the collection of this excessive data.
- Ascertain how many customers were charged extra for their insurance premium as a result of this 5 year penalty point data.
- Rectify these identified issues.

The DPO subsequently confirmed that 21,000 policies were deemed to be in scope of these criteria and reviewed. 94 policies were identified as having been charged the additional premium on the basis of over-processing and the company had begun contacting these customers to refund the additional charges.

The DPO further confirmed that all required changes to its websites which had been requested by the DPC were now implemented, and the practice of seeking five-year penalty point history had ceased. The company has also commenced a full review of its databases to ensure that all expired penalty point data is deleted.

Multinational

Facebook Dating

On foot of inadequate information provided by Facebook Ireland in relation to its intended roll-out of a new dating feature in the EU, authorised officers of the DPC conducted an inspection at Facebook Ireland Limited's offices in Dublin to gather relevant documentation.

Having reviewed the documentation, the DPC raised a number of concerns regarding the proposal. The DPC awaits a substantive response from Facebook. Facebook has advised that the DPC will be updated with the relevant documentation and that they will respond to our concerns.

Facebook also advised that they have postponed the roll-out of this feature, subsequent to DPC engagement.

Facebook – Election Day Reminder

The Election Day Reminder (EDR) feature is one which is provided by the Facebook platform during election campaigns across Europe. Upon examination of the feature, the DPC raised a number of concerns - particularly in relation to the transparency of processing and the means by which personal data is collected when interacting with the feature and subsequently used by Facebook.

The DPC sought a number of remedial actions from Facebook. However, as it was not possible to implement these in advance of government elections in Ireland, Facebook decided not to launch the EDR during the Irish general election. Facebook have also confirmed that the Election Day Reminder feature will not be activated during any EU elections, pending its response to the concerns raised by the DPC.

Google Location Tracking

Since late 2018, the DPC has had ongoing supervisory interactions with Google, in respect of both complaints and external reports of excessive data collection and location tracking by the company.

On foot of these interactions, Google has implemented changes to Location History and Web & App Activity. The updates include changes to settings, to facilitate greater transparency and user control.

Notwithstanding the interactions that the DPC has had with Google and despite changes being introduced, the DPC has launched a separate inquiry into the matter. The scope of that inquiry has been informed by the supervisory interactions to date.

Voice Data – Microsoft/Google/Apple

The DPC have engaged with these three companies regarding processing of voice data and related compliance matters. This has resulted in changes being made as to how voice data is being processed with additional controls/transparency being provided to users by all three.

The DPC engaged with other concerned Supervisory Authorities on this matter to discuss and identify the key data protection implications that this type of technology poses, with a view to developing pan-European guidelines for future use. As a result of this engagement, Ireland now has a mandate from the EDPB to draft guidelines in this matter.

LinkedIn – Member-to-Guest Connection

Following numerous engagements with the DPC, LinkedIn has ceased to display the member-to-guest connection invitation screen on its platform, which was previously generated by syncing the address books of its European members.

LinkedIn state that this decision was made as a result of reviewing feedback from the DPC, whereby it concluded that the feature was no longer providing significant value for its European members and subsequently decided to remove this feature in Europe. The DPC welcomes the upgrade and views it as a positive step taken by LinkedIn Ireland in meeting its GDPR requirements, particularly for the processing of non-user data.

Other Regulatory Activity

Direct Marketing Complaints

In addition to complaints handled under the GDPR and the Data Protection Act 2018, the DPC receives a significant number of complaints in relation to unsolicited direct marketing sent by electronic means – primarily by text message and email.

These complaints are investigated pursuant to **S.I. No. 336 of 2011**, the European Communities (Electronic Communications Networks and Services)(Privacy and Electronic Communications) Regulations, and the DPC actively prosecutes entities for breaches of the law in this area.

Since May 2018, the DPC has **opened approximately 282 new direct marketing complaints and concluded approximately 247**. A total of 85 of those new complaints were opened in the first five months of 2020 and 78 complaints have been concluded this year to date.

While the investigation and prosecution of direct marketing complaints is carried out pursuant to the ePrivacy Regulations, in the course of its investigations into these matters the DPC also identifies potential GDPR-related systemic issues that may indicate unlawful processing of personal data, including issues arising in specific sectors where the DPC identifies trends in the nature or volume of the complaints received.

Where particular concerns are identified, this will result in the DPC instigating separate inquiries under the GDPR and the Data Protection Act 2018.

Prosecutions

In the period from May to December 2018, five entities were prosecuted in respect of a total of 30 offences under the ePrivacy Regulations. These included Viking Direct (Ireland), Clydaville Investments Ltd t/a The Kilkenny Group, DSG Retail Ireland Ltd, Vodafone Ireland and Starrus Eco Holdings t/a Panda and Greenstar. Vodafone was also among the organisations prosecuted by the DPC in 2019.

At the Dublin Metropolitan District Court on 29 July 2019, Vodafone Ireland Limited was fined a total of €4,500 having entered guilty pleas to five separate offences under S.I. No. 336/2011 ('the ePrivacy Regulations').

On the same date, the DPC also prosecuted the food ordering service Just-Eat Ireland Limited, and online retailers Cari's Closet Limited and Shop Direct Ireland Limited (t/a Littlewoods Ireland). The Probation of Offenders Act was applied in respect of each of these organisations, on condition that they make donations to named charities.

On 2 March 2020, at the Dublin Metropolitan District Court, the DPC prosecuted Three Ireland (Hutchison Limited) on eight charges under Regulation 13(1) of SI 336 of 2011.

Guilty pleas were entered on two charges and the remaining charges were withdrawn. The court applied section 1(1) of the Probation of Offenders Act on the basis that the company make a donation of €200 to Little Flower Penny Dinners in respect of each charge and with agreement that it would discharge the costs of the DPC.

Mizzoni's Pizza & Pasta Company Limited was also prosecuted before the court on 2 March 2020 on four charges under Regulation 13(1). The company entered a guilty plea on one charge and the remaining charges withdrawn. Section 1(1) of the Probation of Offenders Act was applied on the basis that the company make a donation of €200 to Little Flower Penny Dinners and with agreement that it would discharge the costs of the DPC.

Cookies Sweep 2019-2020

In April 2020, the DPC published a **report** on the use of cookies and other tracking technologies along with new **guidance** for controllers on the use of these tools on their websites and in other products and services.

These two documents were published following a cookies sweep which commenced in August 2019 and which examined practices on websites across a number of industry sectors and the

public sector. They are the first outcomes of one of the most extensive pieces of work carried out to date in this area by the DPC but they mark only the beginning of our work in this area.

The use of cookies and tracking technologies is primarily examined through the lens of the ePrivacy Regulations, which protect privacy in electronic communications. However, where personal data is also processed as a result of the use of these technologies, the GDPR applies to that processing.

The DPC's report outlined a number of significant concerns about the use of cookies – in particular the failure of many organisations to obtain valid consent from the users of their websites for the use of such tracking. The DPC also highlighted in the report how organisations were relying on so-called 'implied consent' for the use of these tracking tools and that this does not meet the standard of consent required by the GDPR.

Transparency in relation to the use of cookies and tracking, and in particular the requirements for valid consent, will be to the fore in our ongoing examination of controllers' practices.

In the course of this project, the DPC also identified a number of wider issues that will be the focus of its attention in the coming months and years. These include concerns about the potential processing of special category data, including health data, on some websites.

The report and guidance has been circulated to all 38 controllers who took part in the cookies sweep and also more widely to industry and business representative bodies, to our DPO network and to membership-based compliance organisations.

The DPC also produced a **podcast** to accompany these documents.

The DPC now expects that all controllers who use cookies and tracking technologies will begin to audit their practices and policies and that they will, in particular, be able to demonstrate that they obtain valid consent for the use of these tools on their websites, apps and other products.

The DPC will allow a period of six months from the date of the publication of the report and guidance on 6 April 2020 for controllers to identify any areas of non-compliance and to bring themselves into compliance. After 5 October 2020, the DPC will commence enforcement action against controllers who fail to comply.

Such action will include enforcement notices under the ePrivacy Regulations and, where the controller is processing personal data resulting from its use of cookies, the DPC will use its powers under the GDPR and the Data Protection Act 2018 to initiate inquiries and investigations and to carry out inspections where required.

Law Enforcement Directive Complaints

66 LED complaints have been handled by the DPC since the Law Enforcement Directive came into force in May 2018, as transposed in the Irish Data Protection Act 2018. The majority of complaints handled concerned the Irish police force (An Garda Síochána) and its alleged failure to provide all the personal data of an individual in response to a subject access request, in addition to

complaints regarding driving penalty notices, traffic accidents and CCTV footage. Many LED cases are complex and sensitive, with files relating to arrest warrants, sexual abuse, rape and gangland activity. Data gathered in connection with fines incurred travelling on public transport have also emerged on the LED radar as well as complaints in relation to the Revenue Commissioners, the Irish Prison Service and several local authorities.

Section 94 of the 2018 Act allows data controllers to restrict access to personal data on grounds such as the prevention of crime and to avoid prejudicing an investigation or prosecution. Where an individual is made aware that their rights have been restricted under the provisions of Section 94, they may request that the DPC independently review their case under Section 95 (Article 17, EU 2016/680). To date, **five Section 95 reviews** have been conducted. In the majority of cases, DPC authorised officers were satisfied the restrictions were lawful. In one case, additional clarification was requested with regard to the restrictions relied upon as set out in the schedule issued by the data controller to the data subject. This clarification is still pending.

Binding Corporate Rules (BCRs)

The EDPB has issued Article 64 opinions on five Binding Corporate Rules. The most recent of these was a dual BCR-Controller and BCR-Processor of Reinsurance Group of America for which the DPC acted as Lead Authority. This is the first dual BCR that has been issued with an Article 64 opinion to date. BCRs with both controller and processor documents incur a significant workload, as they require two separate opinions from the Board and two separate decisions from the Lead Authority (DPC), requiring a large number of documents to be circulated, comments collated, applicant amendments reviewed and updated documents made available to all DPA's in timely fashion.

Brexit and Transfers

Since the end of 2018, the DPC has been proactively involved in awareness raising to advise Irish entities transferring data to the UK on what Brexit meant for them, particularly if a withdrawal agreement was not achieved. The DPC has:

- Attended stakeholder events with IBEC for both smaller and large entities;
- Participated in webinars;
- Provided written guidance to assist Enterprise Ireland;
- Published guidance on the DPC's website;
- Recorded an episode of the DPC podcast dedicated to this issue; and
- Presented extensively at stakeholder events in an effort to reach the largest audience possible.

This work is ongoing as the Brexit transition period reaches expiration if there is not an adequacy decision in place.

Codes of Conduct and Certifications

The DPC has been closely involved in the development of operational rules to implement two of the accountability tools called out in the GDPR; specifically, Codes of Conduct and Certification Mechanisms. These tools will enable organisations to align their processing activities with defined specifications, as agreed with their peers in the various sectoral areas and approved through the relevant supervisory authorities and the EDPB. Both codes and certifications will make it possible for organisations to move beyond guidance and best practice; instead specifying the means by which processing activities within their respective sectors are to be conducted in accordance with defined, validated and recognised standards.

Codes of conduct may have associated monitoring bodies, while certification for particular processing activities will be awarded by entities accredited by the Irish National Accreditation Board (INAB) and in accordance with international standard ISO-17065. Codes of conduct and certification mechanisms may be national or have EU-wide scope.

In 2020, the DPC successfully completed the EDPB Article 64 consistency opinion process for both Codes of Conduct monitoring bodies and for the "additional requirements" under Article 43(1)(b) for the INAB. These represent the first steps toward operationalising accountability tools for use by organisations in Ireland. As certifications and codes of conduct begin to shape processing activities for their relevant sectors, the DPC will include compliance with the provisions of these tools as part of its adjudication process.

Data Protection Officers

DPO Notifications

Sector	Number of notifications
Private	1,390
Public	231
Not-for-profit	202
Total	1,823

The advent of the GDPR also saw the introduction of the **Data Protection Officer requirement**, for public sector bodies and organisations whose core processing activities could be classed as high-risk or far-reaching in scope.

The DPO is the intermediary point of contact between the data protection authority and a given organisation; driving compliance with data protection legislation and ensuring that processing activities – and all attendant activities, including DPIAs where necessary – are carried out in line with the provisions of the GDPR.

In the two years since the introduction of the role, there have been 1,823 DPOs registered with the Data Protection Commission. The DPC anticipates that this figure will grow consistently over the coming years, as processing operations become more complex and more and more organisations reach the required threshold.

As indicated by the **trends and patterns** that have been observed in the DPC's complaint and breach statistics over the lifetime of the GDPR, the DPC continues to see high volumes of cases that could be resolved at DPO or controller level; either by appropriate engagement with customers or by implementing pertinent technical and organisational measures to mitigate against breaches. In order to redress the imbalance in volume and to improve response times for individuals, the DPC identified DPOs as a sector in need of additional supports.

The DPC reached out to DPOs across many sectors and established networks - public, private and not-for-profit – to garner on-the-job insights into their challenges and opportunities, the resources at their disposal and the data protection issues that reoccur for them.

What emerged from this engagement was a prevailing sense of disconnect between the role of the DPO as described in the **GDPR** and its manifestation in reality, albeit a disconnect that may have its roots in misunderstanding.

Many DPOs reported feeling isolated in their role, under resourced and solely accountable for the activities of the data controller. Data controllers, in their turn, reported confusion regarding the necessary qualifications for DPOs and the way in which DPOs were to be incorporated into planning and operations. For many organisations, the role of DPO was not bedding down in a harmonised way.

The non-prescriptive phrasing of **Article 37(5)** - wherein the professional qualities and subject expertise of the DPO role are not quantified by a specified qualification - allows organisations the latitude to assess for themselves what attributes and experience are necessary to meet the needs of their individual circumstances. The DPO, for their part, should have a thorough knowledge of the processing activities of their organisation, and the overall structure of the business, with which they can identify and address risks. The introduction of DPOs was not intended to stymie business, but rather to facilitate the provision of a critical friend – bespoke to the needs of an organisation – to ensure that business could progress in a compliant manner. Significantly, the mere appointment of a data protection officer does not signify compliance; neither are infringements of the legislation solely accountable to the DPO. Data protection remains the responsibility of all staff; an understanding that needs to be inculcated throughout organisations.

As part of its efforts to empower DPOs in the conduct of their duties, the DPC established a Data Protection Officer Network in late 2019. The purpose of the network is to facilitate the sharing of knowledge and good practice through peer-to-peer DPO support. In order to strike the appropriate balance between guiding and regulating, the DPC sought to create a climate that allows professional relationships to build and knowledge to be shared between those who inhabit the DPO role.

Due to global circumstances, the planned conference that was to address these recurring issues, specifically: risk assessing, breaches, access and erasure requests, legal basis, legitimate interest and data sharing was necessarily postponed. The DPC has instead taken these supports online, with a dedicated section for **DPOs** on its website where the resources are centralised for ease of access. The DPC continues to engage with DPOs on an ongoing basis, to ensure that the resources it produces are informed by the needs of the cohort.

In addition to its work to further the education and empowerment of DPOs, the DPC will also be commencing enforcement actions against organisations that are obliged by the stipulations of the GDPR to appoint a DPO and have failed to do so. This enforcement action will also encompass the organisations where a DPO has been appointed, but that appointment has not been notified to the DPC in accordance with **Article 37** of the GDPR.

SMEs

In advance of the GDPR coming into effect on May 25 2018, the DPC identified the small-to-medium enterprise sector as an area that would require additional supports in order to meet its responsibilities under the Regulation. In most instances the operational scale of SMEs means that their finite resources must be shared between multiple areas of compliance. This limitation of resources is in stark contrast to the sector's correspondingly high reach in terms of data subject interaction; over the last decade, the SME and micro-enterprise sector in Ireland has been consistently poised at approximately 70% of people engaged in employment.[11]

The DPC is in regular and ongoing engagement with the representative bodies who advocate on behalf of the SME sector. In addition to producing **guidance** to foster compliance, staff from the DPC also regularly speak at industry events to further drive compliance and the responsible use of personal data.

The Arc Project

In late 2019, in an extension of its activities in support of SMEs, the DPC agreed to partner with the Croatian Data Protection Authority, AZOP, and Vrije University in Brussels on an EU-Funded project (**The ARC Project**) specifically targeting SMEs. The purpose of the project is to increase compliance across the SME sector.

Initial engagement with SMEs began in Q1 of 2020 and will run for a further two years. Through this engagement - which includes **surveys**, roadshows and conferences - the project intends to develop a more detailed understanding of the climate in which SMEs are operating and how that might vary in response to geographical or other factors. The ultimate output from this project will be a suite of compliance resources that are informed by robust stakeholder insight and scalable according to the needs of the user.

[11] https://www.cso.ie/en/releasesandpublications/ep/p-bii/businessinirelandabridged2012/smallandmediumenterprises/

Children's Data Protection Rights

Public Consultation on the Processing of Children's Data

In early 2018, the DPC allocated specific resources to assessing the particular needs of children in relation to data protection, as a first step towards meeting its enhanced obligations arising from the GDPR with regard to the processing of children's personal data and the rights of children as data subjects. Given the significant new provisions for children's data introduced by the GDPR, as well as a lack of clarity as to how these new rules should be interpreted and implemented in practice, it quickly became clear that a core responsibility of DPAs would be to produce guidance to clarify the standards around the processing of children's personal data for organisations, the wider public and children themselves.

Following exploratory work and engagement with established children's rights stakeholders in Ireland in the run-up to 25 May 2018, the DPC decided to embark upon a public consultation project focusing on several key provisions of the GDPR, relevant to the processing of children's data, in order to inform the drafting of guidance in this area. The purpose of this consultation was twofold: to gather the views of all interested parties and to ensure that children themselves would have a voice in this process, as is their right under Article 12 of the UN Convention on the Rights of the Child.

The consultation was divided into two streams: Stream 1, which launched in December 2018, sought the views of all interested adult stakeholders, in particular parents, educators, and children's rights organisations. Respondents were invited to answer a set of 16 questions set out in the consultation document published on the DPC's website. Stream 2 sought to gather the views of children and young people directly in the classroom through a specially-designed and innovative consultation process that was developed in partnership with the Ombudsman for Children's Office (OCO).

The DPC contacted every school and Youthreach centre in Ireland and invited them to participate in the consultation. The DPC also designed and distributed a "lesson plan pack" of materials to assist teachers in facilitating a discussion with their students about personal data protection rights and to give children the necessary grounding and context to participate meaningfully in the consultation. These materials were tested in a series of pilot workshops organised in October 2018 with the support of the OCO and featuring three school classes across three different age groups.

As a result of these workshops, the DPC was able to test the materials and to ensure that they resonated with children and young people ahead of the launch of Stream 2 in January 2019.

The Stream 2 lesson plan and consultation materials placed a strong emphasis on social media in order to highlight data protection issues in a manner that would engage children and be familiar to them. To this end, the lesson plan was structured around "SquadShare", a fictitious social media app created by the DPC for educational purposes. Children were encouraged to learn about their data protection rights through studying this app, its functionalities and, in particular, SquadShare's privacy policy, which was provided first in adult and then child-friendly language.

As SquadShare resembled many contemporary apps that are popular with children, children were able draw parallels between SquadShare's terms and conditions concerning data processing, as explained in the lesson plan, and the terms and conditions of many of the apps that children use on a daily basis. Once the lesson plan had been completed, children were invited to write down their answers to a series of six consultation questions on feedback posters that were then returned to the DPC.

In total, the DPC received 30 submissions in response to Stream 1 of its consultation, with participants encompassing government departments, public bodies, social media platforms, technology companies, consultancies, trade associations, and charities. Stream 2 gathered the views of approximately 1,200 children with a broad spectrum of representation in terms of geographical spread, types of educational establishment, age range – in both primary and secondary level institutions. The level and quality of engagement and variety of submissions received in response to both streams of the consultation indicate that this area is of critical importance moving forward.

The DPC spent the months following the closure of the consultation analysing the submissions from all respondents. This process culminated in the publication of two statistical reports, each focussing on a separate stream of the consultation. The DPC's report on the children's stream of the consultation ("**Some Stuff You Just Want to Keep Private**") was published in July 2019 and the report on the adults' stream ("**Whose Rights Are They Anyway?**") was published in September 2019. These reports provided a statistical overview of participation in the consultation, the DPC's views in relation to the questions asked in both streams, along with select quotes and suggestions put forward by respondents. The project was cited by the ICDPPC Digital Education Working Group (DEWG) as a core international initiative under the DEWG's Action Plan for "Awareness-raising on the exercise of digital rights by the children themselves".

The DPC is preparing draft guidance on the processing of children's personal data and the rights of children as data subjects. This guidance will provide baseline standards for organisations that interact with children – particularly in the digital environment - and is informed by the submissions received in response to the public consultation.

Other Activities

The DPC engages with child policy and online safety stakeholders in Ireland and further afield. It meets regularly with representatives from technology companies, the public sector and non-profit organisations in order to present the outputs from the DPC's public consultation and to keep the public abreast of the DPC's various initiatives in the field of children's policy and promotes greater awareness of children's data protection issues and how these differ to online safety issues more generally, such as cyberbullying or harmful online content.

A representative from the DPC sits on the National Advisory Council for Online Safety (NACOS), where the DPC has proactively contributed to the Council's scrutiny of the **General Scheme Online Safety and Media Regulation Bill** - published by the Department of Communications, Climate Action and Environment (DCCAE) in October 2019. In this capacity, the DPC also contributed to the DCCAE's public consultation on the regulation of harmful online content in 2019.

Conclusion

There can be no question that the last two years of its regulatory life have been extraordinarily busy for the Data Protection Commission. The sheer volume of cases that have moved through both Assessment and Breaches in the last two years testifies to this. However, the volumes alone are not representative of the fuller picture; far more significant is the fact that the patterns within the numbers show no signs of tapering off. Insofar as past trends can be taken as a reasonable indicator of future progressions, the DPC can expect to see continued growth in these volumes. There is nothing to suggest that the numbers will level out on their own, which is a learning that must be factored into any regulatory approach for the future. The focus on numbers and volumes is important in terms of considering how best customer service, support and enforcement levels can be maintained and indeed improved.

In the reasonable expectation that its workload will continue increase, and cognizant that the Coronavirus crisis is likely to have implications for future funding, the DPC must approach the future with the twin aims of maximising its resources and increasing efficiencies in its processes. Since 2014, the DPC's funding and staffing allocations have been increasing year-on-year in anticipation of its enhanced remit under the GDPR.[12] Notwithstanding these increases, there remains a considerable disparity between the DPC's workload and its available assets. When considering the future-state of the Commission, the DPC will seek to maximise its resources, including how its staffing grades are structured, in a way that focuses on improved outcomes for the greatest number of people.

As it moves forward – and to facilitate improved outcomes for individuals while assuaging disparities of staff and funds – the DPC's regulatory approach must be influenced by those avenues which allow it to reconcile these two prerequisites. One such possible avenue is the promotion of greater data protection knowledge within the community. It is clear from the complaint and breach figures shown in this report that levels of data protections awareness are quite high – 84% according to latest **EU Fundamental Rights Agency figures**. Stakeholders know that the DPC is there and how to reach out to it when they have an issue. However, equally clear from the figures, is the fact that many of these contacts arise as a first resort, rather than necessary adjudications flowing out of efforts to exercise individual rights. Similarly with breaches and the notably high proportion – in excess of 80% - that arise in manual processing contexts the DPC should not have to intervene in these instances because sufficient oversight should be so embedded at source as to mitigate risks before they become problems. The frequency of these first-resort contacts and

[12] For details of funding and staffing figures, please refer to the DPC's **Annual Reports**.

avoidable breaches indicates that, while there are high levels of data protection awareness, there is yet some work to be done in order to build the commensurate data protection knowledge that is required to change society's approach to data protection to coalesce with its rising importance. Awareness is not equal to understanding.

As part of its efforts to redress this gap, the DPC has already commenced supportive projects directed at DPOs and the SME sector and these efforts will continue into the future. Consideration will also be given to the ways in which the DPC can engage with representative bodies and agencies acting on behalf of individual citizens; moving forward, the DPC will examine the ways in which it can bolster the aforementioned levels of understanding, so that individuals can feel confident in exercising their rights for themselves. In keeping with its Public Sector Duty – and as a matter of good regulation - the DPC will ensure the representative bodies with which it engages are drawn from all elements of the community, so that those whose rights are most at risk of infringement can be assured of fairness of access.

Education alone – while essential – will not be sufficient to reconcile the DPC's resource disparities to the extent that they are fully mitigated. Consideration will have to be given to the way in which the DPC handles complaints in the future. Efficiencies are possible, but they incur necessary adjustments. Requirements under legislation will always be honoured, but there remains leeway in how best to meet them in order to benefit the maximum amount of people. Where both finances and personnel are fixed, capacity in other areas must be found. To resolve this inherent tension in the most equitable way possible, the DPC will consult on the approaches by which it can refine the scope of an investigation to ensure that an outcome is reachable. It will also consider how best to investigate systemic issues and the extent to which the DPC can limit the scope of an investigation where its current ambit is such as to make investigatory progress untenable.

In order to move forward fairly, the DPC will take into account the views of stakeholders when identifying the balance points between its priorities. Based on the findings in this report, as well as extensive engagement with disparate interested parties over the course of the last two years, the DPC will now publish its Draft Regulatory Strategy for public consultation. The Draft is a roadmap for the next five years of the DPC's regulatory undertakings, including how it intends to resolve the constriction between its mandatory and discretionary functions.

The experience of the last two years has been such that there can be no question but that the GDPR has had a seismic impact on the way in which personal information is transacted across Europe and the wider world. It is, however, still very early in the lifespan of such a sizable piece of regulation to try to predict the point at which that impact will reach critical mass. What can be said with certainty is that the consistent primary goal will always be to protect the fundamental right to data protection that has been guaranteed to European citizens under the law. The DPC, in moving forward with its regulatory remit, is committed to upholding that right and ensuring that the principles that underpin the General Data Protection Regulation are augmented for all stakeholders within its purview.

18/06/2020

Appendices

Appendix 1: Surveillance by the State Sector for Law Enforcement Purposes

Background

In June 2018 the DPC commenced a number of own-volition inquiries under the Data Protection Act 2018 into surveillance of citizens by the state sector for law-enforcement purposes through the use of technologies such as CCTV, body-worn cameras, drones and other technologies such as automatic number-plate recognition (ANPR) enabled systems. These own-volition inquiries are being conducted under Section 110 and Section 123 of the Data Protection Act 2018 and they have been split into a number of modules. The first module focuses on the thirty-one local authorities in Ireland, and the second on An Garda Síochána. Further modules are likely to be added as the inquiries progress. The first and second modules commenced using the data protection audit power provided for in Section 136 of the Data Protection Act 2018.

Progress to date - An Garda Síochána

The first phase of the inquiry concerning An Garda Síochána (AGS) was conducted in relation to Garda-operated CCTV schemes (Section 38(3)(a) of the Garda Síochána Act, 2005 provides a legislative basis for such schemes). The inquiry involved inspections at Garda Stations in Tullamore, Henry Street Limerick, Pearse Street Dublin, Duleek and Ashbourne Co. Meath.

Decision

Having considered the final inquiry report, in August 2019 the decision maker made thirteen findings in her decision in respect of infringements of a number of law enforcement provisions in the Data Protection Act, 2018. The following is a summary of the issues of concern identified during the inquiry and the decision findings in each case:

Use of ANPR cameras

The inquiry identified that, of the fourteen cameras deployed in the Duleek and Donore Garda operated CCTV scheme in Co. Meath, seven are Automatic Number Plate Recognition (ANPR) cameras. Reports can be exported from the recording system to show a complete log of activity

by vehicle. By inputting details of either a full or partial vehicle registration number plate, the system can perform a search and return a still image of the vehicle, including the vehicle registration plate, if it was captured by an ANPR camera. This still image can then be used to pinpoint the date and time that the registration plate was captured, and the footage from the other CCTV cameras for the same time and date can then be searched to examine the movement of the vehicle concerned. Therefore, each time a vehicle passes one of these ANPR cameras – regardless of whether or not these motorists are suspected of any wrongdoing – a precise record of this activity by date and time is logged and retained for thirty-one days in accordance with the AGS Code of Practice for CCTV in Public Places. In addition, searches from the ANPR feeds produce a clear image of the vehicle's driver and front-seat passenger, if any. While this CCTV scheme was ultimately authorised by the Garda Commissioner, it was in fact presented as a *fait accompli* scheme by the 'text alert' communities of Duleek and Donore to the AGS. It was the 'text alert' community which drove and sourced the funding for its installation. Although AGS acknowledged that it is the data controller, the documents underpinning the processing operations (a CCTV policy and a Privacy Impact Assessment) were drawn up by the "Duleek and District Text Alert Community" group. Overall it was noteworthy that the Privacy Impact Assessment focused on the CCTV scheme as a whole and did not treat the matter of the deployment of ANPR cameras with any adequate degree of consideration.

As no evidence was presented of any consideration being given to the issues of design in terms of what the ANPR cameras capture and how data can subsequently be aggregated, searched, consulted and reported, AGS failed to consider the privacy impact of such surveillance using ANPR cameras.

The decision made the following three findings in relation to the use of ANPR cameras at Duleek and Donore:

- AGS infringed Section 75(3) of the Data Protection Act, 2018 as it has failed as controller to implement an appropriate data protection policy in respect of the ANPR cameras and associated activities.
- AGS infringed Section 76, as it acted passively as the controller in taking over a pre-designed system and cannot have assessed the requirement for or implemented the appropriate data protection by design and default safeguards.
- AGS was in breach of Section 84 by reason of its failure to carry out a data protection impact assessment on the ANPR surveillance system for which it is the data controller, to test the necessity of ANPR cameras and to demonstrate that the use of ANPR cameras is justified and proportionate *vis a vis* the crime levels in the area it is trying to address. In accordance with Section 84(1), this assessment should have been completed before the processing operations commenced.

Excessive access to monitoring rooms

An issue identified in relation to the Garda operated CCTV scheme approved for Pearse Street Garda Station, Dublin, the scheme in operation in Henry Street, Limerick and the scheme in

operation in Ashbourne Garda Station is that the monitoring rooms, while restricted to the public, are co-located with the command centre and radio control centre. This effectively means all Garda members in Pearse Street Station have access to the 34 live-feed CCTV screens; in Henry Street, Limerick, 600 Garda members have access to more than 50 monitoring screens, and in Ashbourne Garda Station all Garda members have access to the one screen with several CCTV views. Furthermore, in Pearse Street Garda Station, recorded footage is viewed in a separate room (the Parade Room), while in Ashbourne Garda Station, viewing occurs in the monitoring room / control centre. It was noteworthy that other schemes operate such that the monitoring room is not generally accessible to all Garda members (for example, at Tullamore Garda Station) as a matter of course.

The decision made the following finding in relation to excessive access to monitoring rooms:

- AGS was not in compliance with Section 77 and Section 75(1)(b) of the Data Protection Act, 2018 for the following reasons: there was no evidence to demonstrate to the DPC that AGS had taken account of Section 77(a) in terms of the requirement to conduct an evaluation of the risks. AGS therefore cannot have implemented Section 77(b), leading to a failure to take measures for the purpose of demonstrating its compliance with Part 5, as required by Section 75(1)(b).

Systems Access

The inquiry identified a range of issues across the Garda operated CCTV schemes where some CCTV systems appeared to have no capability to record access instances. In other cases, the inquiry identified that an electronic audit trail capability that can identify who has accessed the system and at what time by reference to individual Gardaí was in place, but there was no evidence of proactive auditing of the access logs such that improper use could be detected. In a further case, only one generic login to the access system existed with the log-on credentials posted on a whiteboard making it near impossible to identify who had accessed the system.

Maintaining records of downloads

Further issues identified related to a failure to maintain records of CCTV footage downloaded and reviewed by Garda members and there appeared to be an inconsistency across the Garda stations inspected regarding the comprehensiveness of manual records kept.

Training of staff

A further issue concerned the absence of a training programme for members attached to two Garda operated schemes on use of the Garda authorised CCTV systems including reviewing and downloading of images and footage.

Privacy by Design and Default

In the case of the Duleek and Donore scheme, specific issues around the design of the CCTV implementation were in evidence. Members operating the 'pan, tilt and zoom' cameras in this scheme appeared to routinely fail to manually return the cameras to their original focus; in some cases these were left directed at private homes in Duleek Village. Further, the inquiry found that in the village of Donore, one of the CCTV cameras picks up a clear view of the front door of the

house of the local priest, with the result that his comings and goings and those of any visitors to his house were permanently on view at Ashbourne Garda Station.

Retention

The inquiry identified inconsistency in application of the AGS Code of Practice for CCTV in Public Places as regards retention of footage in the course of their inspections. The Duleek and Donore scheme operates a 56-day retention policy rather than the 31 days set out in the Code. No justification was provided for this extended period (such as, for example, that the particular footage was required for a live investigation or prosecution). On the day of the inspection, CCTV footage that was 79 days old was identified.

Data-logging

Section 82(1) of the Data Protection Act, 2018 obliges data controllers to create and maintain a 'data log' in their automated processing systems such that, amongst other things, it can be ascertained when and if personal data was consulted by any person or whether personal data was disclosed or transferred to any other person. Section 82(4) requires the controller to make a data log available to the Data Protection Commission for inspection and examination if requested to do so. Section 82(5) deals with automated systems that predate 6 May 2016 - which appeared to be the case for the CCTV schemes inspected during this inquiry. In such circumstances, compliance with Section 82 is not required in the first instance prior to 6 May 2023 but only where the controller can demonstrate it would involve disproportionate effort to implement the section. The section intends that controllers will implement data logging in advance of the two dates set down above and that where they do not intend to implement before those dates, they must justify why in accordance with Section 82(5). No such analysis or justification was presented to this inquiry by AGS.

General

In overall terms, the inquiry yielded no evidence of AGS having considered and implemented the provisions of the Law Enforcement Directive as transposed by the Data Protection Act, 2018 in respect of the Section 38(3)(a) CCTV schemes. Specifically, the AGS Code of Practice for CCTV in Public Places has remained unchanged since 2006 and does not appear to have been reviewed. Regarding systems identified during the inquiry as lacking digital tracing of individual access, no plans to upgrade were conveyed to the inquiry. Indeed, the inquiry report disclosed no actions undertaken to account for the new legal framework for personal data with the exception of the appointment of a Data Protection Officer in 2018 and a Record of Processing Activities (ROPA) across AGS that was implemented the same year. The AGS circulars accompanying responses to the inquiry questionnaire seeking responses on foot of the audit all date back many years; nothing current and updated to take account of the Data Protection Act, 2018 was attached. Section 77(a) specifically requires competent authorities to "evaluate the risks to the rights and freedoms of individuals arising from the processing concerned", while paragraph (b) requires them to implement a range of protective measures.

The decision made the following seven findings in relation to the governance issues set out above:

- With regard to a number of issues in relation to security measures, AGS has not demonstrated that it has undertaken any of the evaluation steps required under Section

77(a) nor implemented the measures to address the issues identified under Section 77(b). Further, Section 75 requires the controller to implement technical and organisational measures to ensure compliance with Part 5 of the Act and to demonstrate that compliance.

- On the matter of compliance with Section 75 concerning general obligations with regard to technical and organisational measures and Section 77 with regard to security of automated processing:- there was no evidence that AGS, in advance of May 2018, implemented a review and update of its technical and organisational measures surrounding its use of surveillance technologies in public places; and AGS has not demonstrated that it has undertaken any of the evaluation steps required under Section 77(a) nor implemented the measures to address the issues identified under Section 77(b).

- With regard to Section 72 concerning security measures for personal data, the members of AGS operating a number of the schemes inspected had received no training on the operation of the CCTV systems and the correct handling and protection of the personal data involved. In one instance, the Garda members operating the scheme were unaware of the full range of technical features of their own CCTV system.

- On the matter of compliance with Section 76(1) with regard to data protection by design and default, AGS failed to install CCTV cameras in such a way that they do not unnecessarily infringe the privacy rights of private individuals, and further failed to install technology that defaults back to its original settings without relying on a note attached to the recording units to remind staff to manually restore the position (pan, tilt and zoom).

- With regard to Section 71(1)(e) regarding storage limitation, no justification by reference to the functions of AGS was provided for retaining personal data in a form that identifies a data subject for longer than is necessary. (Duleek and Donore CCTV scheme).

- On the matter of compliance with Section 82 concerning data logging for automated processing systems, AGS has not identified what actions it intends to take in relation to data logging, and by when, in light of section 82(5). It should evaluate this matter urgently in light of the considerable time required for development of new systems.

- Finally, on the general matters outlined above, AGS has not demonstrated that it has undertaken any of the evaluation steps required under Section 77(a), nor has it implemented measures to address the issues identified under Section 77(b).

Appropriate Signage and General Transparency

Inadequate signage was an issue identified repeatedly across the Garda operated CCTV schemes inspected during the inquiry. In relation to the Duleek and Donore scheme, the inquiry identified only one CCTV sign in the village of Duleek naming AGS. Signage naming a private contractor and with no reference to or contact details for AGS appeared in multiple locations in both Duleek and Donore villages. The private contractor CCTV signage observed was located at such a height on the poles to which it was attached that it is doubtful anyone driving by could read it. No CCTV

signage of any description was observed on the day of the inspection on the approach roads to Duleek and Donore.

At Pearse Street Garda Station, Dublin and Henry Street Garda Station, Limerick the inspection team observed CCTV signage erected adjacent to the respective Garda Stations. No purposes for the CCTV nor contact details for AGS appeared on the signs, although the AGS logo was included. Members of the public approaching the Pearse Street Dublin area from the south side of the city encounter no advance signage to alert that they are coming into a CCTV monitored area. In Limerick, the approach roads to the city and in particular the Dublin Road route into Limerick city travelled by the DPC inspectors had no signage giving advance warning that travellers are approaching a CCTV-monitored area.

Some, but not all, of the approach roads to Tullamore did have signage alerting the public that they are about to enter a CCTV monitored area. However, the signage was deficient in the same manner as that deployed adjacent to the Dublin and Limerick Garda Stations referred to above.

The inquiry noted that the various Garda Stations operating the schemes failed to provide to callers at the public counter information leaflets on AGS CCTV operation in the relevant area. While the Garda website provides extensive information in relation to mobile traffic cameras and their locations, there is no information specific to the individual CCTV schemes authorised under Section 38 of the Garda Síochána Act, 2005.

In relation to the schemes inspected, it is clear that members of the public are not adequately on notice in relation to the processing that is taking place via CCTV operated by AGS. In many instances inspected, the first layer of signage is not present or, where it is present, it is not adequate as no contact details for the controller are supplied nor purposes for processing stated. Nor is there a second layer of information available to the public, either on the garda.ie website or on leaflets in Garda stations. Were they aware, individuals may opt to use a different route or may continue and enter a CCTV-monitored area but secure in the knowledge that they can contact the relevant data controller if they wish to make inquiries or exercise any of their data protection rights.

Further, in relation to the Duleek and Donore scheme specifically where ANPR cameras are deployed, none of the signs inspected mentions that ANPR is in use. In addition, the CCTV policy for Duleek and District fails to address in any meaningful way the purposes for which ANPR has been installed. Furthermore, the CCTV policy in overall terms fails to set out details of the capability of the ANPR cameras and there is little in the policy to explain to the general public what ANPR is, how it processes personal data and why that is necessary. This deficiency is particularly noteworthy given the significance of the use of ANPR cameras from a data protection perspective and its potential impact on the rights and fundamental freedoms of data subjects.

The decision made the following finding in relation to signage and general transparency:

- AGS infringes Section 71(1)(a) and Section 90(2) of the Data Protection Act, 2018 in that information on the personal data it collects and processes via its public CCTV systems (at least as concerns the individual schemes inspected) is not adequately communicated to the public by primary signage setting out the high-level purposes of the processing and

secondary information via its website or leaflets. Nor is the identity of the data controller of the CCTV schemes clear in many instances. The effect of this infringement is to render the data unfairly collected and processed. It is noteworthy that, notwithstanding that AGS is the data controller in relation to each scheme and the purposes are identical in terms of the personal data obtained through each scheme, that there is little consistency observed in the signage inspected for the purposes of this inquiry. AGS needs to identify and procure a consistent form of signage that meets the requirements of the Data Protection Act, 2018 and that will be easily recognisable by members of the public no matter where they travel in Ireland.

Absence of written contracts between AGS and third party data processors

The inquiry identified the absence of contracts for processing between AGS as a controller and maintenance contractors on the CCTV schemes deployed. The inquiry noted that a number of Garda stations were operating without written contracts in place with third party contractors that maintain and service their CCTV systems, which service includes those contractors handling AGS-controlled personal data. In the absence of such a contract, there is no evidence as to how the processor provides the sufficient guarantees required by Section 80(1)(b) of the Data Protection Act, 2018.

The decision made the following finding in relation to the absence of written contracts between AGS and third party data processors:

- AGS infringes Section 80 by failing to put in place a written contract between itself and all third-party contractors servicing its CCTV systems under the authorised schemes, and by failing to ensure the processors in each case provide sufficient guarantees to implement appropriate organisational and technical measures.

Corrective Powers

The decision maker exercised three corrective powers in relation to An Garda Síochána as follows:

In accordance with Section 127(1)(d), AGS was ordered to **bring its processing into compliance** with the relevant provisions of the Data Protection Act, 2018. In that regard, the decision maker set out twelve actions required of AGS and timeframes for AGS to complete the actions or to report to the DPC on how it intends to implement the actions.

In accordance with Section 127(1)(b), a **reprimand** was issued to AGS in circumstances where data processing by AGS infringed a number of provisions of the Data Protection Act, 2018 as referred to in the decision. The reprimand was issued having regard to the number and extent of the infringements identified in the decision which occurred across a range of processing operations and a range of AGS locations. In particular the decision maker considered that these infringements tend to demonstrate a generalised failure by AGS as data controller to implement appropriate technical and organisational measures in order to ensure that the personal data processed by it is processed in accordance with the provisions of the Data Protection Act, 2018 (insofar as they

give effect to the Law Enforcement Directive), and to demonstrate such compliance, this obligation under Section 75 being at the core of a controller's responsibilities and obligations.

In accordance with Section 127(1)(f) a **temporary ban was imposed** on processing specifically in relation to the Garda operated CCTV scheme in Duleek and Donore, insofar as such processing involves the operation of ANPR cameras. AGS was ordered to switch off the seven ANPR cameras operating on that CCTV scheme within seven days of receipt of the decision. (AGS complied with this requirement). The temporary ban will remain in place and the ANPR cameras will not be reactivated without the approval of the DPC. Such approval will only be given after AGS has carried out the actions required to bring the processing on this CCTV scheme into compliance. This includes the carrying out of a comprehensive data protection impact assessment and the implementation of a new CCTV data protection policy, both of which must be approved by the DPC.

Implementation of Actions

In May 2020 AGS provided the DPC with details of the measures it has put in place to implement the actions outlined in the decision. In that regard, the DPC noted that progress has been made on a number of fronts. Most importantly, the DPC noted that AGS remain fully committed to comprehensively addressing all of the findings across all of the Garda CCTV schemes authorised under Section 38(3)(a) of the Garda Síochána Act, 2005 as well as taking the findings fully into account when planning the design and roll-out of future such schemes.

In particular, the DPC welcomes the CCTV review that has been carried out to examine all Garda Commissioner CCTV authorisations and the policies, procedures and guidelines that apply to such authorisations. The establishment of a CCTV Implementation Working Group is another welcome development as its key task will be to ensure full implementation of all of the actions required by the DPC decision.

Conclusion in relation to AGS Inquiry

This inquiry in relation to data protection compliance on Garda operated CCTV schemes (Section 38(3)(a) schemes) was long overdue given that the primary legislation was enacted in 2005 and the statutory instrument was signed in 2006. The enactment of the Data Protection Act, 2018 which, among other things, transposed the Law Enforcement Directive into Irish law presented the DPC with a significant opportunity to carry out a statutory inquiry in relation to the operation of such schemes. Our inquiry commenced in early August 2018 - some eleven weeks after the new Act came into force. The inquiry process involved a questionnaire phase, an inspection phase at five Garda stations, and an inquiry report phase. Following the submission of the final inquiry report to the decision maker, the decision-making phase commenced. This culminated with the issuing of the final decision to AGS in August 2019 – one year after the inquiry process commenced.

From the DPC perspective, this inquiry has already yielded positive results and it will continue to do so as AGS continues to implement all of the actions required by the decision. The cooperation of An Garda Síochána with the inquiry and decision-making processes must be acknowledged. In

particular the positive role played by the Data Protection Officer at AGS, his team in the Data Protection Unit, and the assistance given to our inquiry team by Garda members at the Garda stations inspected, all contributed in a significant way to the delivery of the outcomes we achieved in this whole process. Furthermore, AGS is to be commended for the manner in which it has accepted in full the findings of the DPC decision and embarked on an implementation process. This reflects well on its attitude to the DPC's mandate and competence and we look forward to a continuation of this positive approach to all of the DPC's work, and in particular to its engagement with us on further phases of this inquiry which will be rolled on in the near future.

Progress to date - Local Authorities

Since September 2018 the DPC has conducted inspections in the following local authorities: Kildare County Council, Limerick City and County Council, Galway County Council, Sligo County Council, Waterford City and County Council, Kerry County Council and South Dublin County Council. Between them, these seven local authorities have more than 1,500 CCTV cameras in operation for surveillance purposes. (*The inquiries do not apply to security cameras such as those deployed for normal security purposes).*

The inquiries in the local authority sector also involve auditing the deployment of community-based CCTV systems authorised under Section 38(3)(c) of the Garda Síochána Act. These schemes require that the local authority be a data controller and that prior authorisation of the Garda Commissioner be obtained. The inquiries are examining, among other things, how data controller obligations are being met by the local authorities as required under that Act.

At the time of writing, DPC has completed its inquiries in respect of six of the aforementioned local authorities and a draft inquiry report for the seventh local authority has been finalised in recent days.

As the inquiries continue to progress, the scale of the significant workload involved for our inquiry team in carrying out thorough probing and fact-finding has become clear. Having completed the inspection phase at seven local authorities, it is clear that no two local authorities are the same in relation to data protection issues arising out of the use of surveillance technologies. While some issues of concern are common to several local authorities, new issues of concern have arisen in every local authority inspected. Also notable from our perspective is a vast difference in the professional qualities and competence levels of data protection officers across the sector. Clearly the inquiry process can progress with greater efficiency when we are working with a data protection officer that has a full grasp of their brief and a deep awareness of the data processing that their local authority is engaged in. Much preparation is done in advance of the arrival of our inquiry team by some, but not all, data protection officers. This shows, very clearly, when our inquiry team arrives on the first inspection day. Where our experience of working with the data protection officer is positive from the beginning because of their preparations and their command of their brief, we find that this positivity continues throughout the remainder of the inquiry process.

It is worth emphasising that these inquiries in the local authority sector are specifically focussed on the use of surveillance technologies and they do not extend to other areas of work in local authorities where personal data is processed such as in planning, human resources, libraries, arts, etc. Despite the single focus of this inquiry on the use of surveillance technologies, the number and variety of issues of concern that have come to our attention is far in excess of what we anticipated when we began this work two years ago. Our completed inquiry reports, which are considered by the Commissioner in the decision-making stage of the process, highlight significant data protection compliance issues in relation to matters such as the use of covert CCTV cameras, CCTV cameras at bottle-banks, the use of body-worn cameras, dash-cams, drones and ANPR cameras, CCTV cameras at amenity walkways or cycle-tracks, the lack of policies and data protection impact assessments, as well as several other issues. These include significant concerns about how some local authorities are discharging their data protection obligations as a data controller for the purposes of the community-based CCTV schemes in their areas that have been authorised by the Garda Commissioner under Section 38(3)(c) of the Garda Síochána Act, 2005.

However, we do recognise the significant challenges that the GDPR and the Data Protection Act, 2018 present to the local authority sector. One of those challenges at the very outset is to identify under which regime the data processing using surveillance technologies takes place – the GDPR or the Law Enforcement Directive provisions of the Data Protection Act, 2018. This challenge is pronounced by the fact that the work of local authorities may involve significant law enforcement activity as well as tasks involving more general elements of personal data processing. From our work to date on these inquiries, we are encouraged by the eagerness shown by some local authorities to assist our efforts to dig deep for the purpose of identifying all the issues of concern with regard to the use of surveillance technologies. Some have taken immediate steps during our inquiries towards remedial action – a response that is indeed welcome and which demonstrates a fruitful engagement with, and positive attitude towards, our work.

Kerry County Council decision

The inquiry conducted at Kerry County Council was an example where the local authority engaged in a very positive manner with the Inquiry Team and facilitated the Inquiry Team in all aspects of its work. This is the first of the local authority inquiries to conclude. In this case, the decision maker has issued a final decision.

Kerry County Council has lodged an appeal of this DPC decision at the Circuit Court under Section 150 of the Data Protection Act, 2018. The setting of a hearing date for this appeal is currently pending.

Data Protection Commission,
21 Fitzwilliam Square,
Dublin 2.

www.dataprotection.ie
Email: info@dataprotection.ie
Tel: 076 110 4800

An Coimisiún um Chosaint Sonraí
Data Protection Commission