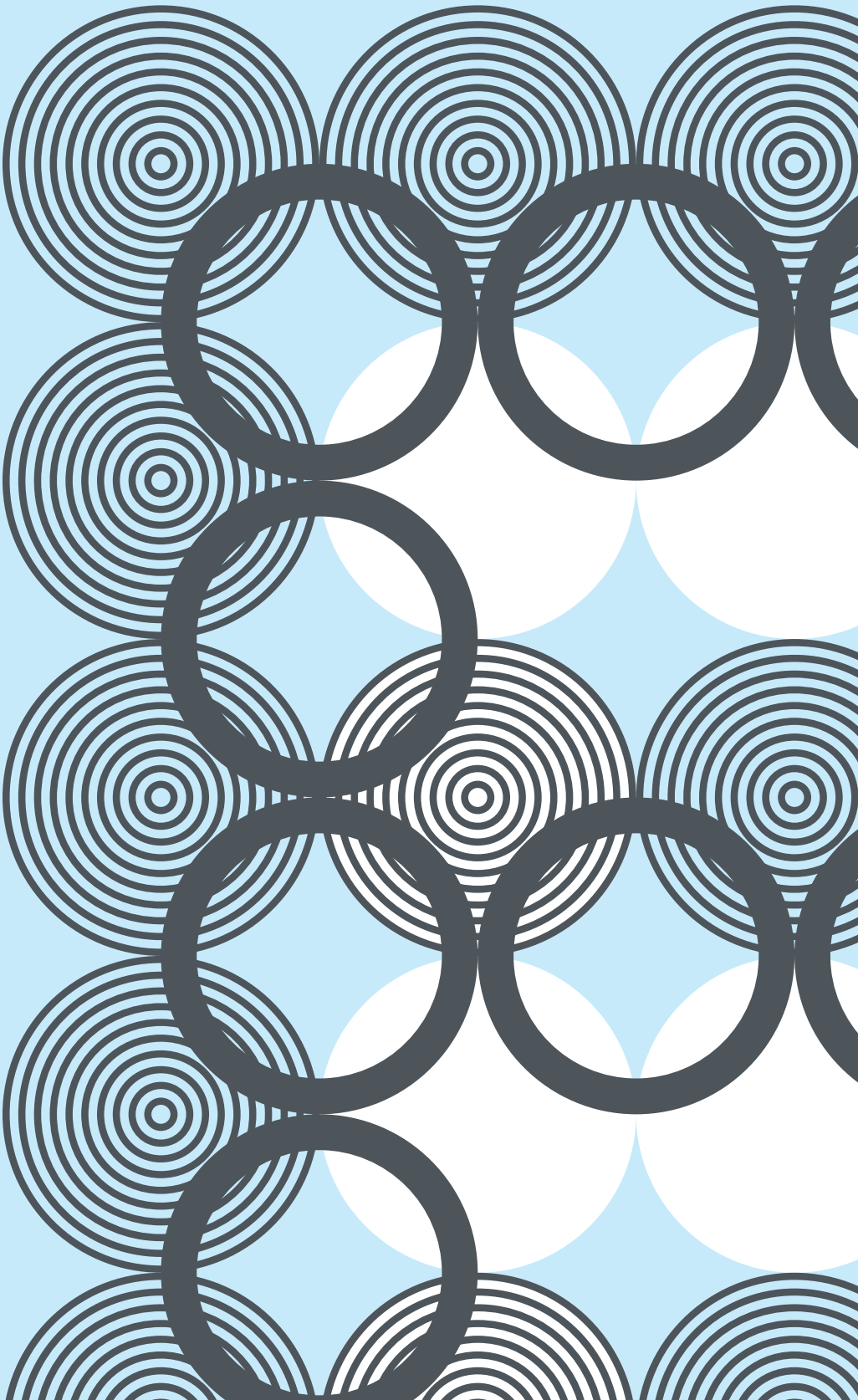
An Coimisiún um Chosaint Sonraí
Data Protection Commission

Case Studies 2025

Introduction

The mission of the Data Protection Commission (DPC) is to uphold the fundamental right to data protection through the consistent and effective application of data protection law. This is achieved through meaningful engagement, robust supervision and enforcement, and by driving compliance across all sectors. A central pillar of this mission is supporting organisations in understanding and meeting their obligations. To further this goal, the DPC is committed to publishing case studies that illustrate how data protection law is applied in practice, how instances of non compliance are identified, and how corrective measures are implemented.

This booklet presents the case studies compiled throughout 2025 and reflects the DPC's ongoing commitment to ensuring the proper and proportionate application of data protection law. It may be read in conjunction with other cases as set out in this year's Annual Report.



Contents

Subject Access Request Case Studies

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.

Case Study 1

Application of restrictions under the GDPR and the Data Protection Act 2018 in relation to a Subject Access Request

The DPC received a complaint from an individual who had submitted a Subject Access Request under Article 15 of the GDPR to their former employer, a national school. The school had provided a response to the individual within the statutory period of one month, but the complainant had sought the release of additional documents.

The DPC commenced its examination and in responding to the DPC, the school advised that they had released personal data to the individual, but that it had:

- redacted information due to the presence of third-party data in line with Article 15(4) of the GDPR; and

- issued a refusal in relation to records containing personal data on the basis of legal advice privilege and litigation privilege as provided for under Section 162 of the Data Protection Act 2018.

The DPC examined the application of the restrictions and sought details of the completed balancing test, which is required to be undertaken in relation to an individual's right of access and the rights and freedoms of other individuals. The DPC also reviewed copies of the unredacted versions of the records to ensure that the restrictions had been applied fairly and appropriately. Following further engagement with the school and a detailed review of information provided the DPC was satisfied that the organisation had correctly applied Section 162 of the Data Protection Act 2018.

The DPC informed the individual that after careful examination of their complaint, the DPC was satisfied that the organisation had provided all outstanding personal data and had correctly applied restrictions in limiting access to third-party data under Article 15(4) of the GDPR and under Section 162 of the Data Protection Act 2018, in the context of legal advice privilege and litigation privilege.

KEY TAKEAWAY

- A data controller can rely on restrictions to releasing personal data in certain circumstances, but must ensure a balancing test has been applied fairly and appropriately in these circumstances. Evidence of this balancing test should be made readily available to the DPC, if requested.

Case Study 2
Application of restrictions for withholding personal data

The DPC received a complaint from an individual who had submitted a Subject Access Request under Article 15 of the GDPR to their former employer, a pastoral centre who offered counselling services.

The organisation had informed the individual that the record sought, which contained their personal data, was being withheld in its entirety. The justification provided for the full refusal was that, while the record contained the individual's personal data, it further contained the personal data of a third party who was a user of the pastoral centre's counselling services. The individual subsequently lodged a complaint with the DPC, expressing concern that the organisation was incorrectly withholding the data in full without considering provisions for partial disclosure.

The DPC engaged with the organisation to assess the validity of restricting the individual's right of access, which included the provision of information around the application of restrictions, in particular Article 15(4) of the GDPR, and the requirement to undertake a balancing exercise.

While it was clear that the organisation had undertaken a full and thorough balancing exercise, the DPC was of the view that the organisation's determination to withhold the data in its entirety did not balance the rights of the individual and third-party rights proportionally. The DPC advised the organisation that its obligation to protect the rights and freedoms of others does not permit a blanket refusal of an individual's right of access to their personal data.

The DPC provided the organisation with information regarding a judgement by the Court of Justice of European Union (CJEU) in Case C-487/21 (F.F. v Österreichische Datenschutzbehörde and CRIF GmbH), which clarifies what a 'copy' of personal data is. In summary, the Court ruled that a data subject must be given a faithful and intelligible reproduction of all personal data being processed by a controller. This means, depending on the exact details of the record, the individual has the right to obtain either entire records, or if third party data is present in those records, they are entitled to extracts or a summary of the personal data contained in those records.

The DPC advised the organisation to reconsider its application of the exemption with regard to the judgment of the CJEU and with consideration for the data protection rights of the third party. The organisation proceeded to provide the individual with an intelligible reproduction of the record with the appropriate redactions applied.

This case underscores the importance of proportionality when applying restrictions to the right of access under Article 15 of the GDPR, and the importance of balancing the rights of an individual and the rights of third parties.

KEY TAKEAWAYS

- When seeking to rely on the application of a restriction to withhold access to personal data, an organisation must undertake a thorough examination of the validity of such restrictions to ensure personal data is not withheld without careful consideration of the concept of necessity and proportionality.
- 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 or by providing a faithful and intelligible reproduction of the data.

Case Study 3
Unfounded refusal of a Subject Access Request

The DPC received a complaint from an individual in relation to a Subject Access Request made under Article 15 of the GDPR to an organisation, an independent publisher. The access request had been made almost three months prior to the complaint being submitted to the DPC. The organisation had informed the individual that the access request was being refused on the basis that it deemed the request to be manifestly unfounded and excessive.

Upon commencement of the examination of the complaint, the organisation advised the DPC that it was a small-sized company and that the access request was very broad; which would involve an extensive review of records possibly containing personal data which might fall for release under Article 15 of the GDPR.

In progressing matters, the DPC provided the company with guidance in relation to access requests, in particular, advising the company to issue an interim release of records containing personal data to the individual while the remainder of the data was being reviewed by the company. The company complied with the DPC's advice and released the records containing personal data to the individual in batches.

As a result of the DPC's intervention, the company and individual engaged with each other and refined the parameters of the access request initially made. Following this, the access request was fulfilled and the individual received all the records.

KEY TAKEAWAYS

- The guidance from the DPC to the company provided clarity as to its responsibilities as a data controller and assisted in an amicable resolution process by promoting positive engagement between the controller and the individual. The fact that a large volume of records containing personal data exists, and that its review requires a large dedication of resources, is not a valid reason for refusing a Subject Access Request under Article 12(5) of the GDPR.

- 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.

Case Study 4
Right of access and opinions given in a workplace setting

The DPC received a complaint from an individual who had submitted a Subject Access Request under Article 15 of the GDPR to their former employer, an Education and Training Board. The individual disagreed with the decision by their employer to redact information contained within one document and to withhold the release of two other documents. The employer stated that the data was submitted to it in confidence and would therefore not fall to be released.

In correspondence to the DPC, the organisation stated that it was restricting access to the individual's personal data under Article 15(4) of the GDPR and Section 60(3)(b) of the Data Protection Act 2018. Section 60(3)(b) of the 2018 Act may permit an organisation to withhold information from an individual, to the extent that the information constitutes: (a) an expression of opinion; and (b) that it is given in confidence.

The DPC engaged with the organisation regarding which restrictions were being relied upon and requested sight of the unredacted copy of the document which had been restricted under Article 15(4) of the GDPR. The DPC also requested that the organisation provide background information regarding the use of Section 60(3)(b) of the 2018 Act to restrict access to the personal data.

Upon receipt of the documents the DPC determined that, in line with Article 15(4) of the GDPR, the redactions were applied correctly in order to protect the rights and freedoms of third parties. However, in response to queries raised by the DPC in relation to Section 60(3)(b) of the 2018 Act, the organisation confirmed that the opinion had been given in a managerial capacity concerning an employee in a work performance context.

Section 60(3)(b) of the 2018 Act has a high threshold for the criteria of confidentiality to be achieved. Supervisors and managers will not normally be able to rely on this provision as providing opinions on staff performance is an expected part of their role, and they should be in a position to stand over the opinions provided.

The DPC engaged with the organisation and recommended that it release the personal data to the individual. The individual subsequently confirmed that they were satisfied that all of their personal data had been released to them.

KEY TAKEAWAY

- When responding to a Subject Access Request, an organisation may be entitled to restrict the release of personal data, provided it can demonstrate its reliance and application of the restrictions and/or exemptions under the GDPR and/or the Data Protection Act 2018. In such a case, the organisation must be able to demonstrate the reasoning for any restrictions and/or exemptions made over the right of access and should consider the relevant thresholds related to restrictions and exemptions.

Case Study 5
Charging a fee to access personal data

An individual contacted the DPC as they had made a Subject Access Request to their GP for a copy of their medical records and was advised that there would be an administrative fee for responding to their request.

Following receipt of this complaint, the DPC corresponded with the GP to determine why a fee had been sought for this individual's access request. The GP advised the DPC that the access request in question had been a repeat request from the individual for the same information within a short time frame. As this repeat request did not include any new or additional information, the GP found that the fee was required in this instance to cover administrative costs.

When responding to the individual, the DPC advised them that while there is generally no fee payable by an individual to make an access request; as this request was a repeat request for identical information, the DPC had established that the GP was charging the fee to cover the administrative costs in handling the repeat request.

Under Article 12(5) of the GDPR, organisations must deal with access requests free of charge. However, where the organisation believes a request is manifestly unfounded or excessive (for example, where an individual makes repeated access requests for the same information), the organisation may either charge a fee, taking into account its administrative costs in dealing with the request(s), or refuse to act on the request(s). The burden of demonstrating why a request is manifestly unfounded or excessive rests on the organisation.

KEY TAKEAWAY

- Under the GDPR, organisations must respond to Subject Access Requests free of charge. A fee is only permitted where the request is manifestly unfounded or excessive, and the organisation must be able to justify this. Individuals are encouraged to make requests in writing and retain a copy of their request and/or any response(s) received. Further guidance on making an access request, including information on accessing medical records is available on the DPC website.

Information on accessing medical records

Case Study 6
Access request on behalf of a family member

A family member submitted a Subject Access Request seeking a copy of the personal data of an individual with additional needs who was living in a residential service. Although the family member was one of the person's primary carers, the residential facility refused to release a copy of the records because the requester did not hold the necessary legal authority to act on the individual's behalf. The facility did, however, arrange a meeting to discuss the records with the family member so they could remain informed, while maintaining that copies would not be provided without proper authorisation.

The DPC considered the facility's approach appropriate. The organisation protected the data protection rights of the individual while still supporting the family member in their caring role.

KEY TAKEAWAY

- A person can only make a Subject Access Request on behalf of someone else when they have the legal authority to do so. Organisations must verify that any request made on the behalf of another individual is valid, prior to the disclosure of any personal data.

Case Study 7
Dissatisfaction with an organisation's response to a Subject Access Request

An individual submitted a complaint to the DPC regarding a retail sector organisation. They claimed that the organisation's response to their Subject Access Request was incomplete and that additional personal data, particularly certain emails, had not been provided.

The DPC contacted the organisation and informed them of the complaint. The organisation confirmed it had supplied all personal data in its possession to the requester.

When the DPC communicated this to the complainant, the individual maintained that emails involving a named third party were missing. The DPC clarified that an access request only entitles an individual to their own personal data, not to the personal data of third parties; nonetheless, the DPC further enquired with the organisation regarding the alleged missing correspondence. The organisation provided evidence demonstrating the data it had released and confirmed that no additional personal data existed.

Where two parties provide conflicting accounts, the DPC cannot determine that an infringement has occurred without clear evidence. In this case, the individual did not provide any documentation or information to substantiate the claim that further personal data existed or had been withheld. As no evidence supported the allegation of omission, the DPC concluded that no infringement by the organisation could be established.

KEY TAKEAWAY

- Individuals often assume that additional personal data must exist beyond what they receive in response to a subject access request. When a complaint is made, the DPC will engage with the organisation to verify that all relevant data has been provided. However, the DPC cannot find an infringement without concrete evidence that personal data has been withheld.

Case Study 8
Redactions in a Subject Access Request Response

An individual contacted the DPC after receiving a response to a Subject Access Request they had made to their employer. While the employer provided all personal data relating to them, some documents contained redactions, with only limited personal data visible.

The individual sought clarification on whether the GDPR permits the redaction of entire documents and whether the employer had met its obligations.

The DPC explained that, under the GDPR, an access request entitles an individual to their own personal data only. They are not entitled to receive the personal data of third parties, commercially sensitive information, or any material that is not personal data. Where documents contain mixed information, controllers may redact non personal or third party data to ensure compliance.

In this case, the employer had redacted the documents so that only the requester's personal data remained visible. This approach was consistent with GDPR requirements. The individual accepted that the organisation had provided the information to which they were entitled, and the matter was closed.

KEY TAKEAWAYS

- Under the GDPR, redaction of third-party data is often required where documents for release also contain personal data relating to another individual. It is not uncommon for individuals to receive redacted material in response to a Subject Access Request made under Article 15 of the GDPR.
- Where an individual is concerned about the level of redaction, it is open to them to contact the organisation and request the basis on which the redaction was carried out. If they remain dissatisfied after this engagement, the individual can then submit a complaint to the DPC and it will then be assessed for compliance with the GDPR.

Case Study 9
Failure to respond in full to a Subject Access Request for medical data

An individual contacted the DPC regarding a Subject Access Request they had submitted to a hospital. In their request, the individual sought access to video footage and an audio file that had been created when the individual took part in a medical study. The hospital refused access to the information, advising that the video footage had been automatically over-written after two weeks, and that the audio file could not be accessed without special software that the hospital did not have access to.

As part of their complaint, the complainant told the DPC that that the hospital had not informed them, at the time of participating in the medical study, that the video footage would be deleted after two weeks.

The DPC contacted the hospital to request clarification on the retention period for the video footage, and whether or not it could provide a copy of the audio file. The hospital confirmed to the DPC that the video footage was retained for two weeks to allow the consulting doctor to review the information gathered and, unless further review was required, there was an automatic process in place to delete the information after two weeks. The hospital further informed the DPC that, as the audio file was not required by the hospital, it did not have the necessary software to access it. The hospital also confirmed that the audio file had been deleted after a two-week period.

As the complainant had submitted their request to the hospital more than two weeks after the end of the study, the information had already been deleted. As such, the DPC found that the hospital had responded to the access request in full. However, the hospital had not been transparent with the complainant in relation to the retention periods for the video or the audio file. The DPC engaged with the hospital in relation to its obligations in terms of improving its transparency with individuals regarding the personal data it processes. transparency with individuals regarding the personal data it processes.

KEY TAKEAWAY

- Organisations should be clear and transparent with data subjects when processing their personal data, including informing them of retention periods. It is important that retention policies are detailed and include specific reference to information that does not fall within the broader retention periods of data processed by an organisation.

General Data Protection Case

Case Study 10
A request to a school from An Garda Síochána

A school informed the DPC that it had received a request from a member of An Garda Síochána under Section 41(b) of the Data Protection Act 2018, seeking access to personal data relating to one of its students. The Garda member stated that the information was required for an official purpose.

The school sought guidance from the DPC on how it should respond. The DPC advised that, before disclosing any personal data, particularly where special category data under Article 9 of the GDPR might be involved, the school was entitled to seek further clarification. As the Data Controller, the school needed to verify the requester's identity and authority and confirm the lawful basis being relied upon under Section 41(b), and understand the purpose for which the data would be used.

The DPC also explained that, once a valid legal basis under Article 6(1) of the GDPR was established, the school could release the data if satisfied that the request was necessary and proportionate. The school, as Controller, was required to justify the processing and maintain records demonstrating compliance. After receiving this guidance, the school then sought the necessary clarifications from the Garda member and was satisfied as to the legal basis and the authority provided.

KEY TAKEAWAY

- When responding to a Section 41(b) request, a data controller, such as a school, does not have to disclose personal data automatically. The school should first check the request is valid and clarify the lawful basis being relied upon, and then ensure that the disclosure is necessary and proportionate to the stated purpose. The DPC considers that requests from An Garda Síochána should be in writing and clearly set out the purpose for the request. The authority can be signed by an officer superior to the Garda member carrying out the lawful activity.

Case Study 11

A request for historical documents which were no longer held

An individual submitted a complaint to the DPC after a bank declined to provide copies of their historical bank statements. The individual believed the bank was refusing to release their personal data in response to a Subject Access Request.

The DPC contacted the bank to determine why a copy of the requested data had not been provided. The bank explained that the account in question had been closed 20 years earlier and, in line with the bank's retention schedule, all associated records had been permanently deleted.

This position was relayed to the individual. While they rejected the bank's position, the DPC advised them that it was satisfied that the personal data requested had been erased by the bank in accordance with its record management policies and storage limitation principle under Article 5(1)(e) of the GDPR. The bank had complied with its obligations, and therefore there was no evidence to suggest an infringement of data protection law.

KEY TAKEAWAYS

- A Subject Access Request provides access only to personal data that exists at the time of the request being made. Under the GDPR's storage limitation principle, organisations must not retain personal data longer than necessary and should routinely delete data that is no longer required.
- When requesting older or historical records, individuals should be aware that the data may have been lawfully deleted in line with an organisation's retention policy. If the data no longer exists, the organisation cannot be required to provide it.

Case Study 12
A request for erasure of medical data

The DPC received a complaint from an individual under Article 17 of the GDPR (the right to erasure). The individual informed the DPC that they had submitted an erasure request to an organisation operating in the occupational health sector, but the organisation had not responded. The personal data at issue consisted of health information, which is classified as special category data under Article 9(1) of the GDPR.

When contacted by the DPC, the organisation provided a detailed response. The organisation explained that it continued to process the complainant's personal data under Article 9(2)(h) of the GDPR, which permits processing where it is necessary for purposes such as occupational medicine, assessment of working capacity, medical diagnosis, or the provision and management of health or social care services.

The organisation also outlined its legal basis for refusing the erasure request. It pointed to its being regulated by the Medical Council, which has the authority to investigate complaints and impose significant sanctions where necessary. To defend itself in the event of a complaint, the organisation must rely on medical notes and records documenting its interactions with a service user. Deleting these records prematurely could compromise the organisation's ability to respond to regulatory scrutiny and potentially lead to unfair outcomes. The organisation also informed the DPC that the complainant's personal data would be deleted seven years after its last engagement with them, in line with its data retention policy.

While the complainant was not satisfied with this explanation, the DPC found that the organisation had a valid legal basis to refuse the erasure request.

However, the DPC further found that the organisation failed to meet its obligation under Article 12(3) of the GDPR, which requires controllers to respond erasure requests within one month. The DPC engaged further with the organisation to remind it of its obligations in relation to Article 12 of the GDPR.

KEY TAKEAWAYS

- The right to erasure in the GDPR is not an absolute right. Organisations may be legally required to retain personal data, particularly medical or other sensitive records, for regulatory, professional, or liability-related reasons. These obligations can justify refusing an erasure request; however, organisations must balance individuals' rights with their own statutory and professional duties.
- As this case illustrates, even where erasure cannot be granted, organisations must still comply with procedural requirements, including responding to requests within the mandated timeframe. Further guidance on this topic can be found at amending or erasing medical records.

Amending or erasing medical records

Case Study 13
Proving identity as part of making a GDPR rights request

An individual submitted a complaint to the DPC regarding a request for personal data they had made to a state body. The state body replied to the individual requesting a certified copy of their photo identification. The individual believed that this request for certified identification was excessive and this formed the basis of their complaint to the DPC.

The DPC contacted the organisation. In their response, the organisation highlighted that, as a state body handling highly sensitive child protection data, it is imperative that they are assured of an individual's identity prior to the release of any personal data. In an effort to resolve this complaint, the organisation proposed an alternative means for the individual to confirm their identification by providing a copy of a government issued ID. However, the individual maintained that this alternative was also excessive.

Article 12(2) of the GDPR states that *'The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject'.* As further outlined in Recital 64 of the GDPR, a data controller must adequately identify the requester's identity (meaning securely associate the data subject to a name and surname) having used all reasonable measures.

The DPC found that the organisation had demonstrated that they were unable to verify the individual's identity to the level of certainty required and that they had provided an additional, alternative valid means for the individual to verify their identity. The DPC considered the actions of the organisation to be a reasonable measure to ensure the security of the sensitive personal data under their control. The DPC concluded the case under section 109(5)(c) of the 2018 Act, advising the individual to consider co-operating with the organisation's efforts to verify their identity, using any of the methods proposed. By so doing, this would enable the organisation to comply with the access request and provide the requested personal data.

KEY TAKEAWAY

- Organisations have an obligation to ensure the security of the personal data which they process. This includes having appropriate verification processes in place to handle Subject Access Requests to ensure that personal data is only released to the appropriate person. The process required to verify a person's identity can vary between organisations. Verification processes can often depend on the type of data which the organisation processes and the sensitivity of the data being requested.

Case Study 14
Erasure request submitted after an unsuccessful job application

The DPC received a complaint regarding a refused erasure request. The complainant had submitted an erasure request under Article 17 of the GDPR seeking the deletion of their personal data relating to an unsuccessful job application. The organisation denied this request, advising that, in line with its retention policy, records relating to recruitment competitions were kept for 12 months. However, the complainant believed that the organisation had failed to identify a valid basis under Article 17(3) of the GDPR, or an exemption, to justify its refusal to erase their data.

The DPC's examination focused on whether or not the organisation had responded appropriately to the complainant's erasure request. The organisation informed the DPC that it was standard practice to retain all information relating to unsuccessful job applications for a period of 12 months, after which the information would be erased. It further explained that its retention of recruitment records for unsuccessful candidates was for the 'defence of a legal claim', and made specific reference to complaints made to the Workplace Relations Commission (WRC) under the Employment Equality Acts. A person who believes they have been discriminated against during a recruitment process, can lodge a complaint with the WRC within six months of the incident of alleged discrimination, with a possible extension of a further six months in certain circumstances.

While the GDPR is not prescriptive with regard to retention policies, data controllers must establish retention periods and be able to justify them. While the organisation was able to direct the DPC to the appropriate policy in place, it had failed to properly rely on Article 17(3)(e) of the GDPR when responding to the complainant's erasure request. 17(3)(e) of the GDPR provides an exemption from granting an erasure request where the information is necessary for the establishment, exercise or defence of legal claims. Where a controller seeks to rely on an exemption to an Article 17 erasure request, it should clearly establish which exemption it seeks to rely on.

Following its investigation, the DPC communicated the organisation's lawful basis for refusing the erasure request to the complainant. The DPC also provided guidance to the organisation in relation to the information that must be communicated to individuals in response to a GDPR Article 17 request, in line with the obligations set out under Article 12 of the GDPR.

KEY TAKEAWAYS

- A data controller may rely on an exemption to restrict a data subject's rights, but it must still respond to that request in full and in line with the obligations under Article 12 of the GDPR.
- Although the GDPR does not mandate specific retention periods, data controllers must be able to justify their chosen retention periods and, where relevant, identify any valid legal basis for continuing to process personal data after the data subject's relationship with the controller has ended.

Case Study 15
Excessive information on sick certs and the importance of transparent policies

An individual contacted the DPC advising that their employer required more health information than was necessary when they took sick leave. They also raised concerns that sick certificates had to be emailed to HR with a member of the finance team copied into the correspondence. The DPC sought clarification from the organisation on the specific information employees were required to provide when absent due to illness, and who had access to that information. The organisation, a charity working with vulnerable individuals, set out that it generally only required confirmation that an employee was unwell. Additional medical details were requested solely where an infectious illness could pose a risk to vulnerable clients, and such information was to be shared directly with the employee's line manager. The additional information was not required by HR and did not need to be included on a sick cert from a GP.

The DPC requested a copy of the organisation's policy to confirm that this distinction was clearly communicated. The DPC found that the policy provided was ambiguously worded, and that the policy suggested additional information should always be provided on sick certificates and with line managers. As a result of this lack of clarity, the organisation was processing unnecessary special category personal data. The DPC engaged with the organisation regarding its obligations under Article 5(1)(a) and Article 13 of the GDPR to ensure transparency and clear information with employees.

The DPC further queried the practice of copying a finance team member on sick certificate submissions. The organisation set out that the finance team required absence dates for payroll purposes. The DPC highlighted that this did not require access to the sick certificate itself. Following this engagement, the organisation conducted a data protection impact assessment and determined that there was no basis for the finance team having access to this information. It subsequently implemented revised procedures to ensure that access to sick leave information is limited to what is strictly necessary.

KEY TAKEAWAYS

- An organisation must ensure that its policies are clear and transparent when requesting personal data, especially special category data. Ambiguous policies risk the collection and processing of information that it does not require.
- Access to employee health information must be appropriate and role specific. Organisations should ensure that assessments are carried out to determine which employees require access to which information in order to carry out their duties.

Case Study 16
Special category data published without a lawful basis

An individual informed the DPC that they had submitted a planning application to a County Council. As part of their submission, they had included a paediatric occupational therapist's report in support of the application. The paediatric occupational therapy report was made publicly available by the County Council.

The DPC raised the matter with the County Council, which confirmed that, while much of the information contained within a planning application must be published in accordance with planning legislation, its policy is to remove any special category data from the published documents. Unfortunately, due to human error, the occupational therapy report was not removed from this application. The County Council confirmed to the DPC that it had removed the report as soon as it was made aware of the matter. The documentation had been available online for a period of approximately four days.

The DPC engaged with the County Council in relation to its obligations to ensure that its staff are fully trained in data protection, and that they understand the additional protection afforded to special category personal data, such as that in an occupational therapy report.

KEY TAKEAWAYS

- Planning legislation requires that planning applications be made available to the public. However, organisations must ensure that any information that is published as part of such application is strictly necessary for the purposes of fulfilling the obligation to publish said documents.
- Organisations must have robust procedures in place to review planning submissions before publication, ensure that staff are trained to recognise sensitive information, and apply the principle of data minimisation effectively.
- Organisations have a responsibility to ensure that there is a lawful basis under the GDPR for any personal data it publishes.

Case Study 17
Request for the erasure of a news article

The DPC received a complaint from an individual regarding an erasure request submitted to a news organisation for the erasure of articles relating to the complainant's criminal conviction. The news organisation had refused the erasure request, and had referenced both the exemption provided under Article 17(3)(a) of the GDPR, which refers to the right of freedom of expression and information, and the exemption provided under section 43 of the Data Protection Act 2018 (the 2018 Act), which is known as the 'journalistic exemption'.

While the exemption from complying with the rights and freedoms set out within the GDPR is intended to be interpreted in a broad manner, the DPC is tasked with ensuring the correct application of such exemptions. Therefore, the DPC considered the circumstances of the complainant's case, and raised the issues concerned with the news organisation. In this instance, the news organisation was able to show that there was a continued public interest in the publication of the complainant's personal data, as the matters that resulted in the complainant's criminal conviction had been brought before the courts very recently. It further stated that the published material was in the court record, the personal data contained therein was accurate, and is publishable information. The organisation reiterated its reliance on Article 17(3)(a) of the GDPR and section 43 of the 2018 Act.

The DPC considered the news organisation's response, giving specific consideration to the fact that Section 43 of the 2018 Act provides a broad exemption from compliance with certain provisions of the GDPR, including the right to erasure under Article 17 of the GDPR. The DPC accepted that the right to freedom of expression and information took precedence over the GDPR in this instance, as the articles in question remained in the public's interest.

When concluding the complaint, the DPC found that the news organisation was justified in their reliance on these exemptions to refuse the erasure request and informed the complainant of this outcome.

KEY TAKEAWAYS

- Section 43 of the 2018 Act provides for a broad exemption from compliance with a rights request submitted by a data subject to a news organisation. However, an organisation that receives such requests and seeks to rely on such exemptions should be in a position to clearly demonstrate to the DPC, upon request, its justification for the application of the journalistic exemption.
- Balancing individual rights with the importance of the freedom of expression and information in a democratic society is an important part of ensuring compliance with the GDPR.

Case Study 18

Disclosure of an individual's personal data by their former employer to third parties without their consent

The DPC received a complaint from an individual regarding the disclosure of their personal data to third parties by their former employer following the termination of their employment. The complainant had been employed at a residential centre and was dismissed after a disciplinary process.

As part of the examination of the complaint, the DPC sought to establish if the organisation had a valid lawful basis under Article 6 of the GDPR for disclosing the complainant's personal data to third parties. In its response, the organisation acknowledged that it could not identify any lawful basis that would justify disclosing the complainant's employment status to the residents.

The DPC also assessed whether the data disclosed was relevant and limited to what was necessary for the stated purpose, in accordance with the principle of data minimisation. The organisation accepted that there was a more appropriate way of notifying residents of the complainant's departure from their role, which would not have disclosed that their employment had been terminated. The organisation further acknowledged that the letter circulated was poorly drafted and disclosed unnecessary information, which subsequently resulted in a failure to limit data to what was necessary in accordance with Article 5(1)(c) of the GDPR.

The DPC reminded the organisation of its obligations, pursuant to Article 6 of the GDPR to identify a lawful basis prior to any processing of personal data it undertakes or plans to undertake. The DPC further referred to Recital 74 of the GDPR, reminding the organisation that it needs to be able to demonstrate the compliance of its processing activities with the GDPR, taking into account the nature, scope, context, and purposes of the processing, and the risk to the rights and freedoms of natural persons.

The organisation accepted responsibility for the unlawful disclosure of the complainant's personal data and implemented appropriate organisational measures, including data protection training, to prevent similar incidents in the future.

KEY TAKEAWAYS

- All organisations that process personal data must be in a position to identify the lawful basis underpinning their processing activities, including the processing of employee data.
- Organisations must apply the principle of data minimisation to all processing activities, to ensure that they only process information that is adequate, relevant and necessary for the purposes for which they are processed.

Rectification Request Case Studies

Article 16 of the GDPR provides individuals with the right to request the rectification of their personal information when it is incorrect or incomplete. An organisation in receipt of such a request should assist the individual in a timely, sufficient and transparent manner.

Case Study 19
Rectification request submitted to a taxation authority

The DPC received a complaint from an individual regarding an application to a taxation authority for a tax exemption based on their medical status. The taxation authority advised the individual that they were not entitled to the exemption, as they had not demonstrated that it was applicable in their circumstance. The individual was of the view this determination was incorrect and submitted a rectification request under Article 16 of the GDPR regarding the determination that they did not meet the criteria for an exemption from tax liability. The tax authority had refused to comply with this rectification request.

Upon receipt of this complaint the DPC engaged with the taxation authority, which responded advising that the complainant had failed to provide any evidence that they met the requirements to avail of the tax exemption. The DPC was informed that the onus of proof is on the applicant and in the absence of any evidence the taxation authority had to determine that the complainant was not entitled to benefit from the exemption. As such, the taxation authority maintained that there was no inaccurate personal data being processed by the authority in relation to the complainant which would be eligible for rectification under Article 16 of the GDPR. Furthermore, the taxation authority informed the DPC that it had advised the complainant on multiple occasions of the options open to them if they disagreed with the authority's decision.

Following its examination, the DPC advised the complainant the right to rectification under Article 16 of the GDPR is not an absolute right and in this instance, as the information held on file was an accurate reflection of the determination made by the taxation authority based on the evidence provided to them by the complainant, the taxation authority was correct to refuse their rectification request.

The DPC informed the complainant that if they disagree with the taxation authority's determination it is open to them to engage in the process, as set out by the taxation authority, by amending their tax returns and claiming the exemption again.

KEY TAKEAWAYS

- When a public authority has made a determination under the legislation governing it, it is not appropriate for an applicant to use a rectification request, under Article 16 of the GDPR, to have this determination overruled e.g.: The DPC cannot make a determination as to whether or not an applicant has sufficiently met the requirements to avail of an exemption; such a determination can only be made by the appropriate body, or via the appropriate appeal mechanisms.

- As with all data protection rights, the right to rectification is not an absolute right. The right must be examined on a case-by-case basis, depending on the nature of the personal data for which rectification is being sought and the purposes for which the personal data was collected.

Case Study 20

Rectification of a report which had been ordered by the Irish Circuit Court

The DPC received a complaint regarding a refused rectification request that had been submitted to a public body under Article 16 of the GDPR. The rectification request related to a report that had been prepared by the public body in response to a request from a District Court judge in a legal matter. The complainant stated that the report contained several inaccuracies.

Upon receipt of this complaint, the DPC contacted the public body to ascertain why this request had been refused. The public body advised the DPC that the legislation under which it compiled the report provided that a Court can direct specific public bodies to carry out investigations and to report back to the court on said investigations. In such circumstances, the public body is acting under the direction of the Court, and therefore it is not the data controller of the report in question. Therefore, it could not act on any Article 16 rectification request. The public body advised the DPC that the individual should make any rectification request in respect of the report to the Court Service of Ireland.

In its response to the individual, the DPC advised them that public body was not in a position to act upon their rectification request as it was not the data controller. The DPC also advised the individual that, should their rectification request to the Court Service of Ireland in respect of this report be refused, it would be open to them to submit a complaint to the assigned judge, as per Section 157(1) of the Data Protection Act 2018.

Article 55(3) of the GDPR sets out that supervisory authorities will not supervise the processing operations of courts when acting in their judicial capacity; this was transposed into Irish law under section 157 of the 2018 Act and provides for an assigned judge to act as the supervisory authority in respect of the courts when acting in their judicial capacity.

KEY TAKEAWAYS

- This case highlights that where an entity is processing personal data on instruction of a judge of any competent court of jurisdiction, that said entity may not be considered to be the controller of that personal data. Consequently, that entity may not be able to act on any request for rectification of personal data under Article 16 of the GDPR.

- Equally, the DPC will not be the competent authority to examine such a complaint from a data subject, as the complaint concerns the processing operations of competent courts of jurisdiction acting in their judicial capacity. In such circumstances, it is open to the data subject to contact the Courts Service of Ireland and, specifically, the current assigned judge, to set out their request for rectification under Article 16 of the GDPR.

Case Study 21
Right to rectification in a medical context

An individual contacted the DPC after their former GP surgery failed to act on an Article 16 of the GDPR rectification request.

The individual had first obtained a copy of their medical records from the GP surgery under Article 15 of the GDPR, and after reviewing them, believed several items related to their personal data were inaccurate.

The individual submitted a rectification request to the surgery to have these alleged inaccuracies corrected. Although the surgery acknowledged the request and provided a timeframe for its completion, the individual received no further communication from the surgery.

Upon receipt of the complaint from this individual, the DPC contacted the surgery to progress the matter. The DPC reminded the surgery of their GDPR obligations as a Data Controller, drawing their attention to Article 12(3) and 12(4) of the GDPR, which outlines:

- the timeframes required for a data controller to respond to requests (one calendar month upon from receipt of the request); and

- a data controller's requirement to provide a valid reason to refuse a request.

In its response to the DPC, the surgery confirmed that it had reviewed the records containing the individual's personal data. Following this review, it had concluded that the entries reflected the clinician's professional medical opinion at the time and, therefore, were not factually inaccurate. The GP surgery advised the DPC that, as the records in question constituted a medical professional's opinion, it did not believe a response was required in this case, given that no data was found to be factually inaccurate. However, the surgery did offer to add a supplementary statement in the individual's records, recording the individual's disagreement.

Following the DPC's intervention, the GP surgery offered an apology to the complainant for the delay in responding to their request. The DPC explained to the individual their rights under Article 16 of the GDPR and that it applies only to factually inaccurate data. Medical diagnosis and clinical notes are considered professional opinions based on the information that is available and are generally not subject to rectification. The individual was informed that medical opinion or diagnosis can provide important context for any subsequent medical treatments and that a supplementary statement can be added where the individual believes the record is incomplete or misleading. The individual rejected the offer of a supplementary statement.

In its final response to the individual the DPC advised that it had found that the surgery had provided a valid reason for refusing rectification and reminded them that the offer to add a supplementary statement stood.

KEY TAKEAWAYS

- The right to rectification is not an absolute right.
- Article 16 of the GDPR allows correction of factually inaccurate or incomplete personal data, i.e. straightforward data (such as names and dates of birth). Clinical notes and diagnoses tend not to fall into this category.
- Medical records are based on professional judgement at a point in time, and are not generally subject to rectification. When rectification is not appropriate, it may still be possible for a supplementary statement to be attached to the medical record to record additional views.
- The DPC cannot determine whether a medical diagnosis is clinically correct and will not substitute its judgement for that of healthcare professionals.

Case Study 22
Rectification of inaccurate personal data

An individual contacted the DPC after an organisation refused their request to have their personal data rectified under Article 16 of the GDPR.

The complainant informed the DPC that they had signed up to become a customer of an energy company when a door-to-door sales agent called to their residence. Upon receiving a welcome pack email from the company, the complainant noted their postal address was incorrectly listed on this email. Separate to this, the complainant decided to terminate the contract with the company within the cooling-off period.

The complainant proceeded to call the company and made a rectification request, under Article 16 of the GDPR, asking for the incorrect postal address to be amended to the correct address. The company responded advising that since the complainant was no longer a customer and no longer had a live account that it would not be possible to amend the address.

The DPC engaged with the company, who responded stating that it had no record of the complainant requesting rectification of the incorrect postal address but that the company had, on the foot of correspondence from the DPC, rectified the address. The complainant disputed the company's claims and provided the DPC with a copy of an email, in which the complainant had previously informed the company that it had the wrong address on file. Furthermore, this email made reference to the Article 16 of the GDPR request the complainant had made to the company.

As part of its examination of the matter the DPC found that, as the information held on the company's records was demonstrably inaccurate, it had an obligation to correct the information without undue delay. The company should have responded to the complainant's request by rectifying the data within the timeframe as set out in Article 12(3) of the GDPR.

In this instance, the company had failed to fulfil its obligation to keep personal data accurate and up to date according to Article 5(1)(d) of the GDPR. It also failed to rectify information that was inaccurate as to a matter of fact within the statutory timeframe set out under Article 12(3) of the GDPR. The DPC engaged with the Data Controller, issuing recommendations to it under section 109(5)(f) of the 2018 Act.

KEY TAKEAWAYS

- When an individual's personal data is inaccurate, and the data subject can provide objective information that demonstrates that the personal data is inaccurate, data controllers are obliged to rectify the inaccurate personal data without undue delay.
- Data controllers must also have appropriate technical and organisational measures in place to process data subject rights, including non-customer requests, as per their obligations under Article 12 of the GDPR.

Data Breach Case Studies

Case Study 23
Allegation of a breach in the financial sector

An individual contacted the DPC claiming that their bank had breached their personal data after they received another customer's information in the post. Although concerned that their own data might also have been disclosed, the individual provided no evidence to support this belief.

The DPC contacted the bank involved for clarification. The bank confirmed that, while an accidental disclosure of a third-party's data had occurred, and the complainant had been the unintended recipient, there had been no breach of the complainant's own personal data. The DPC shared the bank's position with the individual, who remained concerned but was unable to provide any information indicating that their data had been compromised.

Having examined the matter, the DPC was unable to establish an infringement of the GDPR.

KEY TAKEAWAYS

- On occasion individuals may receive correspondence, either via post or electronically, that was not intended for them and which may contain another individual's personal data. In such cases, the DPC advises notifying the sending organisation immediately, and seeking guidance from them on what should be done with the data.
- Receiving another person's information does not automatically mean that the recipient's own data has also been breached.

Case Study 24
Unlawful disclosure of financial information

A family member of a vulnerable adult contacted the DPC after a financial institution sent sensitive financial information about the individual to the residential facility where they were residing. The family member explained to the DPC that the individual lacked capacity to handle their own affairs. The letter in question had been addressed to the residential home where the individual resided but it was not addressed to the individual themselves, resulting in the facility receiving information it was not entitled to access.

The DPC raised the matter with the financial institution. The organisation acknowledged that the correspondence had been incorrectly addressed and confirmed that the letter should have been sent to the individual c/o the residential facility. It accepted that it had no lawful basis for disclosing the customer's sensitive financial data to the residential facility.

The financial institution issued an apology to the affected individual and notified the breach to the DPC. They also reviewed their processes and procedures and circulated a reminder to staff outlining the steps required to prevent similar data breaches in future.

KEY TAKEAWAYS

- Organisations must ensure that all personal data they hold is accurate, current, and regularly reviewed, with clear processes in place to correct any inaccuracies.
- Contact details should always be verified before sending personal information, using checks and confirmation steps to maintain data integrity and protect individuals' personal data.

Case Study 25

Processing more personal data than is necessary, giving rise to the risk of unauthorised disclosure

A breach was notified to the DPC regarding unauthorised disclosure of staff members' sensitive personal data. The human resources unit of the organisation, a public health facility, made available to its staff an attendance rota. Staff members were able to add details of medical-related issues to the rota when making rota change requests. Medical information is considered sensitive personal data. The organisation became aware of the matter when a staff member drew their attention to the information being circulated as part of the staff rota.

The organisation notified the breach to the DPC, following which they conducted an internal investigation. On foot of this investigation a number of issues were discovered, specifically that the rota was not password protected and it contained the personal email addresses of some staff.

Following engagement with the DPC, new measures were implemented by the organisation to ensure only the appropriate level of information was made available and that staff could access the rota using a secured and structured pathway.

KEY TAKEAWAYS

- Organisations need to be mindful of the personal data they process in all contexts. The processing of personal data must be limited to what is necessary, pursuant to Article 5(1)(c) of the GDPR. Organisations must implement appropriate security measures for the protection of personal data, pursuant to Article 5(1)(f) of the GDPR.

  In this instance, while the sensitive personal data was being submitted and added by staff members, the organisation remained responsible for its overall contents.

Case Study 26

Lack of awareness of, and responsibility for, controller obligations in a sports setting

A sports club reported a breach to the DPC regarding an unauthorised disclosure of personal data. An email containing details of a complaint made against one of the coaches was sent to the club Child Safety Officer and was in turn forwarded to one of the coaches of the sports club in error. The email was subsequently read out at a meeting attended by a number of coaches and the sender of the email was also identified.

During the DPC's assessment of the incident, it became evident that the organisation did not have a specific person responsible for data protection matters and there was no formal data protection training or awareness in place. The breach highlighted a deficiency in the process of handling sensitive communications and identified a failure to ensure that emails containing personal information were addressed correctly and sent to individual recipients to prevent unauthorised disclosure.

Following engagement with the DPC, the organisation implemented mitigation measures and has met with the affected individuals regarding the disclosure.

KEY TAKEAWAYS

- All organisations need to be aware of their obligations as data controllers, and while in certain circumstances a verbal disclosure may fall outside the scope of the GDPR, as in this instance, the GDPR did apply as the personal data originated in an email, which constitutes a relevant filing system.
- To ensure compliance with the principle of data minimisation, and to avoid breaches occurring, organisations should ensure only the appropriate level of details are included in correspondence and the 'intended recipient' fields are checked before sending any communications.

Case Study 27

Lack of awareness leading to an inadvertent disclosure in a school setting

A breach was notified to the DPC relating to a secondary school. A student observed a teacher inputting their password into the school's education administration software system. The breach occurred as a result of the student memorising the password and then using it to access the system over a five-month period. Subsequent investigations discovered the breach had occurred 18 months earlier. The school became aware of this incident from a parent and reported it to the DPC within the 72-hour requirement. In the initial breach notification, the organisation could not confirm whether vulnerable individuals were involved or affected, and so it was initially reported as a low-risk breach.

The DPC assessed the breach and determined that the breach was high risk.

This was due to the student being able to access the school's system for a lengthy period of time, and also that there were a significant number of students, with a considerable subset falling into the vulnerable category, affected by the breach. As such, it was further determined that the personal data accessed by the student included special category data as defined by Article 9 of the GDPR.

During the breach assessment it became evident that the school was not familiar with its data protection obligations and had not implemented appropriate technical and organisational measures to ensure the security of the data in its charge. The DPC advised the school of its obligations in line with the GDPR and directed the school to the guidance available on the DPC website to better support them in meeting these obligations. Following engagement with the DPC, the school implemented stronger security processes surrounding access to data processing systems, and introduced updated data protection training for all staff members. The school also issued letters to the parents of all the affected students, outlining how the breach occurred and advising them of their rights under Article 34 of the GDPR.

KEY TAKEAWAYS

- Organisations have a duty to protect the personal data they process by ensuring that they have appropriate measures in place, as required by Article 5(1)(f) of the GDPR. Furthermore, they must ensure that they give particular regard to special categories of personal data and/or where the personal data relates to vulnerable individuals or children, as defined by Article 9 of the GDPR.

  In this instance, there were clear deficiencies in staff training, as well as insufficient monitoring and security around access to systems processing sensitive information.

Case Study 28
Employee uploading Curricula Vitae to Artificial Intelligence (AI) tool

A breach was reported to the DPC relating to an organisation which operates within the financial sector. The organisation had a Data Loss Prevention (DLP) tool in place, and an alert was flagged indicating that 32 Curricula Vitae containing personal data had been uploaded by an employee using their work computer to an external free AI tool. The Curricula Vitae included personal data such as names, contact details, addresses, employment history, references, passport/visa details, and photographs.

The organisation notified the personal data breach to the DPC, as the personal data contained in the Curricula Vitae had been uploaded to a third-party site where there was no data processing agreement in place and the personal data was now no longer under the control of the Data Controller. The organisation advised the DPC that an employee had utilised the free AI tool in an effort to carry out their role more efficiently. The organisation also advised that it had no policies in place around the use of free external tools, including AI.

Upon engagement with the DPC, the organisation agreed to review its policies and provide direction/training to its staff around the appropriate use of external tools in line with data protection best practices.

KEY TAKEAWAYS

- This case highlights the ongoing risk connected to the availability of free AI tools in the context of personal data, and the ease with which these tools can be used without the knowledge of organisations.
- This case further demonstrates the importance of organisations creating appropriate and informed usage policies and, in turn, ensuring that all staff are aware of these policies and of their obligations in relation to data protection.

Case Study 29
Cybersecurity breach via scam call

A breach was reported to the DPC concerning an organisation that operates in the third-level educational sector. An employee of the organisation received a scam phone call to their personal phone while working from home, claiming to be from a national cybersecurity organisation. During the course of this call, the bad actor convinced the employee that their bank account had been compromised.

The employee, on the instruction of the bad actor, downloaded remote viewing software on to a corporate laptop while on their home wi-fi. The employee was signed into their corporate email account on their work laptop at the time of this incident, and the software which was installed by them allowed the bad actors to gain access to the college network in a manner that went undetected. The organisation had no security monitoring system, alert notifications on the enterprise environment, or software in place. Upon investigation, it was determined that no personal data had been detected as being exfiltrated in this incident.

Following the DPC's engagement, the third-level organisation implemented updated cybersecurity and data protection training for all staff, including raising awareness of potential scam calls. Additionally, the organisation introduced improved security and monitoring processes to mitigate the possibility of a re-occurrence of this kind of breach.

KEY TAKEAWAY

- This case illustrates the value of staff awareness and training and the importance of monitoring of systems to prevent unauthorised access by bad actors. It also highlights the importance of having sufficient and effective security in place on corporate systems to prevent and detect unauthorised access.

Case Study 30
Using insecure email systems in the medical field

A breach was reported to the DPC relating to a small GP surgery where a patient had entered an incorrect email address on a form during an appointment, and this email address was recorded without verification. This resulted in email correspondence being sent from the GP's office to an unintended third-party recipient which included the patient's personal data and was sent in an unencrypted format.

The DPC engaged with the surgery, which resulted in the organisation conducting an internal review of their systems. A number of issues were highlighted, specifically that the surgery was using a generic free email account for communication to patients, and that no encryption of content was used in these communications. Following this engagement, the surgery implemented the following measures:

- updated their email systems to a more secure paid service, and ensured that all historical emails were transferred to the new mailing system;
- implemented a process whereby all correspondence, including results, were encrypted;
- introduced staff training for the use of the system and the use of encryption in email communications; and
- commenced the rollout of a secure patient portal. The platform allows patients, with their consent, to access and share documents via a two-factor authentication (2FA) protected login system. Once fully implemented, email will no longer be used for sending patient documents and this platform will significantly enhance the security of patient communications.

KEY TAKEAWAYS

- This case highlights the challenges a smaller enterprise may face in meeting their obligations under the GDPR, and the costs that can be incurred by not updating software technologies. Any security features should be configured appropriately to the nature of the business, and the users of the system should be fully aware of what information is required and necessary, only permitting such personal data as is required to be uploaded.
- Organisations, including smaller enterprises, should have processes in place to ensure that all personal data collected and processed is accurate.

Case Study 31
Loss of official documents highlighting the requirement for secure processes

A breach was reported to the DPC concerning a national regulatory authority. The organisation was notified of a personal data breach following communication from an individual informing them that official documents (in the form of an original official ID and new official documentation) that the individual had expected to receive in the post from the organisation had not been received. After an internal investigation, the documents were deemed to be irretrievably lost.

During assessment by the DPC, it was discovered that the organisation had initially sent the documents by standard post. When the organisation became aware the documents were missing, a registered letter of recovery was sent to the same address. This letter was returned as undeliverable due to an incomplete address being used. The investigation report set out that the individual had submitted a manual application with a handwritten address. Part of this address was missing, though the Eircode used was correct. A replacement of the new official documentation was subsequently issued by registered post to the individual using the full address.

Through its engagement with the organisation, the DPC made recommendations for implementing risk mitigation measures. Following that, the organisation has since confirmed it has adopted multiple updated processes and policies to minimise risk. For example, the organisation has now implemented a policy whereby all documents containing personal data must be sent by registered post.

In relation to verification and security of customer data, a new verification process has since been adopted by the organisation. This system implemented two key changes:

- contact details such as addresses, are now taken from the customer's initial application to the organisation either online or in person. Applicants for the service are no longer required to write an address by hand on an additional application form. The customer is also advised to make the organisation aware of any changes to their address; and

- the submission of original documents is no longer a requirement as scanned copies are now accepted for application purposes.

Additionally, the organisation is currently implementing a 'single customer view/master data record' which will be linked to the various individual databases across the organisation, helping to keep personal data updated and accurate.

The DPO of the organisation has actively partnered with the individual business units and has updated training programmes within the organisation.

KEY TAKEAWAY

- This case highlights the challenges a smaller enterprise may face in meeting their obligations under the GDPR, and the costs that can be incurred by not updating software technologies. Any security features should be configured appropriately to the nature of the business, and the users of the system should be fully aware of what information is required and necessary, only permitting such personal data as is required to be uploaded.

CCTV Case Studies

Case Study 32
Access rights request for CCTV footage

An individual contacted the DPC after an organisation refused their request for personal data – specifically, CCTV footage of an incident involving them on the organisation's premises. The individual also stated that the organisation had not provided any reason for the refusal.

Upon receiving the complaint, the DPC sought clarification from the organisation regarding its reasons for refusing the request. The organisation explained that a copy of the CCTV footage had been provided to An Garda Síochána, and that the individual could obtain the footage directly from An Garda Síochána.

The DPC reminded the organisation of its GDPR obligations. Under Article 15 of the GDPR, organisations must respond to Subject Access Requests within 30 days. If an organisation believes it is justified in withholding the information, it must identify the relevant exemptions being relied on, explain why the exemption applies, and demonstrate that reliance on the exemption is necessary and proportionate. The DPC instructed the organisation to respond to the individual's access request within a set timeframe.

Subsequently, the organisation confirmed that it had provided the requested personal data to the individual and the individual confirmed to the DPC that they had received the requested data without further unwarranted delay.

KEY TAKEAWAY

- This case demonstrates that an organisation must have a legitimate and clearly set out basis to refuse an access request. Simply directing an individual to another body, such as An Garda Síochána, does not remove an organisation's responsibilities under the GDPR if it remains the controller of the personal data. Further guidance for organisations on their obligations regarding Subject Access Requests and CCTV guidance is available on the DPC website.

Subject Access Requests

CCTV guidance

Case Study 33
Commercial CCTV in residential settings

An individual contacted the DPC advising that the owner of the land adjacent to their home had installed a CCTV system, which captured a public road. In their correspondence, the individual advised that two cameras were located on the land: one capturing the land itself; and the other facing a public road and neighbouring residences. The DPC contacted the landowner requesting information relating to the purpose of the CCTV system, as well as confirmation of what was being captured by the cameras. The landowner outlined that the cameras were installed for security reasons, as there had been issues with robbery and vandalism in the past. The landowner confirmed to the DPC that they did not reside on the property, and that it was a commercial farm with livestock and farm machinery. As such, the household exemption did not apply.

In response to queries from the DPC in relation to the lawful basis for processing personal data using the CCTV system, the landowner outlined that they were relying on Article 6(1)(f) of the GDPR (legitimate interests) as the lawful basis for the processing of the CCTV footage.

Article 6(1)(f) of the GDPR states processing is lawful, if necessary for the purposes of the legitimate interests, being pursued by the data controller. To rely on Article 6(1)(f) of the GDPR, data controllers must consider the rights and freedoms of individuals and balance them against the interests of the organisation. However, the landowner did not have a CCTV policy in place at the time of receiving the complaint.

The landowner informed the DPC that once they became aware of the concerns raised by the complainant, they engaged a security expert who installed 'privacy zones' to block the view of all areas that were not the landowner's property. The DPC was satisfied from the evidence provided that all areas not on the landowner's property were sufficiently blocked, and that the complainant's home was not being captured. The camera in question had motion detection capabilities; however, the DPC confirmed that movement based on motion detection did not affect the privacy zones. The landowner further advised that there was a one-month retention period for CCTV footage, and confirmed that they held no recordings of the complainant.

The DPC considered the response from the landowner, including the mitigating actions taken to install privacy zones, and was satisfied from the evidence provided that no data relating to the complainant was retained. The DPC provided further guidance to the landowner in relation to their obligations as the Data Controller operating CCTV, with particular focus on ensuring an appropriate CCTV policy is in place in circumstances where visitors to the property might be captured by the cameras.

KEY TAKEAWAY

- The use of CCTV for security purposes will generally be lawful where it is supported by an appropriate lawful basis for processing, and documented in a comprehensive CCTV policy. This policy should specify a reasonable data retention period and provide individuals with clear information on how they can exercise their data protection rights.
- The DPC's examination of any complaint concerning a CCTV system will first assess whether personal data is being processed. Where privacy zones are configured so that only the controller's property is recorded, and no personal data of passers-by is captured, the DPC's examination of the CCTV system will conclude at that point.
- Further guidance on the use of CCTV can be found here and here.

CCTV guidance

Domestic CCTV

Case Study 34

Request for CCTV footage where requester refused to assist in narrowing scope

An individual complained to the DPC after a large organisation failed to respond to their in person request for CCTV footage of an alleged incident on the organisation's premises.

When contacted, the organisation provided records which demonstrated that it had repeatedly asked the individual to supply essential details, specifically the date, time and exact location of the alleged incident, so it could identify the relevant footage. Despite serval requests, the individual did not provide this information. The individual was also unable to provide this information to the DPC during the complaint process.

While the DPC recommended that the individual supply the requested information, the individual chose not to cooperate with either the organisation or the DPC in identifying when or where the incident occurred, as a consequence of which the DPC could not continue handling the complaint.

KEY TAKEAWAY

- While organisations facilitate rights requests under the GDPR, individuals must provide enough information to allow the organisation to identify the personal data being sought. The DPC expects that individuals engage in the process and supply the details needed to progress their requests.

Case Study 35
Employee concerns around CCTV in the workplace

An individual contacted the DPC in relation to a CCTV system that their employer had installed in the workplace. While the individual had previously raised their concerns with their employer, they were dissatisfied with the response received. The individual was concerned that the CCTV system was being used to monitor employees, that a monitor showing the images was located in a public area where all employees could view it, and that the organisation's managing director had remote access to the CCTV system.

Upon receipt of this complaint, the DPC engaged with the organisation, setting out the importance of recognising an employee's right to privacy in the workplace. In the organisation's response, it stated that the CCTV system had been installed due to concerns around security, that a robust CCTV policy was in place and the system had not been accessed for the purpose of monitoring employees or for disciplinary purposes.

With regard to remote access to the system, the organisation stated that the business owner's home was at the same location as the business, and that the owner's remote access to the CCTV system was exclusively intended for periods when the building was unoccupied, and not during working hours.

The organisation also explained that since the individual had raised the initial concerns, it has since installed clearly visible CCTV signage. This signage also contained information as to the point of contact for employees wishing to gain access to, or receive further information in relation to the processing of, their personal data.

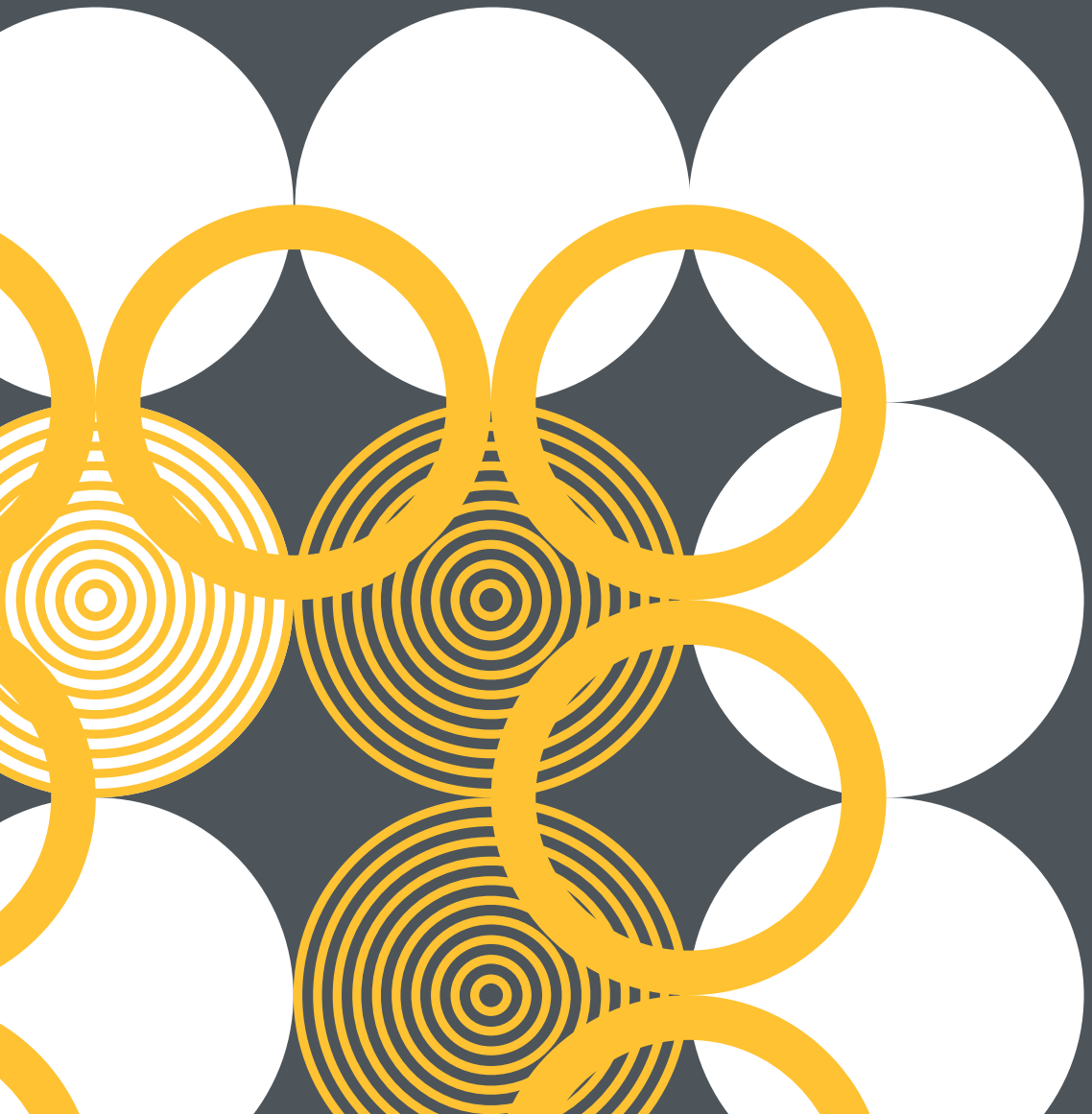
Following the examination of the complaint, the DPC found that although the organisation had identified a lawful basis for operating its CCTV system, it had not adequately considered the security implications of positioning the system where it was visible to all employees. In addition, the circumstances under which remote access to the CCTV system could occur were not clearly defined.

As part of its engagement, the DPC provided the organisation with recommendations and guidance on the use of CCTV in the workplace, including information ensuring it identifies and considers the necessity, proportionality and transparency of processing employee personal data via a CCTV system.

KEY TAKEAWAY

- When operating CCTV systems in the workplace, controllers must ensure that the processing is necessary, proportionate, and transparent, and that it has balanced its employees' right to privacy with its own efforts to ensure safety and security within the workplace.
- Organisations should ensure that cameras and monitors are positioned appropriately, that visible signage is in place, and that a clear CCTV policy (readily available to employees) is in place, setting out the purposes of the system, access arrangements and retention periods.
- More information on this subject matter can be found here:

CCTV Guidance for Controllers



Cross-Border Case Studies

Case Study 36
Cross-border complaint concerning the failure to respond to an access request

An individual contacted a social media company in 2023, requesting access to their personal data. In addition, the individual wanted to know how and when their personal data had been collected by the company and when, if at all, this data might have been transferred to a third party. The individual informed the DPC that other than an automatic acknowledgement from the company to state that their access request had been received, they had not received any other response. That lack of response led the individual to lodge a complaint with the Federal Commissioner for Data Protection and Freedom of Information (BfDI) in Germany. As the DPC is the Lead Supervisory Authority (LSA) for the company within the EU/ EEA area, the complaint was transferred to the DPC for examination through the One-Stop-Shop mechanism.

As part of its complaint handing procedure, the DPC put the complaint to the company. In its reply, the company explained that the individual had made their access request via the company's general 'contact support' channel and, although a process was in place to capture GDPR requests submitted through this channel, it was unable to locate any record of the individual's request. However, the company did accept that the individual's access request may not have been appropriately classified as a GDPR-related request.

On foot of the DPC's engagement, the company reviewed its processes to ensure that the error could not re-occur. In addition, the company also responded to the queries raised by the individual's complaint. The company provided information regarding the delay in the individual receiving their personal data, the individual's request to access their personal data outside of the in-app self-service tools, and further information on all other (i.e. third-party) recipients of the personal data. The company set out the telecommunication providers' names with whom it had shared personal data.

The DPC shared this information with the individual who agreed that their complaint could be closed. This complaint was therefore considered to have been amicably resolved.

Finally, in response to the individual's final follow-up query, the company explained that when a user's account is deleted, any data that had been shared with the third parties, is automatically deleted.

KEY TAKEAWAY

- This case demonstrates how preventable problems can arise where a data controller fails to recognise a valid data subject request—both within its own internal processes, and across the third party bodies with whom it had legitimately shared the individual's data. It further highlights the obligations on companies to respond to data protection requests within the required timeframe, as in the GDPR.

Case Study 37

Cross-border complaint concerning an access and erasure request to an accommodation booking company

An individual contacted an accommodation booking company requesting access to their personal data, pursuant to Article 15 of the GDPR. The company provided the individual with their requested personal data. However, the individual claimed that the company's response was unsatisfactory, stating that the information the company had provided did not contain their personal data from a previous account. As a result, the individual lodged a complaint with the Data Protection Authority of Berlin, Germany. As the DPC is the Lead Supervisory Authority (LSA) for the company within the EU/EEA area, the complaint was transferred to the DPC for examination through the One-Stop-Shop mechanism.

As part of its handling of the complaint, the DPC engaged with the company raising the individual's concerns regarding the data they believed had been omitted from the company's response, which related to a previous account. The company informed the DPC that it was in communication with the individual directly in an effort to resolve their complaint. The company also told the DPC that the individual had submitted a deletion request, to delete '…all existing data on both accounts. The company had advised that DPC that they had deleted the individual's accounts. The DPC then contacted the individual to confirm if they were happy that both their access request, as provided by the company, and their subsequent deletion request, had now been actioned. The individual confirmed that they were satisfied with the outcome of their complaint. As such, this case was closed as 'amicably resolved'.

KEY TAKEAWAYS

- The DPC can assist individuals during the amicable resolution process in explaining their particular requests to a data controller, when previous engagements have been unsuccessful.
- Data controllers should engage in proactive regular testing of organisational and technical processes to ensure compliance with all their obligations under the GDPR.

Case Study 38

Cross-border complaint concerning failure to respond to an erasure request

An individual emailed a multinational tech company in 2025, to request the erasure of their personal data as per Article 17 of the GPDR. The company replied acknowledging the request, and advising that the request would be processed. The company followed up this acknowledgement with a notification advising the individual that they could submit their request via an online form and provided a link. The individual replied that same day advising that they could not make their erasure request in the form provided. The individual then logged a complaint with the Hamburg DPA who in turn transferred it to the DPC in accordance with the One-Stop-Shop provisions.

Upon commencement of the complaint by the DPC, the company acknowledged that the request of the individual had not been handled in a timely manner, contrary to its own procedures. It explained that, due to an internal error, the erasure request was incorrectly processed in a way that resulted in the individual being sent information that was not directly responsive to their erasure request. The company advised that this case was subject to a quality review, and the agent received feedback on their handling of the request and how similar requests should be managed in future. In closing, the company advised the DPC that the individual's account had been deleted, prior to the commencement of the complaint by the DPC.

Through the Hamburg DPA, the DPC was informed that the individual was agreeable to the amicable resolution of their complaint following the confirmation of the erasure of their personal data.

KEY TAKEAWAY

- This case demonstrates that organisations that rely on automated systems / online forms need to conduct regular testing to ensure the technology is operational. This case also illustrates that a proactive approach on the part of data controllers when they receive a data protection request can often resolve matters and avoid the need to engage in a lengthy complaint handling process.

Case Study 39
Cross-border complaint concerning erasure request to gaming company

This complaint concerns an erasure request, as per Article 17 of the GPDR, made by an individual to a gaming company. According to the information provided by the individual, they created a support ticket in 2024 to erase their account. The individual stated that there was no automated tool available for users who want to delete their data, and that the only option available was to open a support ticket. The individual stated that they were asked to verify their identity, despite already having done so through the two-factor authentication beforehand. According to the individual, they were then asked a further 23 'highly technical' questions which were allegedly required in order to confirm their identity. The individual stated that the company refused to comply with their erasure request on the basis that it was not able to verify their identity.

During the complaint handing process, the company informed the DPC that the individual had initiated the account recovery process and not the account deletion process. Subsequently, during a conversation with its support agent, the individual asked for their account to be deleted. The agent then followed the company's procedures to try to authenticate the user as the rightful owner of the account before deleting the account. However, the individual was unable to provide the requested information. The agent then sent the individual a link so they could delete their account. This required the individual to be logged-in at the time. The individual did not use this option.

The company clarified that the individual refused to provide answers to the initial five questions in order to confirm their identity and failed to answer the further 23 follow up questions, which in turn, raised suspicions over the ownership of the account and prevented the deletion. The company clarified that, had the individual provided the company with the required information initially, the agent would have then proceeded with the deletion of the account without the need for further follow-up questions. However, the company advised that it was prepared to delete the individual's account if the individual contacted them from the email address registered with the account. Alternatively, the individual could have proceeded with the automatic deletion using the dedicated tool on the company's website following a link provided.

The individual responded directly to the DPC. In their correspondence, the individual stated that they had tried to use the URL provided by the company and delete their account but were unable to conclude the process in this particular case, as the system did not allow them to proceed. An error message was directing the individual to contact the company's customer support. The individual provided a screenshot of the error message they were getting when trying to use the deletion tool so that the DPC could investigate the matter further.

On foot of this information, the company provided a further response to the DPC's queries and explained that it has since investigated the matter further and could confirm that the account in question contained rare or high-value content. For such accounts, deletion cannot be completed via the automated flow and must be handled manually by its support agents. The company outlined that this safeguard is in place to prevent accidental or malicious deletion of high-value accounts, again reflecting its commitment to security and accountability. This technical limitation meant that, even if the individual had successfully navigated the correct flow, deletion would still not have been finalised without agent intervention. The company confirmed that in light of this, and in the interest of swiftly resolving the individual's request, it was prepared to proceed with deletion of the account manually without further verification.

The company subsequently confirmed to the DPC that the account in question had been deleted. As no further response was received from the individual, this case was closed as 'amicably resolved' in accordance with section 109(3) of the 2018 Act.

KEY TAKEAWAY

- This case underscores the importance of regular GDPR training, particularly for frontline staff, to ensure they can recognise when individuals are exercising their data subject rights.

Notes

Data Protection Commission
6 Pembroke Row
Dublin 2
D02 X963
Ireland

(01) 765 01 00
1800 437 737
www.dataprotection.ie

An Coimisiún um Chosaint Sonraí
Data Protection Commission