Annual Report

CASE STUDIES 2024

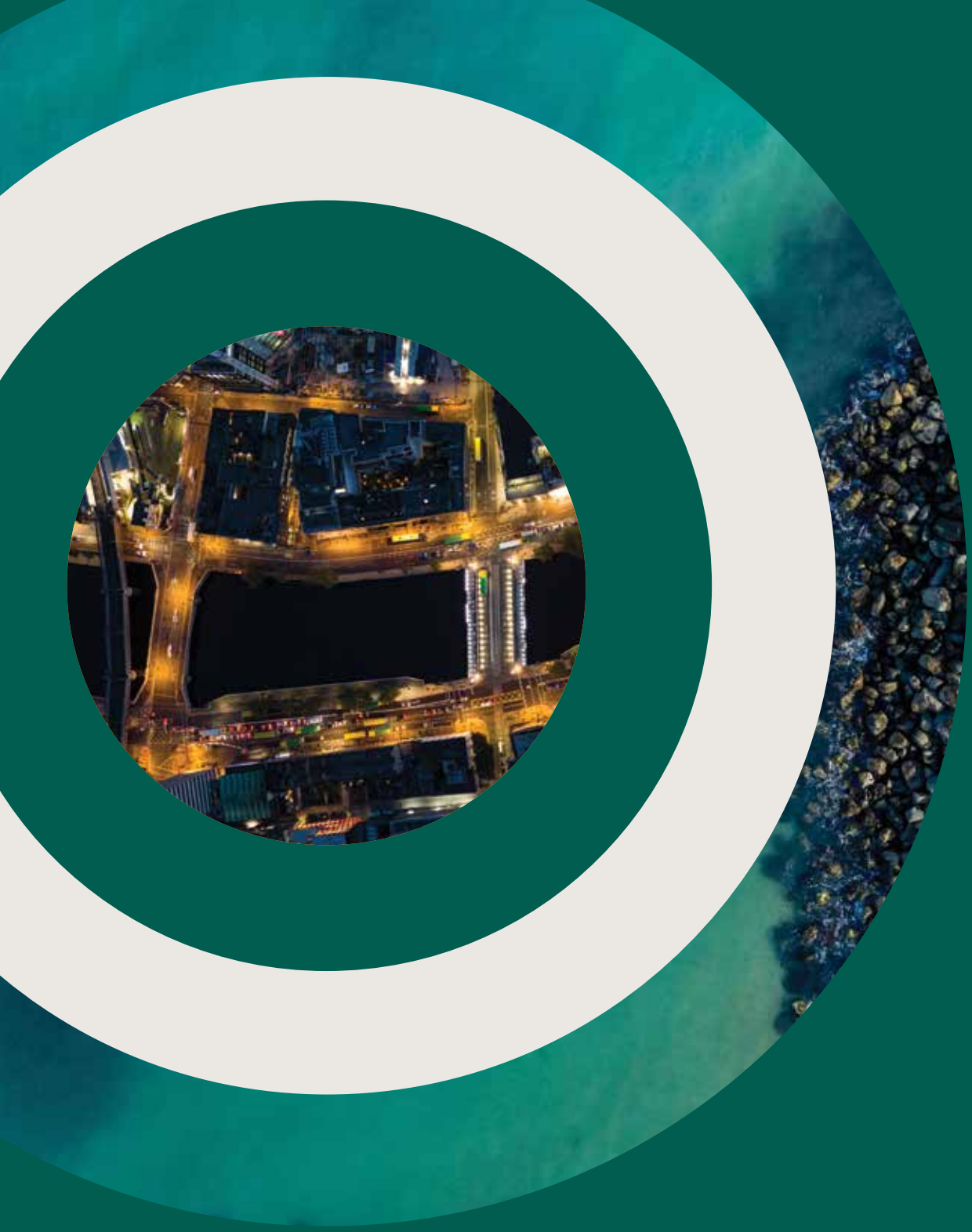
Coimisiún Cosanta Sonraí
Data Protection Commission

Introduction

The mission of the Data Protection Commission (DPC) is to champion the consistent application of data protection law through engagement, supervision and enforcement, and driving compliance through data protection legislation. The DPC recognises that a key pillar to success in this mission is to support organisations and drive compliance. In order to achieve this outcome, the DPC is committed to publishing case studies illustrating how data protection law is applied, how non-compliance is identified and how corrective measures are imposed.

This document sets out the case studies covered throughout 2024 and displays the DPC's continuous effort to pioneer the appropriate applications of data protection law.

L-R Commissioner Dr. Des Hogan and Commissioner Dale Sunderland



Contents

Access Requests	**8**
Failure to respond to an Access Request	9
Seeking access to deceased siblings medical records	9
Refusal of Access Request of a non-customer	10
Withholding of records containing personal data	11
Incomplete organisational search in response to an Access Request	12
Access request redactions	13
Requesting Data relating to a Vehicle	14
Data Controller vs Data Processor obligations	15
General Data Protection Case Studies	**16**
Use of Personal Email in Work	17
Direct Marketing	18
Parent making an erasure request for child who is now an adult	19
Rectification of personal data	20
Prosecution Case Studies	**21**
Prosecution of Pulse Gym trading as (Energie Fitness Dublin 8)	22
Prosecution of Supermac's Ireland Limited	23
Prosecution of Google Ireland Limited	24
Prosecution of Thérapie Clinic Trading as Valterous Limited	25
Breach Case Studies	**26**
Phishing Email Attack in the Broadcasting Sector	27
Digital File Storage Breach	28
Personal Data Accidentally Disclosed Online	29

Contents

CCTV **30**

Domestic CCTV 31

Failure to respond to a request for CCTV footage 32

Use of CCTV to monitor waiting area without adequate transparency measures 33

Data Processing **34**

Sharing personal data with third parties without consent 35

Disclosure of an employee's special category data by their employer to a third party services provider, without the employee's consent 36

Excessive sharing of special category data to a third party in order to seek guidance on behalf of an employee 38

Processing employee's personal data from their private email account/emails for disciplinary purposes 40

Processing occupational health data 42

Law Enforcement Directive (LED) **43**

Law Enforcement Directive (LED) Access Request - Rights and Restrictions 44

Right to be Forgotten (RtbF) **45**

Right to be Forgotten (RtbF) search engine results for an individual's first and last name 46

Cross-Border **47**

Cross-Border Complaint Concerning an Access Request to a Large Social Media Platform 48

Cross-Border Complaint Concerning a Delisting Request 49

Access Requests

Article 15 of the GDPR provides individuals with the right to request access to their personal information. An organisation in receipt of such a request should provide the information to the individual in a timely, sufficient and transparent manner.

Failure to respond to an Access Request

The DPC received a complaint with regard to an individual who made an access request under Article 15 of the GDPR to a public/state hospital for a copy of all personal information held concerning them. The response from the hospital remained outstanding after more than a month, whereas information provided to the DPC indicated that due the health of the individual this matter required urgent attention.

The DPC contacted the Data Protection Officer for the Hospital Group by phone and email to inform them of the urgency of the complaint, and requested they respond to the individual's representatives promptly, providing them with a copy of the individual's personal information as part of the engagement. The hospital followed the instructions from the DPC.

Whilst the hospital acknowledged receipt of the request within one month of its receipt, the personal data the individual was entitled to was only provided to the individual following the intervention of the DPC.

KEY TAKEAWAYS:

Organisations are required to implement appropriate organisational measures in place to ensure that they are in a position to respond to any rights requests within the stipulated timeframes under the GDPR. Organisations should not await the intervention of the Regulator to respond promptly to subject access requests.

Seeking access to deceased siblings medical records

An individual contacted the DPC inquiring about how to access the medical records of their late sibling, who had tragically passed away as an infant many years previously. Since both parents had also passed away several years ago, the individual was unable to obtain information about the circumstances surrounding the death of their sibling.

The DPC recognises the sensitive nature of such queries and always responds with empathy and respect. In this instance, the individual was informed that, as per Article 4(1) of the GDPR, personal data is defined as "*any information relating to an identified or identifiable natural person (data subject).*" However, as also outlined in Recital 27 of the GDPR, the law does not apply to the personal data of deceased persons. Notwithstanding the sensitive nature of the query raised, the DPC advised that while the organisation may choose to release the data they were seeking, unfortunately as outlined above, the DPC could not compel them to do so as there was no obligation on the organisation to do so under the GDPR. As a result, the DPC advised that data protection law could not be engaged in relation the issue in question, meaning the concerns raised were beyond the DPC's remit. Unfortunately, this meant the Office could not assist the individual further in this matter.

KEY TAKEAWAYS:

Notwithstanding the sensitivity of cases such as this one, it is the obligation of the DPC to inform those raising a query with it that data protection legislation only covers a "natural person" and that data protection law does not grant access to personal data relating to deceased individuals. The DPC is conscious of the upset surrounding matters relating to deceased relatives and will always strive to communicate the facts as they relate to data protection in as empathetic a manner as possible when responding to queries of this nature.

Refusal of Access Request of a non-customer

The DPC received a complaint from an individual in relation to an access request made to an internet service provider. According to the individual, they rang the company regarding the possibility of switching broadband services and considered that the level of service received from the customer service agent was unsatisfactory. As a result, they made an access request for a copy of their personal data processed by the company.

In response to the individual's access request, the company sought further information from the individual including an account number. The individual informed the company they could not supply an account number, as they were not a customer, merely a potential customer enquiring about switching their broadband service. In their response, the company advised the individual that without an account number they could not process the access request. On foot of this response, the individual proceeded to make a complaint to the DPC. Following receipt of this complaint, the DPC corresponded with the internet service provider to ascertain why the access request could not be processed without an account number, and to comply with the individual's access request.

The company promptly responded to the DPC accepting that the agent who responded to the individual should not have informed them that they could not process the access request. They also outlined that the agent involved did not follow the correct process for dealing with access requests from non-customers, and advised that additional data protection training would be provided to the agent. The company also provided the individual with a copy of their personal data. The individual confirmed that while they did receive a copy of their personal data, the matter was only resolved following the DPC's intervention.

KEY TAKEAWAYS:

Under Article 15(3) of the GDPR, there is an obligation for an organisation to provide a copy of the personal data, whether the individual is a customer of the organisation or not. This particular case highlights the importance of data protection training including refresher training for all employees in customer facing roles to ensure that an individual's right to access to their personal data is upheld in all instances and that appropriate and accurate information is provided to the public by organisations.

Withholding of records containing personal data

The DPC received a complaint from an individual regarding the withholding of records containing personal data in response to an access request. The individual had made an access request under Article 15 of the GDPR to a financial service provider, following the sale of the individual's mortgage to the organisation.

The organisation advised that personal data was being withheld from the customer in line with Section 60(3)(b) of the Data Protection Act 2018 (DPA 2018). The organisation stated that "*securitisation documents did not constitute [the complainant's] personal data*".

The DPC informed the organisation as to the definition of personal data under Article 4(1) of the GDPR and that if any of the stated documents being withheld contained the individual's personal data, clarification would be required as to the reliance on the restrictions applied. The DPC received a response from the organisation confirming that no personal data existed in the securitisation documents with additional reference to a *"final response letter"* that it issued to the individual. Subsequently, the DPC requested a copy of this "*final response letter"* and requested a list of alleged outstanding personal data or any further information as to the location of records containing personal data from the individual. The DPC also requested the organisation to outline specifically each record containing personal data being withheld and the legislative basis for doing so.

The organisation initially advised it was relying on sections 60(3) and 60(7) of the DPA 2018 for not releasing the documents. The DPC further probed the restrictions being applied by the organisation. On foot of this engagement, the organisation confirmed to the DPC that it would no longer be relying on any part of Section 60 of the DPA 2018 to withhold the individual's personal data. In light of the DPC's intervention, the organisation furnished the individual with their personal data, which had previously been restricted.

Following this release of documents, the individual specified the existence of additional personal data and requested copies of mortgage statements from a specific year. The DPC queried this with the organisation, which then released this further personal data to the individual. The DPC determined that the organisation had failed to respond to the access request within the specified timeline under Article 12(3) of the GDPR.

KEY TAKEAWAYS:

Organisations are required to implement appropriate organisational measures to ensure that they are in a position to respond to any rights requests within the stipulated timeframes under the GDPR. When seeking to rely on the application of a restriction to withhold access to personal data, organisation must undertake a thorough examination on the validity of such restrictions to ensure personal data is not wrongly withheld.

Incomplete organisational search in response to an Access Request

The DPC received a complaint from an individual who had submitted an access request under Article 15 of the GDPR to a property management company. The individual was seeking access to any personal data processed by the organisation in relation to them. The organisation responded to the access request explicitly stating to the individual that it did not process any personal data in relation to the individual at the time the access request was made or any time before that.

During the assessment stage, the DPC raised queries with the individual regarding their relationship with the organisation in order to establish if they were *"data processor"* or "*a data controller"* in this instance. Upon a review of the individual's response and the supporting documentation they provided, the DPC established that the property management company was the appropriate "data controller" in relation to this complaint.

The DPC requested the organisation to provide further details in relation to the searches it carried out to identify any personal data belonging to the individual. In its initial response, the organisation advised that it had conducted a search of its 'system' and that the only personal data that could be identified was the initial request made by the individual. The DPC queried the searches completed and requested documentary evidence of the efforts made to locate the individual's personal data including those conducted in other sections of the organisation.

The organisation responded with a comprehensive outline of the searches undertaken and provided the relevant supporting documentation. The DPC reviewed this correspondence and it subsequently identified three records containing the individual's personal data (two (2) invoices & one (1) data entry on a software system) which had not been provided to the individual.

Following further engagement between the DPC and the organisation, the three outstanding documents containing the individual's personal data were provided to the individual.

KEY TAKEAWAYS:

Organisations are required to ensure that appropriate organisational measures are in place to ensure they are in a position to respond to any rights requests within the stipulated timeframes under the GDPR and to be able demonstrate to the DPC that adequate searches have taken place to locate any records containing personal data that may be processed.

Access request redactions

The DPC received a complaint from an individual who had submitted an access request under Article 15 of the GDPR to their former employer (a public health organisation), who provided services in Home Support.

The organisation provided a response to the access request within the statutory period of one month of the date of the receipt of the request. In that response, the organisation had informed the individual that whilst it had endeavoured to comply with the access request, in so far as possible, there were some potential redactions under Article 15(4) of the GDPR that it would be seeking to rely on. The organisation provided the individual with some personal data which contained redactions.

Article 15(4) provides that the right to obtain a copy of personal data undergoing processing should not adversely affect the rights and freedoms of others.

The individual submitted a complaint to the DPC in relation to their concern regarding the organisation's reliance on Article 15(4) of the GDPR. The individual also indicated their concern that the organisation had not released all the personal data.

The DPC advised the organisation that a balancing of rights exercise needed to be conducted by them to balance the right of access of the individual to their personal data against the identified risk to the third party that may be brought about by the disclosure of the information prior to seeking to rely on said exemption. Under the GDPR, organisations should endeavour to comply with the request insofar as possible whilst also ensuring adequate protection for the rights and freedoms of others.

The DPC engaged with the organisation and requested it to release the personal data records to the individual that it had re-examined. The DPC also requested the organisation to confirm to the individual that it was not withholding any other documents containing personal data relating to them.

The organisation, subsequently provided the DPC with a copy of its correspondence addressed to the individual confirming it had now released the personal data records in partially redacted format, which it had initially withheld. The organisation also confirmed to the individual that it held no further records relating to them. The individual was satisfied that all matters had been sufficiently resolved.

Following the intervention of the DPC, the organisation confirmed to the DPC that it had re-examined the records that it had initially released in fully redacted format, and following the review had released parts of the records, redacting data that was third party data.

KEY TAKEAWAYS:

- Where an organisation has concerns about the impact of complying with an access request, its response should not simply be a refusal to provide the information to the individual, but to endeavour to comply with the access request insofar as possible whilst ensuring adequate protection for the rights and freedoms of others.
- An organisation can meet its obligations under the data protection legislation by releasing documents in redacted format, as per Article 15(4) of the GDPR. Therefore, it may be the case, that an individual would receive redacted material in response to an access request.

Requesting Data relating to a Vehicle

An individual raised a query with the DPC about gaining access to information held by a garage detailing the history of the vehicle the individual now owned, including details of damages assessed, recommended repairs, and an engineer's report conducted towards the end of a particular year. The individual submitted an access request under Article 15 of the GDPR to the garage for all data related to the vehicle. The garage refused the request. As they were dissatisfied with the response received from the garage, they contacted the DPC to raise their concerns.

In response, the DPC reviewed the request and provided relevant information, advising that under GDPR, "personal data" is defined in Article 4(1) as any information relating to an identified or identifiable natural person. While a vehicle's registration plate could be considered personal data, the condition of the vehicle itself prior to a person's ownership did not relate to the individual as a natural person. Consequently, the DPC considered that data protection law did not apply in this case, and the concerns raised fell outside its remit.

KEY TAKEAWAYS:

It is important to note that while the scope of the definition of personal data as defined by the GDPR is broad, it does have limits. In this instance, the condition of a vehicle before an individual's ownership would not necessarily be considered personal data, as it would not relate to a specific natural person, in particular not a new owner. Therefore, as a result, the individual's request in this particular case fell outside the scope of data protection law.

Data Controller vs Data Processor obligations

An individual made an access request under Article 15 of the GDPR to an organisation they believed to be processing their personal data. Upon receipt of this request, the organisation notified the individual that it was not the data controller in this instance. The organisation advised the individual that it had referred the request to the actual data controller in line with its obligations under Article 28(3)(e) of the GDPR to assist *"...the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights"*. With the individual was not satisfied with the response and submitted a complaint to the DPC.

The DPC requested documentary evidence from the organisation (data processor) which would support its assertion that it was not the data controller in this instance. The organisation provided the DPC with a copy of a data protection agreement, which explicitly detailed the organisation as the data processor and the other party as the data controller in relation to the personal data being processed in this instance. This agreement outlined in specific detail that the organisation only processed personal data upon instruction from the data controller. The DPC examined this agreement and affirmed that the organisation to which the individual submitted the access request was the data processor in this instance.

The DPC accepted that the organisation was the data processor for the personal data which had been requested in this instance and that it had complied with its obligations under both Article 15 and Article 28(3)(e) of the GDPR.

KEY TAKEAWAYS:

- Sometimes, an organisation will need to engage the services of a sub-contractor or agent to process personal data on its behalf. Such an agent is termed a "data processor" under data protection law. Where a data controller engages the services of a data processor, it must take certain steps to ensure that data protection standards are maintained in line with Article 28(3) of the GDPR. While organisations may outsource its processing of personal data activities to a third party, it cannot outsource its responsibility and obligations under the GDPR.
- Prior to the commencement of processing activities, data controllers and data processors must enter into a written legally binding agreement in order to define their respective roles and responsibilities in the context of their business activities. Such agreement is usually in the form of a contract and the obligations of the data processor should be as detailed as possible.

General Data Protection Case Studies

Use of Personal Email in Work

An organisation in the voluntary sector became aware during an internal audit review that during their employment, an ex-employee had forwarded emails, and attachments, from their work account to their private email account. The emails contained personal data, including the special category health data under Article 9 of the GDPR of a number of vulnerable individuals.

The DPC engaged with the organisation to establish the root cause of this breach and to ascertain what measures the organisation had in place in order to protect the rights and freedoms of the affected data subjects. The organisation carried out an investigation and received assurances from the ex-employee that the personal data had been deleted and was never shared with any third parties, and that they had used their personal email address for convenience in certain circumstances.

The organisation's Data Protection Officer (DPO) also engaged with the organisation's Head of IT to examine if technical measures could be implemented to reduce the risk of this issue reoccurring. All affected data subjects were notified and were advised that the DPO was available to assist them should they have any queries.

Following engagement with the DPC, the organisation implemented a number of solutions, both technical and organisational, to prevent this issue from occurring again. The organisation also launched an awareness campaign to remind all staff, volunteers and the Board of Directors of their responsibilities to keep personal data safe and private; and to ensure compliance with the organisation's Data Protection Policy.

KEY TAKEAWAYS:

- Organisations should have a Data Protection Policy in place to cover all personal data processing carried out by employees or volunteers in the course of their duties. It is important that employees are familiar with this policy.
- Organisations should also have procedures in place for removing access to physical and electronic data when an employee leaves service, to ensure that personal data remains secure.
- Strict rules should be in place prohibiting employees from sending work related correspondence to their personal email under any circumstances

Direct Marketing

An individual raised a query with the DPC concerning the marketing communication practices of an airline following a recent trip with that airline. The issue arose when the individual received an email requesting feedback on their recent trip, which they perceived to be a marketing email. The individual contacted the DPC advising that they could not find an unsubscribe option in this communication.

In an effort to resolve the issue, the individual had to navigate to airline's website to find the option to unsubscribe, a process they documented with an attached screenshot. Additionally, the individual expressed uncertainty about having signed up for this communication, as they noted being careful to avoid consent for unwanted marketing. The individual sought clarification on whether organisations are required to include an unsubscribe link in emails or surveys that are not directly related to a specific service, such as a flight.

In response to the individual, the DPC highlighted that, under Regulation 13 of the ePrivacy Regulations (S.I. 336/2011), as a general rule electronic direct marketing requires the affirmative consent of the recipient. Direct marketing can also be defined as communications aimed at promoting a product or service or encouraging additional enquiries from the recipient. The DPC further clarified that correspondence sent solely for informational or feedback purposes does not constitute direct marketing. However, if such communications included marketing content, they could be classified as direct marketing, thus necessitating the inclusion of an unsubscribe option.

In this particular scenario, having reviewed the communication message, the DPC noted that it did not include marketing content and that the organisation was only seeking feedback in order to improve the service offered. As such, the DPC determined that this communication did not constitute direct marketing or an infringement of data protection rights.

KEY TAKEAWAYS:

This case highlights the importance of clear communication practices and the need for organisations to comply with the requirements of the E-Privacy Regulations regarding consent and unsubscribe options when communicating with customers. The individual's experience serves as a reminder for companies to ensure transparency and accessibility in all their communications.

Parent making an erasure request for child who is now an adult

A charity contacted the DPC seeking advice on a query they had received from a parent asking whether they could request the erasure of their child's personal data. The data in question dated back several years when the child was a minor. However, the child was now an adult, and the parent, who was their guardian at the time, wanted to know if they could still request that the data be erased.

The DPC advised the charity that, under section 29 of the Data Protection Act 2018, a child is defined as an individual under the age of 18. This meant that, as the individual was now over 18, they were considered an adult and, therefore, had the full legal capacity to exercise their own data protection rights, including the right to request erasure of their personal data.

The DPC also clarified that while the parent could no longer directly request the erasure of the data on behalf of the now-adult child, the affected individual could choose to provide their parent with a signed letter of authority. This was an option that could be drawn to the attention of the now-adult child and their parent. Such a letter of authority would allow the parent to act on their behalf in making the data erasure request. The DPC reminded the charity that it was their responsibility to verify and ensure that any such request was valid under the circumstances.

The charity thanked the DPC for their response and confirmed that they would share the information with the individual who had initially contacted them. This guidance helped to ensure that both the individual's rights and the role of the charity were clearly understood, while also acknowledging the potential complexities involved in handling requests from parents of adult children.

KEY TAKEAWAYS:

This interaction highlighted the role of the DPC in dealing with concise queries relating to who can access personal data and the responsibility and appropriateness of the individual to exercise their own rights under the GDPR. Once an individual attains 18 years, they have full control over their own data protection rights, including the ability to request erasure of their personal data. Parents or guardians may act for them with their authority by providing a letter of authority, something that should be communicated to both the now-adult child and their parent/ guardian. It is for the organisation in question to ultimately verify and ensure that any such request is valid under the circumstances, to ensure that no unlawful disclosure of personal data takes place.

Rectification of personal data

An individual flew with an airline to a destination in Europe. When undertaking their return flight, the individual encountered a situation when their luggage was misplaced. After reporting the issue at the airport, they received a missing luggage slip that contained the name of a different individual but correctly listed the details of their missing luggage.

The individual promptly raised their concerns with the airline, seeking a resolution to ensure their luggage was properly tracked and identified. However, despite the customer's efforts, the airline was unable to provide a satisfactory resolution, and refused to issue a new ticket reflecting their correct name on the luggage slip. This lack of resolution prompted the individual to escalate the matter further by filing a complaint with the DPC.

In response, the DPC liaised with the airline's DPO to address the issue of the recording of incorrect personal data. The DPC emphasised the importance of accurate data handling and the implications of data errors on customer experiences. Through this intervention, the DPO worked swiftly to rectify the situation, ensuring that the individual received an updated luggage slip that included their correct name.

This updated slip was crucial for this individual as it allowed them to file a claim with their insurance provider for the lost luggage. The case highlights the importance of effective data management practices and serves as a reminder for organisations to prioritise accurate record-keeping and responsive customer service, especially in situations involving personal belongings.

KEY TAKEAWAYS:

This case highlights how personal data inaccuracies can lead to significant customer dissatisfaction, which can in turn lead to a complaint to the DPC. It also emphasises the role of data protection authorities in assisting with a resolution in a swift manner, and the interplay that often occurs between customer service issues generating data protection complaints to the DPC.

Prosecution Case Studies

Prosecution of Pulse Gym trading as (Energie Fitness Dublin 8)

In October 2023, the DPC received notification from an individual regarding unsolicited marketing SMS messages received from Pulse Gym, trading as Energie Fitness Dublin 8. An investigation was launched during which Pulse Gym explained that when a member signed up online, they agreed to Pulse Gym's terms and conditions, which included a reference to giving consent to receive marketing materials by electronic means.

The DPC requested a copy of the consent referred to under Article 7 of the GDPR, but Pulse Gym was unable to provide such a copy. The DPC highlighted that consent for marketing is required to be "freely given, specific, informed and unambiguous", and that Pulse Gym was not permitted to "bundle" consent for processing of individuals' personal data for different purposes.

Pulse Gym also confirmed during the investigation that the opt-out attempts made by the individual had been unsuccessfully implemented as there was a fault in the service provider's software.

A warning had previously been issued to Pulse Gym following an investigation of a similar complaint in July 2023. As part of this warning, the DPC had made Pulse Gym aware of their requirements to ensure that their mailing list only contained details of individuals who had explicitly consented to receive marketing communications and to ensure their opt-out function was operational and opt-out requests were respected. However, upon receipt of this further complaint in October 2023, it became apparent that not all changes identified in the DPC's warning letter had been implemented. As a result, the DPC decided to move to prosecution proceedings in this instance.

Pulse Gym pleaded guilty to one charge of sending unsolicited marketing SMS messages at Dublin Metropolitan District Court on 27th May 2024 under Regulation 13 of S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011. In lieu of a conviction and fine, Judge Halpin applied the Probation Act and the company was instructed to make a donation of €700 to the Little Flower Penny Dinners charity and to pay the DPC's legal costs in full.

KEY TAKEAWAYS:

This case demonstrates the importance of ensuring that when consent is sought for marketing purposes, that this consent be individualised, clearly distinguishable and not "bundled" in with other requests for consent to data processing activities. Organisations must also ensure that their opt-out procedures work properly and are tested regularly to ensure their functionality.

Prosecution of Supermac's Ireland Limited

In August 2023, the DPC received a complaint from an individual regarding alleged unsolicited marketing SMS messages received from Supermac's Ireland Limited. The DPC launched an investigation, in the course of which Supermac's Ireland Limited explained that the individual had registered for their online ordering system in 2018 and had ticked the box to receive SMS and email marketing communications. The individual subsequently placed an online order in 2023 and was added to an active marketing list for SMS purposes.

The DPC requested that the individual's details be removed from the active marketing list in August 2023. Supermac's Ireland Limited confirmed to the DPC that the opt-out had been successful and the individual had been removed from their marketing list. However, the individual contacted the DPC again in October 2023 to inform the DPC that they had received a further marketing SMS from Supermac's Ireland Limited, despite assurances that they had been removed from marketing lists. Upon further investigation, Supermac's Ireland informed the DPC that, due to a technical error by their subcontractor, the individual's phone number had not been removed properly.

The DPC's investigation of this complaint established that Supermac's Ireland Limited did not have valid consent to send electronic marketing communications to the individual concerned. As the DPC had issued a warning to the company in February 2023 with regards to a previous complaint, the DPC decided to prosecute the case.

On 3 September 2024 before Judge Fahy in Galway District Court, Supermac's Ireland Limited pleaded guilty to five charges of sending unsolicited marketing SMS messages under Regulation 13(7) and Regulation 13(13)(a)(i) of S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011. Galway District Court ordered the company to make a contribution of €3,500 to the Galway Simon Community and Cope Galway, in lieu of a conviction and fine. The company was also required to discharge the DPC's legal costs.

KEY TAKEAWAYS:

This case highlights the importance of maintaining marketing lists in accordance with customer preferences. The data controller is ultimately responsible for the personal data they process, even when utilising third-party processors, such as a sub-contractor in this case. Organisations must implement effective systems to manage opt-out requests and prevent the continued sending of unsolicited electronic communications.

Prosecution of Google Ireland Limited

In November 2023, the DPC received notification from an individual of alleged unsolicited marketing communications via telephone from Google Ireland Limited. The individual in question had received three separate phone calls in the space of a 4-hour period from individuals identified as sales representatives on behalf of Google Ireland Limited. The DPC launched an investigation, during the course of which Google Ireland Limited confirmed that a third-party contractor had disregarded the individual's previous request to opt-out of marketing communications, resulting in a number of calls being made to the individual.

The DPC had previously issued a warning to Google Ireland Limited in July 2023 concerning unsolicited phone calls made without consent to the same individual. As part of this warning, Google Ireland Limited was notified that if the individual was to receive further phone calls, Google Ireland Limited may face prosecution.

Google Ireland Limited breached the rules governing unsolicited marketing phone calls, as the company continued to make marketing phone calls after the individual had explicitly withdrawn their consent.

At Dublin Metropolitan District Court on 25 October 2024, Google Ireland Limited pleaded guilty to two charges of making unsolicited marketing telephone calls under Regulation 13 of S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011. Dublin Metropolitan District Court directed the company to contribute €1,500 to the Little Flower Penny Dinners charity and to pay the DPC's legal costs in lieu of a conviction and fine.

KEY TAKEAWAYS:

This case highlights the importance of effectively managing opt-out requests. Explicit consent is required in order to conduct electronic direct marketing activities, including marketing telephone calls. Where a contractor acting on behalf of a company fails to comply with corporate policies and procedures (e.g. cold-calling a person who has unsubscribed and opted out of such communications), it is the data controller who is ultimately responsible.

Prosecution of Thérapie Clinic Trading as Valterous Limited

In February 2024, the DPC received notification from an individual of an alleged unsolicited email communication from Thérapie Clinic. The individual had provided the DPC with a copy of their marketing preferences and a copy of an unsolicited email communication.

Subsequent to further investigation, Thérapie Clinic confirmed to the DPC that the complainant was a client of theirs and had not given consent to receive marketing communications. Thérapie Clinic conducted an internal investigation, which found that the email message, which was the subject of the complaint, had been sent manually by a member of staff in one of their clinics.

The email was not a system-generated message, and therefore no opt-out mechanism had been included in the communication. As such, the individual had received an unsolicited marketing email message without an option to opt-out of receiving further marketing messages. As the DPC had issued a warning in February 2023 to Thérapie Clinic in regards to a previous complaint, the DPC decided to prosecute arising from this complaint case.

On 25 October 2024, Thérapie Clinic was prosecuted for sending unsolicited emails to a customer who had previously opted out of receiving marketing communications. The company was found to have violated Regulation 13(12)(c) and Regulation 13(13)(a)(i) of S.I. No. 336/2011 - European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011. In lieu of a conviction and fine, the Dublin Metropolitan District Court ordered the company to make a donation of €325 to the Little Flower Penny Dinners charity and to pay the DPC's legal costs.

KEY TAKEAWAYS:

This case emphasises the need for organisations to establish effective communication of its policies and procedures to all of its staff members. Companies must ensure that staff members are fully aware of the implication of conducting ad hoc marketing activities outside of the company's marketing applications and systems. Individuals' preferences must be respected, and once an individual has opted out, there should be no further electronic marketing communications sent to that individual.

Breach Case Studies

Phishing Email Attack in the Broadcasting Sector

An organisation operating in the broadcasting sector notified a data breach to the DPC relating to an employee who had fallen victim to a phishing email. The email, purporting to be an advertisement for an internal vacancy, requested that the employee input their email and data storage platform credentials as well as their Multifactor Authentication (MFA) Authenticator Prompt. Having obtained this information from the employee, the bad actor who sent the phishing email was then able to gain access to this employee's email and data storage platform account.

Categories of personal data that were potentially accessed by the bad actor included names, email address, photos/videos, financial data and special category data (health data). The affected individuals included employees within the organisation and third party contacts who had engaged with the broadcaster. The organisation became aware of the breach when the employee reported issues logging into their email and data storage platform. The organisation's phishing detection systems had disabled the phished account automatically after 17 minutes, but the account was then manually reactivated by their in-house IT team in error. A manual review of audit logs showed suspicious logins attempted from different locations leading to the account being reset and the bad actor being locked out permanently.

The DPC reminded the organisation of its obligations as a data controller. On foot of this, the organisation implemented preventative measures in order to mitigate against a recurrence of this breach. These measures included spam/phishing filters, reminders to all staff to exercise caution opening external emails, increased training and staff awareness exercises, and new guidelines in relation to the reactivation of suspended user accounts.

KEY TAKEAWAYS:

Organisations should be aware of the importance of utilising preventative measures against data breaches that consist of both technical (phishing detection, spam/phishing filters) and organisational measures (staff training/awareness, simulated phishing attacks) and should monitor and check that these measures continue to be fit for purpose.

Digital File Storage Breach

A third level institution reported a data breach to the DPC relating to the storage of student medical certificates for a particular course. A student had discovered medical certificates relating to other students when attempting to upload their own certificate to the institutions Virtual Learning Environment (VLE). The institution immediately informed the DPO and their IT department removed the files.

The DPC assessed the notification and, given the nature of the special category (health) data involved, requested further information from the organisation. The investigation by the organisation determined that human error had led to a misconfiguration on the VLE, which meant that medical certificates were displayed to a group of students, rather than solely to the course coordinator/ lecturer.

The breach was originally deemed high risk by the organisation but following a review of the breached data and the risks posed to the rights and freedoms of the affected individuals, it was deemed to of lesser risk than originally assessed. The organisation decided to notify the impacted individuals about the breach out of an abundance of caution.

In order to prevent a recurrence of this situation, the institution issued an email to all staff to remind them not to use the VLE for the submission of personal data. The institution also added messages to the VLE platform to remind both staff and students of their data protection obligations when using the system.

The organisation engaged with the provider of the VLE to introduce measures to ensure that personal data is stored and processed securely, and security settings configured appropriately.

KEY TAKEAWAYS:

When utilising systems that require an individual to upload personal data such as medical certificates, organisations should be aware of the importance of ensuring that the data is securely obtained, accessed and processed. Any security features available should be configured appropriately and the users of the system should be fully aware of what is required. Only personal data that is required should be uploaded. Organisations can ensure this through clear messaging and training.

Personal Data Accidentally Disclosed Online

A third level institution reported a data breach to the DPC that related to a survey, it had carried out on former students. Each year recently graduated students were surveyed with a focus on their further studies and employment and this data was then used to publish a report on graduate outcomes. The summary statistics, which were not anonymised in this instance and included personal data, were published on the institution's website.

A member of the public reviewing the 2023 reports noticed that they were able to view the personal data of the survey respondents by right-clicking on the tables and brought this to the attention of the institution. This data included name, salary information and details of work or further studies. The third level institution removed the report and other externally available reports which were thought could experience the same issue. The third level institution also sought assurances that the personal data had not been saved or shared by the individual who discovered the dataset.

As part of the investigation of this breach, the institution informed the DPC that a new system was introduced for producing reports in 2022 and that a lack of familiarity with the new system had led to the data being published in a non-anonymised format. To mitigate against a recurrence of this issue the institution reviewed its internal processes for generating reports, as well as liaising with their internal IT teams to ensure appropriate technological measures are now in place.

KEY TAKEAWAYS:

When organisations choose to publish any statistics on websites, they must ensure that no personal data is included unless there is a clear lawful basis for the processing of that data. This can be achieved through aggregation, anonymisation, or redaction. Organisations are required to ensure that no unauthorised personal data is publicly displayed without a lawful basis.

CCTV

Domestic CCTV

During 2024, the DPC received **157 complaints** from individuals regarding the use of recording devices, for example domestic CCTV systems and smart doorbells by private individuals to protect their homes and property.

In examining these complaints, the DPC's focus is whether the processing of personal data by these devices comes within the scope of the GDPR or not. This is because of the household exemption under Article 2(2) (c) of the GDPR, which applies where personal data is processed by a natural person in the course of a purely personal or household activity. In the sphere of CCTV and smart doorbells, this would generally mean that as long as the images captured are within the perimeter of an individual's own home and are only used for their personal purposes, the domestic exemption is likely to apply. However, where a device operates in such a way as to capture images of people outside the perimeter of a home (in public spaces or in neighbouring property), individuals are no longer able to avail of the domestic exemption. In those circumstances, either the camera operation must change the way the device captures images to limit this to only within their property or they must comply with data protection law and their obligations as a data controller.

One complaint examined in 2024 by the DPC was from an individual against their neighbour alleging that the entire CCTV system, made up of multiple cameras, was capturing their personal data. The DPC contacted the camera operator who provided footage from the CCTV system. Upon examination of the footage provided to the DPC it was noted that a number of the cameras were capturing areas outside the perimeter of the operator's own home and that the remaining cameras were dummy cameras. The DPC engaged with the operator to bring the relevant devices into line with the domestic exemption.

The complainant in this case remained dissatisfied and requested additional details from the DPC about the cameras. The DPC engaged further with the individual to advise that once the cameras were being operated within the parameters of the domestic exemption and/or were dummy cameras, that it could not provide further information.

More information on this subject matter of domestic CCTV can be found at:
Domestic CCTV

KEY TAKEAWAYS:

- If you are operating a domestic CCTV system, you should ensure that it is not capturing public footpaths or roadways; under no circumstances should cameras be able to view the homes or gardens of neighbours.
- If the domestic exemption applies to the operation of domestic CCTV cameras, the operators are not deemed to be data controllers for the purposes of the GDPR and in such circumstances the DPC has no role to play. The DPC encourages individuals with concerns about a neighbours CCTV system to engage directly with the neighbour themselves in the first instance, so that a satisfactory resolution can be achieved.
- The nature of domestic CCTV systems, and their potential engagement of both the provisions of the GDPR and any possible exemptions from data protection law, requires that the DPC be cognisant of the particular circumstances of each individual case which it handles.
- Where a domestic CCTV system is being operated in line with the household exemption the DPC will not disclose details of that system to a complainant, as the GDPR would not be engaged and any such disclosure may compromise the security of the domestic CCTV operator.

Failure to respond to a request for CCTV footage

The DPC received a complaint from an individual who had made an access request to a transport company. They sought a copy of CCTV footage of an accident they were involved in with one of the transports company's buses. The individual did not receive a response to this request.

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

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

KEY TAKEAWAYS:

- Organisations should be aware that footage or images containing identifiable individuals captured by CCTV systems are personal data for the purposes of data protection law.
- More information on this subject matter can be found at: *Domestic CCTV*
- Organisations are required to implement appropriate organisational measures in place to ensure that they are in a position to respond to any rights requests within the stipulated timeframes under the GDPR.

Use of CCTV to monitor waiting area without adequate transparency measures

An individual was employed at a medical practice, which used CCTV footage of the waiting room to assess patient waiting times. When the medical practice was reviewing the CCTV footage, in the presence of the employee, the employee realised that their image had been recorded by the CCTV system throughout their employment without being aware of it. The individual tried to resolve the issue with the medical practice but was ultimately dissatisfied with the response they received and contacted the DPC to make a complaint.

The DPC contacted the medical practice to enquire about its legal basis for processing personal data in this manner. The medical practice advised that it had a CCTV policy in place prior to the individual commencing employment with it and that the purpose of the CCTV system was to ensure the health and safety of staff and clients of the medical practice. Having requested a copy of the CCTV policy, upon review the DPC noted that it was drafted prior to the introduction of the GDPR and had not been updated since.

Having engaged with the individual, the DPC established that they had not been made aware that CCTV was in operation constantly, including the areas where they worked, when they first joined the practice. There was one small sign on the entrance door of the practice that stated CCTV was in operation but the sign did not specify that the CCTV cameras were recording within the practice building.

During the course of the DPC's examination of the complaint the medical practice adopted measures to restrict the recording by the system so that it would no longer be in operation during business hours.

In this instance, the DPC found that the medical practice did not provide a valid lawful basis under Article 6 of the GDPR for this type of monitoring. Furthermore, the medical practice did not fulfil its transparency obligations under Article 13 of the GDPR, as it did not inform individuals at any point that the CCTV system would process their personal data, by recording their image, whilst in the practice.

In light of the medical practice's voluntary restriction of the CCTV cameras to operate outside of business hours only, the DPC engaged with the medical practice providing recommendations and guidance around the use of CCTV. On foot of this engagement, the medical practice increased the size, and the number of signs informing staff and patients of the use of CCTV and the contact details of the data controller in compliance with its obligations.

KEY TAKEAWAYS:

- Fairness and transparency are key to implementing proper privacy policies and procedures. As a general rule, nobody should be surprised to discover their personal data is being processed by a data controller.
- Proper signage around the use of CCTV and ensuring staff are given a copy of the current CCTV Policy are simple measures that can avoid complaints such as this case occurring.

Data Processing

Sharing personal data with third parties without consent

An individual was owed a debt from the Estate of a deceased person. The individual wrote to the law firm representing the Estate of the deceased to relay that they were no longer interested in pursuing the debt owed to them by the Estate. The law firm subsequently shared this letter with third parties – the executors and other beneficiaries to the Estate. The individual became aware that a copy of their letter was shared and contacted the law firm asking why their letter was shared without their consent. The law firm replied that as the individual had voluntarily written to it to decline any claim on the Estate, it had assumed it had the individual's consent to share with third parties for the purposes of disclosing the individual's now defunct claim on the estate. It also advised that the individual had given their consent for their personal data to be shared with third parties, including their name and address as well as the letter itself. The individual was unhappy with this response and therefore contacted the DPC to make a complaint.

The DPC requested the law firm to outline the lawful basis under which it shared the individual's letter with third parties. It replied that it had shared the letter as part of its contract to administer the Estate of the deceased. Furthermore, the law firm claimed, the individual had voluntarily written the letter and therefore it had inferred consent for the processing of the individual's personal data, as they were part of the claims on the Estate. It also claimed that it had been acting in the best interests of the individual by informing the third parties that they were no longer involved in the case.

Under Article 7(1) of the GDPR data controllers, when relying on consent as a lawful basis for processing personal data, must be able to demonstrate that the data subject has consented through a clear affirmative act in a freely given, specific, informed and unambiguous manner *(as per Article 4(11) of the GDPR)*. The law firm was unable to demonstrate that it had secured the individual's consent for it to process their personal data in the manner described.

The DPC engaged with the law firm further to ensure that going forward it was aware of its obligations under the GDPR in relation to the lawful bases for processing. In this case it was sufficient for the law firm to inform its clients and other third parties that the individual had relinquished their claim and therefore it was unnecessary to share the correspondence itself.

KEY TAKEAWAYS:

Under the GDPR, valid consent must be freely given, specific, informed, and unambiguous. Organisations must ensure that individuals clearly understand what they are consenting to and that they can withdraw their consent at any time. This case study highlights the importance of transparency and accountability when collecting and processing personal data. Non-compliant consent mechanisms can lead to reputational consequences for the organisation as well as regulatory consequences.

Disclosure of an employee's special category data by their employer to a third party services provider, without the employee's consent

An individual submitted an access request to their employer, a SME business-to-business service provider. Based on the documentation provided by the organisation to the individual in response, the individual submitted a complaint to the DPC alleging that the organisation unlawfully disclosed their personal data, including special category data, to a third party, a Human Resources Service Provider (HR provider).

When examining the information provided it became apparent to the DPC that the organisation had engaged the HR provider to investigate an allegation of bullying made by the individual against a co-worker. The organisation provided various categories of the individual's personal data to the HR provider, including the individual's personal contact details, medical data and a letter confirming the individual's fitness to partake in the alleged bullying investigation.

The individual provided evidence to the DPC proving that they had asked the organisation not to disclose their personal data to a third party and claimed that they were not informed that their personal data had been provided to the third party.

As part of the examination of the complaint, the DPC sought to establish if the organisation had a valid lawful basis for disclosing the individual's personal data and special category data to the HR provider in line with Article 6 and Article 9 of the GDPR. The DPC also sought to establish whether the personal data disclosed to the HR provider was relevant and limited to what is necessary for the purposes for which they were processed, in accordance with the principle of data minimisation under Article 5(1)(c) of the GDPR.

From its responses to the DPC it appeared that the organisation relied on Articles 6(1)(b) (contract); 6(1)(c) (legal obligation) and; 6(1)(f) (legitimate interests) of the GDPR, as the lawful bases under which it disclosed the individual's personal data to the HR provider.

The organisation stated it had legitimate reasons to provide the personal data and medical data to the HR provider under the terms of the individual's contract of employment and that the individual had consented to take part in the alleged bullying investigation. Further, the organisation stated that the HR provider requested it obtain from the individual a doctor's letter to confirm that the individual was fit to take part in the alleged bullying investigation.

The DPC accepted that provision of certain categories of the individual's personal data to the HR provider would be necessary under the terms of their employment contract in line with Article 6(1)(b) of the GDPR. However, the organisation failed to identify the legal obligation to which it stated it was subject to rely on under Article 6(1)(c) of the GDPR as a lawful basis for processing the personal data. The organisation also failed to provide evidence that it conducted a balancing test under Article 6(1)(f) of the GDPR prior to providing the individual's personal data to the HR provider. Additionally, the organisation failed to identify a lawful basis for disclosing the individual's medical data under Article 9 of the GDPR.

The DPC engaged with the organisation further to ensure that going forward it was aware of its obligations under the GDPR in relation to the lawful bases for processing.

KEY TAKEAWAYS:

The DPC recommends to organisations that it only process personal data when necessary, and for the stated purpose of processing.

In this regard, an organisation must be able to demonstrate to the DPC that it can provide the necessary, relevant information to the DPC to determine that the identified lawful bases under Article 6 of the GDPR are appropriate for the personal data processing in question. Organisations must also provide a lawful basis to process special category data under Article 9 of the GDPR.

Excessive sharing of special category data to a third party in order to seek guidance on behalf of an employee

An individual submitted medical documentation to their employer's disability officer in order to request reasonable accommodations that would support them in performing their work within a public sector organisation. The disability officer was the central point of contact and service provider for all staff with disabilities working for the organisation and the individual had occasionally had reason to contact the disability officer over the course of their employment.

During the course of a particular meeting with the disability officer, the individual had discussed their health and other personal data relating to their finances and family circumstances, and their concerns regarding their options in the event that they would no longer be able to continue to work. The individual subsequently discovered that following this meeting the disability officer had emailed a separate entity that provides support and assistance to employees across a number of similar organisations with regard to the meeting, including details of the individual's personal data and the matters the individual had disclosed during the meeting in order to get advice from the disability officer. The individual was surprised to discover the extent of what was shared with the third party without their consent.

Following receipt of a complaint from the individual, the DPC contacted the public sector organisation requesting it to identify the lawful bases under which it had shared the individual's personal data with the third party. The public sector organisation responded that the third party it had shared the individual's personal data with was an employee assistance service that provided support to employees on a range of topics. It maintained that the personal data, including special category data, had been processed under Articles 6(1)(d) and 9(2)(c) of the GDPR, "processing is necessary to protect the vital interests of the data subject" as the personal data had been shared with the third party in order to ask for guidance on how best to support the individual.

"Vital interests" refers to tangible life and death situations where life is in immediate or imminent danger and requires assessment on a case-by-case basis by data controllers when seeking to rely on this lawful basis for processing. This lawful basis does not apply to processing that is performed in the data subject's medium or long term best interests. Following the DPC's examination of the information that was shared, it became apparent that the amount of the individual's personal data that was shared was excessive in terms of the purpose it sought to serve.

Data controllers are reminded that, even when acting in the best interests of the data subject, all processing of special category data requires enhanced measures in terms of security and confidentiality that data controllers are obliged to meet. The use of vital interests as a lawful basis will only be valid under an immediate, demonstrable threat to life whereas no such threat existed in this case.

In this instance, the public sector organisation initially considered that sharing this personal data with a third party service provider for the purposes of providing the best advice to the individual was compatible with the original purposes for which it was processed. However, on review of the personal data shared the public sector organisation conceded it had shared an excessive amount of un-redacted personal data in order to achieve its purposes. An anonymised description of the individual's circumstances could have achieved the same purpose without sharing the individual's personal and special category data.

Furthermore, there was no evidence provided by the public sector organisation that demonstrated that the individual was made aware that their personal data could be shared with third parties in order to procure advice on their behalf at the time. Following on from the DPC's examination of this complaint the public sector organisation revised its disability service information notices in order to fulfil its transparency requirements and engaged in appropriate training for staff to ensure that further unnecessary sharing of this type would not reoccur.

KEY TAKEAWAYS:

- Data controllers are reminded that sharing personal data with third parties requires a valid lawful basis. When sharing for compatible further purposes, data controllers are reminded that there is a compatibility test that will assist in determining whether the proposed processing is in line with its legal obligations.
- When considering further processing a good rule of thumb is to ask whether your organisation will use the data in a way in which those who supplied it would expect it to be used. This question should be the starting point for your compatibility test. When processing of this type is proposed safeguards should be built into the data flows to ensure data minimisation is central.
- When personal data is processed under consent as a lawful basis, data controllers are reminded to ensure that any possibility of sharing with third party providers is clearly signposted to individuals before processing the personal data by sharing it.

Processing employee's personal data from their private email account/emails for disciplinary purposes

Two individuals were employed by an organisation that provides services to primary schools. Upon arrival at work, one individual found their personal email account open on their shared computer. A few weeks later, the individual's employment was terminated on foot of disciplinary proceedings. During the course of the proceedings, the individual was presented with printed copies of several emails from their personal email account. The second individual was also dismissed. It became apparent that a third party had been hired by the organisation to handle the disciplinary proceedings and this third party was provided with a copy of both individual's emails addressed to each other.

The reason given for the termination was that both employees had been discussing a business plan that would make them a competitor to their then employer. The emails had been accessed and printed by the employer. Both individuals had also made access requests. Following the disciplinary proceedings and the dismissals, the individuals contacted the DPC and made their respective complaints. Both complaints referred to the processing of their personal data from their email exchanges found in the personal email account that one individual had left open on the shared access computer and the subsequent processing of it to conduct disciplinary procedures that resulted in the termination of both staff members' employment.

The DPC began a parallel but separate examination of the complaints by asking the organisation to provide its lawful basis for processing the individuals' personal data from the personal email account and personal emails. The organisation responded that when searching the email account for client information it was noticed that it was a personal email account but it was also noticed that there were discussions between two employees regarding the setting up of a competing business. The organisation claimed it processed the individuals' personal data for a legitimate interest in that it was an attempt to protect the

business and its other employees. The organisation also claimed that it had processed the personal data lawfully as the individuals had consented to the processing of any/all of their personal data. It argued that this consent had been provided when they had been provided with a copy of the company privacy notice that informed them it would process their personal data (including all IT equipment and assets) and was evident in their signed contracts of employment.

In terms of the reliance on its employee contracts and its company policy and privacy notice to indicate that the individual had provided their consent for the company to use its personal data, the DPC noted that consent to process personal data from personal email accounts was not a valid lawful basis for processing in the circumstances. Additionally, in order for consent to be valid it must be freely given, specific, informed and unambiguous. The reliance on signing a contract of employment to indicate consent for processing does not meet the criteria required to utilise this lawful basis for processing.

The DPC found that the individuals' data protection rights were infringed by the organisation under Articles 5(1)(a),(b),(f) of the GDPR, which relate to the principles of lawfulness, fairness and transparency; purpose limitation; and integrity and confidentiality. Further, the initial accessing and viewing of the individual's personal email account was conducted in breach of their data protection rights, contrary to Article 32(1) and 32(2) of the GDPR.

The organisation implemented a number of security measures to ensure that such an incident would not occur again such as staff training on GDPR and IT, internet and email usage including computer log-in processes.

KEY TAKEAWAYS:

Data controllers should be aware that privacy notices and contracts of employment that stipulate business equipment may be subject to monitoring for business purposes cannot amount to a blanket consent for processing any employee personal data that is found on business equipment.

Processing occupational health data

An individual submitted a complaint to the DPC after a medical facility disclosed their medical data to their employer. The individual attended the medical facility at the request of their employer, due to a long absence of sick leave from work. During the consultation at the medical facility, the individual was queried on their past medical history, which was not directly related to their current illness. The medical facility furnished the individual's employer with a full copy of their consultation notes, including their historical medical data.

In correspondence with DPC, the medical facility advised that it was standard practice for the medical facility to share medical data between medical professionals. However, only the minimum data necessary should be shared with an individual's HR department, advising if an employee is either fit or unfit for work. In this instance, the medical facility shared the full medical data of the individual with the employer's nurse practitioner, a medical professional, it also further processed this data by sharing the full medical data with the HR department.

The medical facility also detailed how the full medical report was incorrectly disclosed to the individual's HR department. It advised that following a phone call with the individual's employer, a manager within the HR department requested a copy of the medical report detailing the individual's fitness to work. The medical facility stated it had incorrectly assumed consent had been given by the individual for this request and subsequently furnished the HR department with the full medical data.

Medical data, or personal data concerning health, is considered a "special category of personal data" under Article 9 of the GDPR and is subject to specific rules, in recognition of its particularly sensitive nature and the particular risk to the fundamental rights and freedoms of data subjects, which could be created by the processing of such data. The processing of medical data is only permitted in certain cases as provided for in Article 9(2) of the GDPR, in conjunction with Article 6 of the GDPR. Furthermore, Article 5(1)(f) of the GDPR relates to the principle of integrity and confidentiality when processing personal data, to include protection against unlawful processing. In this instance, the medical facility advised the DPC that it had not informed the individual that their medical data would be further processed or disclosed to their employer at the time of their consultation.

As the medical facility failed to demonstrate a lawful basis for the processing, the DPC determined the processing to be unlawful and not in compliance with the requirements of the GDPR.

Following the conclusion of the data protection complaint, the DPC engaged further with the medical facility in relation to its data protection practices and policies.

KEY TAKEAWAYS:

Data controllers must always be able to demonstrate a lawful basis for processing and especially in circumstances where the personal data is special category data, which has additional protections under Article 9 of the GDPR.

Law Enforcement Directive (LED)

Law Enforcement Directive (LED) Access Request - Rights and Restrictions

Under the Law Enforcement Directive (LED) as transposed into Irish law by Parts 5 & 6 (sections 69 to 104) of the Data Protection Act 2018 (the Act), there may be restrictions placed on an individual's right of access to records containing personal data.

An individual requested all personal data pertaining to themselves processed by An Garda Siochána (AGS). AGS responded to the individual providing some documentation containing personal data. In its reply, AGS also advised that certain documents were being released in a redacted format and that further documents were being withheld, in their entirety. The exemptions on which AGS were relying were sections 91(7) and 94(3)(a) of the Act. Section 91(7) refers to data that includes personal data relating to another individual that would reveal, or would be capable of revealing, the identity of the other individual while 94(3)(a) relates to data that would prejudice the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties.

As the individual was not satisfied with the response received from AGS, they made a complaint to the DPC. Upon receipt of the complaint, the DPC identified it as being a LED complaint as opposed to a GDPR complaint. As part of the DPC's examination of the complaint, the DPC requested AGS to provide further detail in relation to its reliance on exemptions to withhold personal data in response to the access request. Upon receipt of the requested further detail from AGS, the DPC then requested to view all redacted and withheld personal data and attended at the AGS office to do so.

An on-site visit took place in which the DPC examined the documents in question. During this visit, the DPC engaged with AGS seeking clarification on the exemptions being applied to the documents that were being redacted and withheld in their entirety. Following this engagement, further personal data was identified for release. The outcome of this onsite visit resulted in the individual receiving their personal data and the AGS gained a greater understanding of the how the exemptions can be applied.

KEY TAKEAWAYS:

The viewing of the documentation by the DPC at the offices of the AGS allowed the DPC to engage directly with AGS in relation to its use of exemptions. In requiring AGS to be more thorough in its assessment of such exemptions, the DPC enabled additional personal data to be accessed by the individual – albeit legitimately redacted – per the 2018 Act.

Right to be Forgotten (RtbF)

Right to be Forgotten (RtbF) search engine results for an individual's first and last name

An individual contacted a search engine company to request that a number of websites remove articles about them that contained their name, as they believed the articles were no longer relevant to their current life and circumstances. The search engine organisation replied to them and outlined that their requests did not fulfil the criteria for it to remove them. The individual was unhappy with this response and contacted the DPC to make a complaint.

The DPC began its examination of the complaint by asking the company for the reasons why it believed that the individual's Article 17 rights under the GDPR did not apply to the individual's request. The company responded that it was under the understanding that only the links to articles that arise from a search of the individual's full name can qualify for consideration when requests are made under Article 17 of the GDPR. In other words, the search engine will separate the automatic appearance of those URLs when the individual's full name is searched for in its results listing. However, the original articles remain online on the websites that posted them.

When the individual had made their request to the company, they had listed a series of URLs that contained their full (first and last) name. However when the organisation performed a search of the individual's full name the URLs they had specified did not appear in the results listing and therefore did not fall under the scope of Article 17 of the GDPR. In this instance after performing searches under the individual's full name the DPC did not find the URLs that they had requested be delisted and therefore found that on this occasion the right to be forgotten under Article 17 of the GDPR was not applicable.

KEY TAKEAWAYS:

The right to be forgotten is not an absolute right; it refers only to search engine results and not the links provided by the search engine results. It does not extend to the results of all internet searches and there are key factors that must be present for requests for delisting to be valid. As per guidelines from the European Data Protection Board (5/2019), should an individual obtain from an internet service provider the delisting of a particular content from its search engine, *"this will result in the deletion of that specific content from the list of search results concerning the (individual) when the search is, as a main rule, based on his or her name. This content will however still be available using other search criteria."*

Cross-Border

Cross-Border Complaint Concerning an Access Request to a Large Social Media Platform

The DPC received a complaint via the One-Stop-Shop (OSS) mechanism related to an access request made to a large social media platform (Data Controller) pursuant to Article 15 GDPR.

The individual noticed that their account with the Data Controller appeared to have been hacked and subsequently disabled by the Data Controller. The individual made an access request to the Data Controller in order to obtain a copy of their data. The Data Controller directed them to a set of self-service tools outlining how to access and download their data.

However, the individual was unable to avail of the self-service tools due to the restriction placed on their account. Having raised this issue with the Data Controller, the individual received further correspondence from the Data Controller explaining that for security reasons it was unable to reinstate the account or provide a copy of the data and considered the case closed. Upon receipt of the complaint, the DPC commenced an examination of the complaint with the Data Controller pursuant to section 109 of the Data Protection Act. In response to the DPC's examination, the Data Controller referred the account to its internal team for further investigation, which confirmed that the account showed signs of compromise and that the account had been disabled as a result of activity which occurred on the account during the period it was compromised. The Data Controller therefore agreed to reverse the disablement of the individual's account and facilitate them in regaining access. Once they had regained full access to their account, the Data Controller advised how the individual could access the self-service tools to access and download a copy of their data if they still wished to do so.

In light of the above actions, the Data Subject subsequently confirmed to the DPC that they considered their complaint resolved.

KEY TAKEAWAYS:

This case illustrates the need to ensure appropriate measures are in place to facilitate the exercise of data subject rights, and how directing individuals to self-service tools as a default response to an access request will not always be an appropriate means of doing so. This is particularly so where an individual is unable to avail of the self-service tools for whatever reason, such as where an account may have been hacked by a third party and subsequently restricted by the controller as a result.

Cross-Border Complaint Concerning a Delisting Request

The DPC received a complaint via the One-Stop-Shop (OSS) mechanism related to a "right to be forgotten" delisting request made to a large multinational technology company (Data Controller) pursuant to Article 17 GDPR.

The individual contacted the Data Controller requesting the delisting of several URLs. The content of these URLs described events that transpired at the school of which the individual was the principal. The individual explained that they are not a public figure and were no longer the principal of the school in question. The individual asserted that many of the 'facts' cited in the article were incorrect. The article also referred to certain special category data related to the individual, which the individual asserted was also incorrect. The individual stated that they did not receive a response from the Data Controller and submitted a complaint. Upon receipt of the complaint, the DPC commenced an examination of the complaint with the Data Controller pursuant to section 109 of the Data Protection Act. In response to the DPC's examination, the Data Controller explained that, following an extensive investigation, it could find no record of the delisting request from the individual. The Data Controller asserted that it did not refuse the delisting request; rather, it was unaware of the request prior to the DPC's intervention.

On foot of the DPC's examination, the Data Controller proceeded to carry out a substantive assessment of the individual's request and determined that, although certain of the complained-of URLs were ineligible for delisting for a number of reasons (e.g. because they did not contain personal data relating to the individual, or because they did not provide a return in the EEA (or UK) versions of its search engine when a search was carried out against the names provided), a number of other URLs were potentially eligible for delisting subject to certain further clarifications being provided by the individual relating to their content. The Data Controller reached out to the individual directly outlining the results of its assessment and noting that it would need further information to complete its adjudication of the delisting request. The Data Controller continued to engage with the individual in this regard and the individual later wrote to the DPC to confirm that the complained of URLs had now been delisted to their satisfaction and that the matter was resolved.

KEY TAKEAWAYS:

There are many elements to be considered when assessing a "right to be forgotten" delisting request pursuant to Article 17 of the GDPR. A balancing test must be carried out by the data controller in order to establish whether the public interest in having access to the information in question outweighs the individual's right to have that information erased, accounting for all relevant factors presented in the specific case. In this particular complaint, a comprehensive assessment was carried out by the Data Controller following the DPC's intervention, resulting in the satisfactory resolution of the complaint with the individual.

Notes

Notes