CASE STUDIES
2018 – 2023

An Coimisiún um Chosaint Sonraí
Data Protection Commission

Table of Contents

Introduction

The mission of the Data Protection Commission (DPC) is to uphold the consistent application of data protection law through engagement, supervision and enforcement, and driving compliance with data protection legislation. The DPC recognises that a key pillar to success in this mission is to support organisations and drive compliance. In order to achieve this outcome the DPC committed to regularly publish case studies illustrating how data protection law is applied, how non-compliance is identified and how corrective measures are imposed. In the past five years, since the introduction of the General Data Protection Regulation (GDPR), the DPC has published detailed case studies.

Access Request Complaints

CASE STUDY 1

Late response to an access request (Applicable law — GDPR and Data Protection Act 2018)

The General Data Protection Regulation (GDPR) places timelines on data controllers to respond to requests from data subjects when they are exercising their rights. In the case of one data subject who requested a recording of a telephone call conducted between the data subject and the customer-service operator line of a multinational technology company in order to progress a customer-service complaint, a complaint was made to the Data Protection Commission (DPC) that the access request submitted pursuant to Article 15 of the GDPR had not been processed within the timeframe set out by the GDPR.

Upon receipt of the complaint, the DPC contacted the company concerned to make it aware of the complaint and to enquire as to whether there was any action it would like to take on this matter. The company responded to the data subject with a copy of the requested telephone call and, accordingly, the data subject was satisfied for the complaint to be amicably resolved. Based on the circumstances of this individual case, the DPC deemed no further regulatory action necessary.

CASE STUDY 2

Access request to golf club for CCTV (Applicable law — GDPR ad Data Protection Act 2018)

In November 2018, we received a complaint from a data subject in relation to an access request for his personal data comprising CCTV footage for a particular time and date, made to a golf club, the data controller.

The data subject provided us with initial correspondence from the golf club asking him why he required the footage and subsequent correspondence informing him that it had discovered a problem with the CCTV system software and was unable to provide him with the requested footage.

This complaint was deemed potentially capable of being amicably resolved under Section 109 of the Data Protection Act 2018.

As part of the amicable resolution process, we sought an explanation from the golf club as to why the requested CCTV could not be provided to the complainant. The golf club informed us that its CCTV system was not operational on the date for which the data subject had requested footage, and that this had only been discovered when it sought to comply with the access request. The DPC was not satisfied with the generality of this explanation and required a more detailed written explanation on the issues affecting the CCTV, which could also be shared with the complainant. In response to this request, we were supplied with a letter from the golf club's security company that outlined the issues with the CCTV system, including the fact that the hard drive on the CCTV system had failed and that the system had not been in use for some time. The DPC was satisfied with the technical explanation provided and golf club agreed that this letter could be shared with the complainant. The complainant was satisfied with the explanation, leading to an amicable resolution. This case illustrates that even when working towards the facilitation or arrangement of an amicable resolution of a complaint, the DPC still expects account-ability on the part of the controller or processor, and will scrutinise explanations and reasons given as to non-com-pliance with its obligations in order to ensure that the position put forward is verifiable and demonstrable.

CASE STUDY 3

No response received to subject access request (Amicable Resolution)

The DPC received a complaint from an individual regarding a subject access request made by them to a data controller, an auction house whose platform the complainant had used to sell goods, for a copy of all information relating them. No response was received from the data controller despite the individual issuing two subsequent reminders.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018, with both the complainant and data controller agreeing to work with the DPC to try to amicably resolve the matter. The data controller engaged with the DPC on the matter and informed us that while it previously had a business relationship with the individual in 2016, it did not hold any information relating to them as it had installed a new system in May 2018, and no data was retained prior to that. It further informed the DPC that it had shredded all paper files and that its legal adviser's informed them it was not a requirement to retain same.

The data controller also provided the DPC with screenshots from its electronic system of the results of a search against the individual's name, which did not identify any results to display. Article 12(3) of the GDPR states that "the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request."

Having examined the matter thoroughly, it was apparent to the DPC that the data controller contravened Article 12(3) of the GDPR as controllers have an obligation to provide a response to the individual's subject access request within the statutory timeframe as set out in Article 12 of the GDPR, even where the controller is not in possession of any such data.

Regarding the individual's subject access request no further action on this matter was warranted, as there was no evidence to suggest that any data relating to the individual was held by the data controller. The DPC issued advice to the data controller, reminding it of its obligations specifically under Articles 12 and 15 and the requirement to provide information on actions taken in relation to a subject access request, even in circumstances where this is to inform an individual that it does not hold any data.

CASE STUDY 4

Legal Privilege invoked to withhold personal data (Access Request Complaints)

The DPC dealt with a case that concerned an application by an individual to a hospital for their personal data. This individual had instructed their solicitor in relation to a negligence action against the hospital arising from care they received.

By the time the individual made a complaint, the DPC through their solicitor the hospital had released some medical records, but the individual advised that they were awaiting non-clinical notes, which the hospital was refusing to release on the basis that they were subject to litigation privilege. Specifically the individual (who was represented by their solicitor in the complaint to the DPC) was of the view that various staff statements had been withheld. Through the complaint-handling process, the DPC established that staff statements had been prepared in the course of an internal review by the hospital of the care of the patient.

The DPC requested sight — on a voluntary basis — of the documentation withheld from the individual in response to the access request, in order to be satisfied that their contents and eligibility for exemption from release had been validly applied. In circumstances where the statement had been prepared for the dominant purpose of an internal review and no litigation had commenced or been threatened at the date of the creation of the statements, the DPC was not satisfied that litigation privilege applied and directed that they be released.

CASE STUDY 5

Content absent from an access request (Amicable Resolution)

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

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

The individual remained unsatisfied as they had not been provided with a copy of a particular email, which they had sent to the data controller. They stated that it was important for their appeal that they were able to prove that the data controller had received the email in question.

The data controller subsequently provided this office with a report from the company, which hosts its email services showing that the email in question was received but was quarantined as suspected spam and did not reach any of the intended mailboxes nor was it opened by any persons within the organisation.

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

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

Having examined the matter thoroughly, it was apparent to the DPC that the data controller did not comply with its obligations under Article 12(3) of the GDPR as it had an obligation to provide a response to the individual's subject access request within the statutory timeframe, and the data provided to the individual in this case was provided

outside of this timeframe. Regarding the email, which was quarantined by the data controller's system, it was clear that this email was not in existence at the time the access request was made. When making decisions around the quarantine of emails, the controller must have due regard to security obligations in line with Article 32 but also ensure that it does not infringe on the rights of individuals. In this case, there was no apparent right interfered with through the initial quarantine and deletion of the email in question.

CASE STUDY 6

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

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

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

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

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

CASE STUDY 7

Request for footage from online meeting (Access Complaints)

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

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

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

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

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

CASE STUDY 8

Exemptions applied to CCTV footage (Access Complaints)

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

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

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

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

CASE STUDY 9

Failure to respond to an Access Request

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

The complainant was in particular not satisfied with the fact that certain documents had not been provided in response to his access request. The position of the data controller was that the documents were not provided as the personal data had been provided "in another format". Data protection access rights are not about access to documents per se. They are about access to personal data. An access request may be fulfilled by providing the individual with a full summary of their data in an intelligible form. The form in which it is supplied must be sufficient to allow the applicant to become aware of the personal data being processed, check they are accurate and being processed lawfully. Having examined what data the controller did provide in this case, the DPC was satisfied to advise the complainant that he had been provided with all of the data to which he was entitled under data protection legislation.

CASE STUDY 10

Failure to respond to an Access Request (II)

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

By the time the DPC had received the complaint, it transpires that the data controller no longer held any information relating to her as it was not aware of the access request until it was brought to its attention by this office. This was because the email address to which the access request was sent was not an address that was regularly used, despite this being the email address contained in the data controller's Privacy Policy. The data controller further stated that CCTV footage is retained for 14 days due to the system storage capacity and it was therefore not in a position to provide the requested CCTV footage as more than 14 days had elapsed. Having examined the matter thoroughly, it was apparent to this office that the data controller contravened Article 12(3) of the GDPR as controllers have an obligation to provide a response to the individual's subject access request within the statutory timeframe as set out in Article 12 of the GDPR, even where the controller is not in possession of any such data. The failure by the data controller to monitor the inbox associated with the email address in its Privacy Policy resulted in its failure to secure the relevant CCTV footage before it was deleted in line with its retention policy. In this regard, the failure to have relevant organisational measures in place resulted in the data controller being unable to fulfil the subject access request. The DPC issued directions to the data controller reminding it of its obligation to monitor any email mailbox which they provide for data subject requests. The DPC will take enforcement action if a repeat of this issue arises with the same controller.

CASE STUDY 11

Failure to respond fully to an access request

This complaint concerned an access request made by the complainant. The complainant was dissatisfied that his request for access to a copy of any information kept about the complainant by the data controller in electronic and in manual form was refused by the data controller, a County Council. The data controller instead advised the complainant that the requested files were available online or for viewing at the data controller's premises.

During the course of the investigation of this complaint, the complainant alleged that the files made available to the complainant by the data controller at its premises did not constitute all the personal data concerning the complainant that was held by the data controller.

However, the data controller was of the view that the access request made by the complainant was limited to personal data held in relation to two planning applications due to the reference numbers for the planning applications being quoted by the complainant on the complainant's access request. Accordingly, the data controller sought to distinguish between personal data relating to the publicly available planning files, which were supplied to the complainant at a public viewing, and personal data created following the refusal of the complainant's planning application, which the data controller considered to be outside the scope of the access request.

While the complainant mentioned two specific planning applications, the access request was expressed in general terms and sought access to "any information you keep about me electronically or in manual form". Accordingly, it was considered that the personal data sought by the complainant included all data that arose in the context of the complainant's engagement with the data controller prior to submitting the two identified planning applications and all data that arose after those applications were refused.

The data controller, due to the specific circumstances of the case, contravened its data protection obligations when

it failed to supply the complainant with a complete copy of the complainant's personal data in response to the access request within the statutory period. Under GDPR, Article 15 relates to the right of access by the data subject to personal data relating to them that the controller holds. Article 12(3) sets out the condition under which a controller must provide said personal data. There is an onus on a controller to provide information on the action taken under such a request without undue delay and in any event within one month of receipt of the request. There are also conditions set out in this article that provide for this timeframe to be extended.

CASE STUDY 12

Access to CCTV footage

This complaint concerned an alleged incomplete response to a subject access request for CCTV footage made by the complainant to an educational institution. The complainant advised that they were the victim of an alleged attempted assault. The complainant requested access to CCTV footage from the time the alleged assault happened, in particular in relation to a specific identified time period from two different camera angles.

In response to the request by the organisation, a select number of stills from the CCTV footage relating to one camera were provided to the complainant. The complainant requested to be provided with a still for every second of the recording in which the complainant's image appeared. The response received from the educational institution was that all "significant" footage, in the opinion of the controller, had been provided and as the CCTV cameras were on a 30-day recording cycle, the footage had since been recorded over. The controller clarified that it did not store any footage unless there was a "lawful requirement" to do so.

The DPC noted that, when a valid access request is made to a data controller, the request must be complied with by the data controller with a certain period. (Under Article 12(3) of the GDPR, this is generally set at one month). The right of access to personal data is one of the key fundamental rights provided for in data protection legislation. In the context of access requests to CCTV footage, the data controller's obligation to provide a copy of the requester's personal data usually requires providing a copy of the CCTV footage in video format. Where this is not possible, such as where the footage is technically incapable of being copied to another device, or in other exceptional circumstances, it may be acceptable to provide a data subject with stills as an alternative to video footage. However, in such circumstances where stills are provided, the data controller should provide the data subject with a still for every second of the recording in which the data subject's image appears and an explanation of why the footage cannot be provided in video format. The controller should also preserve all footage relating to the period specified until such time as the requester confirms that they are satisfied with the response provided.

As the data controller had not provided the complainant with either the CCTV footage requested or a complete set of the stills relating to the specified period, the data controller failed to comply with its obligations in relation to the right of access, both from a time perspective (Article 12(3)) and regarding the provision of a full and complete set of personal data processed by the controller (Article 15).

CASE STUDY 13

Obligation to give reasons when refusing to provide access to personal data

This complainant previously owned a property in a development managed by a management company. The complainant made a data access request to the management company but was of the view that the data controller failed to provide all of the complainant's personal data in its response.

The management company was determined to be the data controller, as it controlled the contents and use of the complainant's personal data for the purposes of its role as a management company in respect of a development in which the complainant had owned a property. The data in question consisted of (amongst other things) the complainant's name and address. The data was personal data as the complainant could be identified from it and it related to the complainant as an individual.

During the course of the DPC's examination of the complaint, the data controller provided a description of a document containing the complainant's personal data that was being withheld on the basis that it was legally privileged. This document had not been referred to in the data controller's response to the complainant's access request. It was noted that the data controller should have referred to this document and the reason(s) for which it was refusing to provide the document to the complainant in its response to the complainant's access request.

The DPC also considered whether the data controller had supplied the complainant with all of their personal data, as required by legislation. The DPC noted that the complainant had provided specific and detailed descriptions of data they believed had not been provided. In response, the data controller stated that it did not retain data relating to matters that it considered to be closed and had provided the complainant with all of their personal data held by the data controller at the date of the access request. The office was of the view that it was credible that the data controller would not retain personal data on an indefinite basis. The DPC was satisfied that the data controller had provided the complainant with all of their personal data (with the exception of the document over which the data controller had asserted legal privilege, as set out above). For that reason, no further contravention of the legislation had occurred.

Under Article 15 of the GDPR, a data subject has a right to obtain from a data controller access to personal data concerning him or her which are being processed. However, this right does not apply to personal data processed for the purpose of seeking, receiving or giving legal advice, or to personal data in respect of which a claim of privilege could be made for the purpose of or in the course of legal proceedings (Section 60(3)(a)(iv) of the Data Protection Act 2018). Where a data controller refuses to comply with a request for access to personal data, however, it is required under Article 12 of the GDPR to inform the data subject without delay of the reasons for this refusal.

CASE STUDY 14

Confidential expressions of opinion and subject access requests

This complainant made a data subject access request to their employer. However, the complainant alleged that their employer omitted certain communications from its response, wrongfully withheld data on the basis that it constituted an opinion given in confidence and did not respond to the request within the required timeframe as set out in the legislation.

The complainant's employer was the data controller as it controlled the contents and use of the complainant's personal data for the purposes of managing the complainant's employment. The data in question consisted of the complainant's HR file and data regarding the administration of the complainant's employment. The data was personal data because the complainant could be identified from it and the data related to the complainant as an individual.

During the course of the examination of the complaint, the data controller identified additional documents containing the complainant's personal data and provided these to the complainant. In relation to the document, which the data controller had asserted constituted an opinion given in confidence, during the course of the investigation of this complaint, the individual who had expressed the opinion in question consented to the release of the document to the complainant, and so the document was provided by the data controller to the complainant.

Data protection legislation provides a right of access for a data subject to their personal data and, further, that access must be granted within a certain timeframe. Having investigated the complaint, the DPC was satisfied that the data controller had carried out appropriate searches and had provided the complainant with all the personal data, which the complainant was legally entitled to receive.

The documents provided by the data controller to the complainant during the course of the examination of this complaint should have been furnished to the complainant within the timeframe provided for in the legislation.

Under Article 15 of the GDPR, a data subject has a right to obtain from a data controller access to personal data concerning him or her, which are being processed. The data controller must respond to a data subject access request without undue delay and in any event within one month of receipt of the request. However, section 60 of the Data Protection Act 2018 provides that the right of access to personal data does not extend to data which consist of the expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving the information.

CASE STUDY 15

Access requests and legally privileged material

This complaint concerned an alleged incomplete response to a data subject access request. The background to this complaint was that the complainant had submitted an access request to the trustees of a pension scheme (the "Trustees"). As part of its response to the access request, the Trustees referred to a draft letter relating to the complainant; however, this draft letter was not provided to the complainant.

It was established that the Trustees were the data controller as they controlled the contents and use of the complainant's personal data for the purposes of the complainant's pension. The data in question consisted of (amongst other things) information about the complainant's employment and pension and was personal data because it related to the complainant as an individual and the complainant could be identified from it.

The data controller sought to argue that the draft letter was legally privileged and that therefore the data controller was not required to provide it to the complainant. The DPC sought further information from the data controller regarding the claim of legal privilege over the draft letter. In response, the data controller did not clarify the basis on which privilege was asserted over the draft letter, however, it agreed to provide the data to the complainant.

It was decided therefore that the data controller had failed to establish an entitlement to rely on the exemption in respect of legally privileged data. Accordingly, the letter should have been provided to the complainant in response to the complainant's access request within the timeframe set out in the legislation.

Under Article 15 of the GDPR, a data subject has a right to obtain from a data controller access to personal data concerning him or her, which are being processed. The data controller must respond to a data subject access request without undue delay and in any event within one month of receipt of the request. However, the right of access to one's personal data does not apply to personal data processed for the purpose of seeking, receiving or giving legal advice or personal data in respect of which a claim of privilege could be made for the purpose of or in the course of legal proceedings. Where a data controller seeks to assert privilege over information sought by a data subject under Article 15, the DPC, examining a complaint in relation to the refusal, will require the data controller to provide considerable information, including an explanation as to the basis upon which the data controller is asserting privilege, so that the validity of the claim can be properly evaluated.

CASE STUDY 16

Processing in the context of a workplace investigation

The complainant was involved in a workplace investigation arising out of allegations made by the complainant against a colleague. The complainant's employer appointed an independent consultancy firm (the "consultancy company") to carry out the investigation and the findings of the consultancy company were subject to a review by an independent panel.

After the conclusion of the workplace investigation, the complainant made a data access request to their employer and a number of documents were provided in response to this request. However, the complainant was of the view that the request was not responded to fully. For example, the complainant claimed that the witness statements (that had been taken during the investigation) that were provided to the complainant were factually incorrect and that certain documents were not provided to the complainant (such as access logs to the complainant's personnel files). The complainant further alleged that their employer had disclosed details of the complainant's work performance, sick leave arrangements and copies of the complainant's pay slips to the complainant's colleagues. Finally, the complainant claimed that their employer had failed to comply with the complainant's requests for rectification of the witness statements (which the complainant alleged were factually incorrect).

It was established that the complainant's employer was the data controller as it controlled the complainant's data in the context of the workplace investigation. The data in question consisted of the complainant's payroll information, information relating to the complainant's sick leave and witness statements relating to the complainant. The data was personal data because it related to the complainant as an individual and the complainant could be identified from it.

In response to the complainant's allegation that their access request was not responded to fully, the data controller stated that, in relation to the witness statements, the complainant was provided with the copies of the original witness statements that were held on the complainant's file. In relation to the access logs, the data controller was of the view that these did not constitute personal data (because they tracked the digital movement of other employees on the data controller's IT systems). In relation to other miscellaneous documents that the complainant alleged had not been received, the data controller indicated that, if the complainant could specify details of these documents, it would consider the complainant's allegation further.

Regarding the complaint that the data controller had disclosed details of the complainant's work performance to colleagues of the complainant, the data controller argued that the complainant's performance would have been discussed with the complainant's managers and therefore was disclosed for legitimate business reasons. Regarding the complaint around disclosure of details regarding the complainant's sick leave, the data controller noted that was not aware of any such disclosure. Finally, in relation to the allegation that the complainant's payslips were disclosed, the data controller argued that they were provided to an employee of the data controller to be reviewed in the context of a separate case taken by the complainant.

The complainant also made a request for rectification of witness statements, which the complainant alleged, were factually incorrect. However, the data controller advised that what was recorded in the witness statements represented the views of the people involved and, on this basis, refused to amend the witness statements.

The DPC was of the view that there were five issues to be examined by it in relation to the complaint. The DPC's view on each of these issues is summarised below (under headings representing each of the five issues).

Access request

The DPC noted that the complainant had made a valid access request. However, having considered the matter, on balance, the DPC was of the view that there was no evidence available to suggest that the data controller unlawfully withheld information. The DPC noted, however, that the complainant's data access request had not been dealt with in the timeframe required under the legislation. In this regard, the data controller had committed a data protection breach.

Under Article 12(3) of the GDPR, a data subject has a right to obtain from a data controller access to personal data concerning him or her, which are being processed. The data controller must respond to a subject access request without undue delay and in any event within one month of receipt of the request.

Alleged unauthorised disclosure of the complainant's personal data

Controllers must have a lawful basis, under data protection legislation to process personal data, including the disclosure of that data to a third party. In relation to the disclosure of details regarding the complainant's work performance, the DPC was of the opinion that such processing was lawful as it was for legitimate business reasons. Regarding the issue of disclosure of sick leave details, the DPC concluded that it did not have sufficient information relating to the alleged incident in order to determine whether a breach of the legislation had occurred. In relation to the disclosure of the complainant's payslips, the DPC was of the view that the disclosure was lawful. This was because the payslips were disclosed in order to assist the data controller in defending a separate legal claim brought by the complainant, against it.

Under Article 6 of the GDPR, a data controller is required to have a legal basis for processing (including disclosing) any personal data. The available legal bases for processing include (a) that the data subject has given consent, (b) that the processing is necessary for the performance of a contract to which the data subject is a party, (c) that the processing is necessary for compliance with a legal obligation to which the data controller is subject, (d) that the processing is necessary in order to protect the vital interests of an individual, (e) that the processing is necessary for the performance of a task carried out in the public interest, or (f) that the processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party.

Fair processing

There is an obligation on data controllers to process personal data fairly. During the course of its investigation, the DPC asked the data controller to confirm how it complied with its obligations to process the complainant's data in a fair manner, in relation to each of the alleged disclosures of the complainant's personal data. The data controller failed to provide the information required and in these circumstances, the DPC considered that the data controller failed to process the complainant's data, in line with fair processing obligations.

Under the GDPR, personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. That principle requires that the data subject be provided with certain information under Articles 13 and 14 of the GDPR in relation to the existence of the processing operation and its purposes. Data subjects should be made aware of risks, rules, safeguards and tights in relation to the processing of their personal data. Where personal data can be legitimately disclosed to another recipient, data controllers should inform the data subject when the personal data are first disclosed of the recipient or categories of recipients of the personal data.

Right to rectification

Under Data Protection legislation, there is a right to rectification of incorrect personal data. However, here the data controller had confirmed that what was recorded in the witness statements represented the views of the people involved. The view was taken that where an opinion is correctly recorded and where the opinion is objectively based on matters that the person giving the opinion, would reasonably have believed to be true, the right to rectification does not apply.

Under Article 5 of the GDPR, personal data being processed must be accurate and, where necessary, kept up to date and data controllers are required to ensure that every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purpose for which they are processed, are erased or rectified without delay. Under Article 16 of the GDPR, a data subject has the right to obtain from a data controller without undue delay the rectification of inaccurate personal data concerning him or her. However, under section 60 of the Data Protection Act 2018, this right is restricted to the extent that the personal data consist of an expression of opinion about the data subject by another person given in confidence or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving the information.

Retention of the complainant's personal data

The DPC asked the data controller to outline the legal basis for the retention (i.e. processing) of the complainant's personal data relating to the workplace investigation. The data controller advised that this data was being retained in order to deal with the complainant's requests and appeals under various statutory processes. On this basis, the DPC was of the view that the retention of the complainant's personal data was lawful as it was for legitimate business reasons.

Under the GDPR, not only must a data controller have a lawful basis for initially obtaining an individual's personal data, but it must also have an ongoing legal basis for the retention of those data in accordance with Article 6, as set out above. Under Article 5(1)(e) of the GDPR, personal data which is in a form permitting the identification of data subjects must be kept for no longer than is necessary for the purposes for which they are processed.

CASE STUDY 17

Legal basis for processing and security of processing

A data subject lodged a complaint with the DPC against a data controller following a delayed response to a subject access request. The data subject was concerned about the processing of their personal data between the data controller and a third party, a HR investigator (investigator). Such concerns related to the legal basis for processing the data subject's personal data and the security of processing the personal data, as the investigator was using a Gmail account during the course of the examination.

The data subject had exercised their right under Article 15 of the General Data Protection Regulation (GDPR) by requesting access to their personal data. However, they had not received a response to their request within one month as required by Article 12(3) of the GDPR. Following a period of two months and still no response, the data subject informed the data controller that a complaint would be lodged with the DPC. Following the DPC's engagement, the data controller provided the personal data relevant to the subject access request and explained the delay was due to a technical error in the email system. At this stage the data subject was satisfied they had received all personal data requested as well as some additional data. This data did not relate to the data subject and was un-redacted.

Upon review of the personal data received, the data subject raised concerns in relation to the processing of their personal data between the data controller and the investigator. As part of its examination, the DPC engaged with the data controller on this matter. The data controller citied section 46 of the Data Protection Act 2018 (the 2018 Act) and Articles 6(1)(c) and Article 9(2)(b) as their lawful basis for processing the personal data. In addition to this, the data subject was in fact an employee, as such the data controller highlighted their legal obligations under the Safety, Health and Welfare at Work Act 2005 as set out in their Employee Handbook. The data subject challenged this lawful basis as they were not previously made aware of such.

With regard to the investigator the data subject explained that no consent was sought for processing the personal data between the data controller and the investigator. The data controller explained that consent was not the only lawful basis under GDPR and stated Article 6(1)(b) as their lawful basis. The data subject contested this lawful basis stating the processing of personal data by the investigator was not necessary for compliance with the employment contract. The data subject also raised transparency concerns as when signing the employment contract they would not have anticipated the processing of their personal data by an investigator. When questioned on the use of a Gmail account by the investigator, the data controller stated the email would be encrypted between the data controller and the Gmail account and that no evidence was available of the data subject's personal data being compromised.

During the examination of the complaint the issue arose about whether the investigator was a joint controller or a data processor. The data subject took the view that the investigator was a data processor while the data controller stated the investigator was a data controller in their own right and as a result there were no requirements under Article 28 of the GDPR. The DPC examined the facts in this complaint and established that the investigator was provided a list of individuals to interview in order to compile this report and from the terms of reference, interviews are listed as the primary means of gathering information to compile their report. The DPC also noted the investigator was precluded from deciding on or implementing any sanction arising from the findings of the report. Based on this information, the DPC found the investigator as a data processor on behalf of the data controller and noted that the data controller failed to provide a contract between them and the investigator as required under Article 28(3) of the GDPR.

Due to the failure of the data controller to comply with the one-month obligation under Article 12(3) of the GDPR, the DPC reminded the data controller of their obligations under Article 24 to implement appropriate technical and organisational measures to ensure compliance with the GDPR. In doing so the data controller should also ensure they only provide personal data relevant to the subject access request at hand and redact the personal data of third parties. Secondly, with regard to the lawful basis relied upon by the data controller the DPC were satisfied that such lawful basis were reasonable; however recommended they inform staff members in their staff data protection policies that they may rely on section 46 of the 2018 Act and Articles 6(1)(c) and 9(2)(b) of the GDPR for the processing of staff personal data. In addition to this, under section 109(5)(f) of the 2018 Act the DPC recommended the data controller ensures there is a contract in place when an investigator is involved, that they engage in regular testing of organisational and technical processes, and lastly provide the investigator with an organisation email address.

CASE STUDY 18

Access to information relating to a bank's credit assessment

The complainant in this complaint made a request to a bank under data protection legislation to supply the complainant with a copy of all personal data relating to them held by the bank. The complainant alleged, in particular, that the bank had failed to provide them with any internal analyses which used the complainant's personal data to assess the amount of credit the bank would extend to them.

This office established that the bank was identified as the relevant data controller in relation to the complaint, as it controlled personal data, which the complainant provided to the bank when making a loan application. The data in question was personal data relating to the complainant (consisting of, amongst other things, a completed loan application form and supporting documentation) as the complainant could be identified from it and the data related to the complainant as an individual. This office was therefore satisfied that the complaint should be investigated to determine if a breach of data protection legislation had occurred.

During the course of the investigation of this complaint, this office engaged with the bank regarding the nature of any personal data to which the complainant might have been entitled. The bank took the view that the complainant was not entitled to details of its internal analysis and algorithms or any internal decision thresholds upon which it based its lending decision as, in the view of the bank, this information was not personal data, and, in addition, was market sensitive and was the intellectual property of the bank. In particular, the bank did not provide the complainant with details of the complainant's credit score or the bank's calculation of the complainant's net disposable income, which form part of its credit assessment criteria.

This office considered the explanations provided by the bank and took the view that the complainant's net disposable income figure and credit scope both constituted personal data relating to the complainant as the complainant could be identified from the details and they related to the complainant as an individual. Furthermore, as the bank had not identified a relevant exception under data protection legislation on which it could withhold this data from the complainant, this office considered that the bank had failed to comply with the complainant's request for access to their data. However, this office agreed that the credit scoring models used by the bank in its credit assessment process were not personal data relating to the complainant and that, as such, the complainant was not entitled to a copy of this information.

Finally, this office considered that the bank had further contravened its obligations under data protection legislation by failing to respond to the request made by the complainant within the applicable statutory time limit.

Under Article 15 of the GDPR, data subjects have a right to obtain from data controllers confirmation as to whether or not personal data concerning them are being processed and, where that is the case, access to that personal data. This right only extends to the personal data of the data subject, meaning any information relating to that data subject by which the data subject is identified or identifiable. The data controller must respond to a data subject access request without undue delay and in any event within one month of receipt of the request. However, the right of access to personal data is subject to a number of exceptions under the GDPR and the Data Protection Act 2018 (in particular, sections 59 to 61), such as where compliance with the request for access would adversely affect the rights and freedoms of others.

CASE STUDY 19

Disclosure, withdrawing consent for processing and subject access request

A data subject brought a complaint to the Data Protection Commission (DPC) against their former employer (the data controller). The data subject had a number of data protection concerns namely:

1. The disclosure of their personal email address in a group email by being included in the Carbon Copy (CC) field,
2. The inclusion of their image on the data controllers social media,
3. The data subject was not satisfied to the response received from the data controller regarding a subject access request.

In line with the examination of the complaint, the DPC contacted the data controller and shared the details of the complaint. The data controller informed the DPC that the data subject had previously signed a settlement agreement, which waived their right to make any complaints or claims against the company under the Data Protection Acts 1988, 2003 and 2018. In response, the DPC advised the data controller that they were not a party to that agreement and that the DPC has a statutory obligation to examine complaints to the extent appropriate. An enforcement of any settlement agreement is a matter between the data controller and data subject.

In relation to the disclosure of the data subject's email address in a group email, the data controller acknowledged that the Blind Carbon Copy (BCC) function should have been used in this instance. The data controller also advised that this incident had been reported to the DPC as a breach under Article 33 of the General Data Protection Regulation (GDPR) and additional measures have been put in place to avoid the incident re-occurring. Staff training has been rolled out and the data subject's email address has been removed from the auto-collected email addresses on file. The DPC noted that the circumstances of the breach arose as a result of human error and has not been identified as a systemic issue.

Under Article 17 of the GDPR, the data subject requested the removal of their image from the data controller's social media outlets without undue delay. The data subject withdrew their consent for the processing of their personal data under Article 17(1)(b) of the GDPR. The data controller conducted a search of their social media and removed any posts, which identified the data subject. The data controller advised that where third parties further used these images, the data subject would have to submit an erasure request to these organisations directly.

The data subject also made a subject access request under Article 15 of the GDPR to the data controller. The data controller complied with the request; however, restrictions were applied under Section 162 of the 2018 Acts to restrict the data subject's access to correspondence between the data controller and their legal advisors. While the DPC notes that a right of an individual to access personal data is a fundamental right and any restriction must be interpreted narrowly, the requirement that the restriction of data subjects' rights be necessary and proportionate, is not contained within section 162 of the 2018 Act. Accordingly, not all access requests can be complied with and based on the information provided to the DPC, the DPC found that the correspondence between the data controller and their legal advisers should not be released in response to a data subject access request.

Further to the above, the DPC noted that the data controller had failed to comply with their obligations under Article 12(3) of the GDPR in that, data controllers must respond to data protection requests from data subjects within one month of receiving those requests. A data controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. However, it was noted that the data controller extended the response period of the subject access request after the initial one-month time period had lapsed.

As such, under section 109(5)(f) the DPC wrote to the data controller and reminded them of their obligations under Articles 12(3) and Article 33 of the GDPR.

CASE STUDY 20

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

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

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

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

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

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

- **Article 5(1)(c) of the GDPR**
  The DPC found that Airbnb's requirement that the complainant verify their identity by way of submission of a copy of their photographic ID constituted an infringement of the principle of data minimisation, pursuant to Article 5(1) (c) of the GDPR. This infringement occurred in circumstances where less data-driven solutions to the question of identity verification were available to Airbnb;
- **Article 6(1) of the GDPR**
  The DPC found that, in the specific circumstances of this complaint, the legitimate interest pursued by the controller did not constitute a valid lawful basis under Article 6 of the GDPR for seeking a copy of the complainant's photographic ID in order to process their erasure request; and
- **Article 12(3) of the GDPR**
  The DPC found that Airbnb infringed Article 12(3) of the GDPR with respect to its handling of the complainant's access request. This infringement occurred when Airbnb failed to provide the complainant with information on the action taken on their request within one month of the receipt of the access request.

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

Accuracy

CASE STUDY 21

Right to rectification request to a healthcare group (Applicable Law — GDPR and Data Protection Act 2018)

We received a complaint against a healthcare group arising from its refusal of a request for rectification under Article 16 of the General Data Protection Regulation (GDPR). The complainant alleged that the healthcare group was incorrectly spelling his name on its computer system by not including the síneadh fada, an accent that forms part of the written Irish language.

Hospitals under the administration of this healthcare group use a patient administration system (PAS) to initially record patient data which is then shared with other systems at later points of patient care, that is, laboratory, radiology and cardiology. The healthcare group informed the complainant that it is not possible to record the síneadh fada because syntax characters are recorded as commands on the PAS, impacting on the way data is stored and processed. The healthcare group informed the Data Protection Commission (DPC) that the patient administration system is due to be replaced in 2019/2020. However, the group's new system will not allow for the use of the síneadh fada. The healthcare group informed the DPC this was for the purpose of enabling a streamlined single point of contact for patient information across different systems. This would enable professionals to access this information across different units within a hospital or hospital group without re-entering the data at a later point, thereby avoiding potential for later errors. The other systems across the current healthcare group network and/or wider hospital network do not support the use of the síneadh fada. The healthcare group further advised the DPC that they identify patients with Patient ID numbers rather than isolated names.

The DPC examined this submission and concluded that any update of the computer system would lead to costs in terms of significant costs and time, along with errors in storage and matching of records. The DPC also engaged with An Coimisinéir Teanga (Irish Language Regulator) about its advice to public sector organisations with respect to computer systems supporting the síneadh fada. An Coimisinéir Teanga advised there is no such obligation arising from the Official Languages Act 2003 but such an obligation can arise from a language scheme — an agreement put in place between a public body and the Minister for Culture, Heritage and the Gaeltacht.

The DPC queried the healthcare group on the existence of a language scheme and was provided a copy. This scheme sets out a respect for patient choices regarding names, addresses and their language of choice. The scheme also provides a commitment to update computer systems to achieve "language compliancy". There is no timeframe provided for the fulfilment of this commitment in the language scheme.

The healthcare group advised the DPC they are committed to patient safety as a primary, core concern and further advised the DPC of the difficulties associated with sharing and storing information across other systems

if they updated their system to allow for the use of the síneadh fada. They also advised that they will be testing the possibility of using the síneadh fada in any update of their computer system.

The DPC had regard to Article 16 and Article 5(1) (d) of the GDPR in examining this complaint. Both articles set out the rights of individuals subject to "the purposes of the processing". The right to rectification under Article 16 of the GDPR is not an absolute right. Organisations that control or process personal data are required to take reasonable steps in the circumstances. The DPC had regard to case law from the European Court of Human Rights on linguistic rights and/or naming. This case law reflects that the spelling of names falls under the ambit of Article 8 of the European Convention on Human Rights but that the Court adopts a restrictive approach in this regard. As such, the DPC reiterated the purpose of the processing in the circumstances of the complaint was the administration of health care to the complainant and involved the use of Patient ID numbers. The name of the complainant was not the isolated means of identification and therefore the purpose of the processing is being achieved without the use of diacritical marks.

The DPC had regard to any risks to the complainant in the refusal of their Article 16 request also. The DPC noted the risk to the complainant would increase because of the difficulties associated with cross-system handling of the síneadh fada and the impact this would have on any health care decision making for the individual. In the circumstances, the non-use of the síneadh fada would not constitute an interference with the fundamental rights of the individual.

Under section 109(5) (f) of the Data Protection Act 2018 (the 2018 Act), the DPC requested the healthcare group to inform the complainant of its actions in the implementation of a computer system enabled to reflect the síneadh fada. Also, the DPC requested that the group add an addendum to the individual's file to show the síneadh fada forms part of the individual's name. The DPC, under section 109(5)(c) of the 2018 Act, advised the complainant that he may contact An Coimisinéir Teanga about the language scheme and any contravention of same.

CASE STUDY 22

Inaccurate Information held on a banking system

The complainant in this instance held a mortgage over a property with another individual. The complainant and the other individual left the original property and each moved to separate addresses. Despite being aware of this, the complainant's bank sent correspondence relating to the complainant's mortgage to the complainant's old address, where it was opened by the tenants in situ.

In response, the complainant's bank noted that its mortgage system was built on the premise that there would be one correspondence address and, in situations where joint parties to the mortgage no longer had an agreed single correspondence address, this had to be managed manually outside the system, which sometimes led to errors.

It was apparent that the data controller for the purposes of the complaint was the complainant's bank, as it controlled the complainant's personal data for the purposes of managing the complainant's mortgage. The data in question consisted of (amongst other things) financial information relating to the complainant's mortgage with the data controller. The data was personal data because it related to the complainant as an individual and the complainant could be identified from it.

Data protection legislation, including the GDPR sets out clear principles that data controllers must comply with when processing a person's personal data. Of particular relevance to this claim was the obligation to ensure that the data is accurate and kept up to date where necessary, and the obligation to have appropriate security measures in place to safeguard personal data.

In applying these principles to the facts of this complaint, by maintaining an out-of-date address for the complainant and sending correspondence for the complainant to that address, the data controller failed to keep the complainant's personal data up to date (Article 5(1)(d)). In addition, given the multiple pieces of correspondence that were sent to the wrong address, the data controller's security measures failed to appropriately safeguard the complainant's data (Article 5(1)(f). The obligation to implement appropriate security measures under Article 5(1)(f) is to be interpreted in accordance with Article 32 of the GDPR, which sets out considerations that must be taken into account by a data controller when determining whether appropriate security measures are in place.

CASE STUDY 23

Proof of identification and data minimisation

The DPC received a complaint, via the Berlin Data Protection Authority, from an individual regarding a request they made to a data controller to have the email address associated with their customer account changed. The complainant had made the request via the data controller's online chat function and was subsequently informed that a copy of an ID document to authenticate account ownership would be required in order to proceed with the request. The complainant refused to provide this information and their request was therefore not progressed by the data controller at that time.

Following receipt of the complaint, the DPC engaged with the data controller during which it was established that the data controller does not require individuals to provide an ID document in order to change the email address associated with an account. Furthermore, the customer service agent had used an incorrect operating procedure when responding to the request of the complainant. The data controller's standard procedure directs customer service agents to advise customers that they can change their email address by signing into their own account and making the change directly within their 'Account' settings page. The data controller also advised that if a customer does not wish, or is not able, to change their email address on their own, its procedure directs customer service agents to request limited information from the customer which is already held by them, in order to verify the account holder.

In light of the complaint, the data controller agreed to provide clear instructions on how the complainant could change their email address associated with their account information without providing any additional personal data. The data controller also conducted a thorough review of its customer service systems and provided further refresher training to all of its customer service agents on the correct standard operating procedures to follow in such instances.

The DPC then engaged with the complainant, via the Berlin Data Protection Authority, to provide the information it had received from the data controller in an attempt to facilitate an amicable resolution to the complaint. The complainant subsequently confirmed to the DPC that they had successfully changed the email address on their account with the data controller.

This case study demonstrates the benefits to both data controllers and to individual complainants of engaging in the amicable resolution process in a meaningful way. In this case, the positive actions taken by the data controller, including providing detailed information to the complainant on how to proceed themselves with changing the email address associated with their account, resulted in a good outcome for both parties.

CASE STUDY 24

Data accuracy

The complainant in this case had made a complaint to a professional regulatory body about the conduct of a regulated person. That complaint was not upheld by the professional regulatory body. In his complaint to the DPC, the complainant alleged that the professional regulatory body had inaccurately recorded personal data relating to them in the minutes of its meeting. The complainant also alleged that the professional regulatory body had inaccurately recorded the same personal data relating to the complainant in a letter from it to a third party.

Before commencing an investigation into this complaint, the DPC reviewed the information provided and established that the professional regulatory body was identified as the relevant data controller in relation to the complaint, as it controlled the contents and use of the complainant's personal data for the purposes of investigating the complaint. The data in question was personal data relating to the complainant, the complainant could be identified from it and the data related to the complainant as an individual. The DPC was therefore satisfied that the complaint should be investigated to determine if a contravention of data protection legislation had occurred.

During the course of the investigation of this complaint, the professional regulatory body accepted that the personal data in question had been recorded inaccurately and, in relation to the data recorded in the minutes, corrected the data by way of the insertion of a clarification. On this basis, this office considered that the personal data recorded in the meeting minutes and the letter to the third party had been recorded inaccurately, in contravention of data protection legislation.

This office also examined whether the professional regulatory body had processed the complainant's personal data fairly, as required by data protection legislation. In order to comply with the requirement to process personal data fairly, data controllers must ensure that data subjects are provided with or have made readily available to them certain information. This office reviewed the information that the professional regulatory body stated was available to individuals about making a complaint, in the form of the information booklet. This booklet did not contain, in particular, any details about individuals' right of access to personal data relating to them and individuals' rights to rectify inaccurate data concerning them. Since the information booklet did not contain all of the information that was required to be provided to data subjects under data protection legislation and since the professional regulatory body did not provide any other details regarding other measures that it had in place at the relevant time to address its fair processing obligations, the DPC was not satisfied that the professional regulatory body had complied with its fair processing obligations.

Under the GDPR, data controllers must ensure that personal data are accurate and, where necessary, kept up to date, and every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. Under Article 16 of the GDPR, a data subject has the right (subject to certain exceptions) to obtain from the data controller without undue delay the rectification of inaccurate personal data concerning him or her.

The GDPR also requires that personal data be processed fairly and in a transparent manner. A data controller should provide a data subject with any information necessary to ensure fair and transparent processing, taking into account the specific circumstances and context in which the data are processed. In particular, where personal data are collected from a data subject, Article 13 of the GDPR requires that the data controller provide the data subject with, amongst other things, information as to the identify and contact details of the controller and its data protection officer (where applicable), the purpose of the processing, the recipients or categories of recipients of the data and information as to the rights to rectification and erasure of personal data.

Cross-border Complaints

CASE STUDY 25

Handling an Irish data subject's complaint against German-based Cardmarket using the GDPR One Stop Shop mechanism (Applicable law — GDPR and Data Protection Act 2018)

The Data Protection Commission (DPC) received a complaint from an Irish individual against Cardmarket, a German e-commerce and trading platform. The individual received an email from Cardmarket, notifying them that it had been hacked and that some of its users' personal information may have been leaked. The individual alerted the DPC and submitted a complaint in relation to the breach.

Under the One Stop Shop (OSS) mechanism created by the General Data Protection Regulation (GDPR), the location of a company's main European establishment dictates which European authority will act as the lead supervisory authority in relation to any complaints received. Once the lead supervisory authority (LSA) is established, the authority that received the complaint acts as a concerned supervisory authority (CSA). The CSA is the intermediary between the LSA and the individual. Among other things, the reason for this separation is so that supervisory authorities can communicate with individual complainants in their native language. In this case, the Berlin Data Protection Authority (DPA) acted as the LSA, as the company had its main establishment in the Berlin territorial area. The DPC acted as a CSA, communicating with the Berlin DPA and transmitting updates in relation to the investigation (once they were translated from German to English) to the individual complainant in Ireland.

The Berlin DPA concluded its investigation into the breach and the individual's complaint. It uploaded two draft decisions, one in relation to the overall breach which impacted many other users of the platform throughout Europe, and another in relation to the specific complaint which had been lodged by the Irish individual with the DPC and communicated to the Berlin DPA.

An important aspect of the OSS mechanism is that a CSA may comment on a draft decision issued by a lead supervisory authority. This is to ensure that European supervisory authorities are applying the GDPR consistently i.e. that a final decision reached by the Berlin DPA would have the same conclusion as a decision of the DPC if the company had been located in Ireland and the DPC had investigated the complaint as the lead supervisory authority. The DPC were satisfied with the Berlin DPA draft decisions and did not consider it necessary to raise any points of clarification or requests for amendment on this occasion.

The draft decision in relation to the overall breach described a number of measures taken by the platform to address the breach and mitigate its adverse effects. The measures included taking its servers off of their network and deleting all the data on them, as well as resetting all user passwords and ensuring new passwords were encrypted with the latest hashing methods. The draft decision considered that a repetition of the incident was unlikely, and that the mass disclosure of passwords

had been rendered practically impossible in light of the measures taken.

The DPC informed the individual of the outcome of the Berlin DPA's investigation, providing them with a copy of the overall decision investigating the breach and the decision dealing with their specific complaint.

This case illustrates the challenging handoffs and handovers involved in the OSS mechanism established by the GDPR. It demonstrates the depth of cooperation between European supervisory authorities required for the consistent application of the GDPR in Europe.

CASE STUDY 26

The Operation of the Article 60 Procedure in Cross-Border Complaints: Groupon

The DPC received a complaint in July 2018 from the Polish data protection authority on behalf of a Polish complainant against Groupon International Limited ("Groupon"). The complaint related to the requirements that Groupon had in place at that time to verify the identity of individuals who made data protection rights requests to it. In this case, the complainant alleged that Groupon's practice of requiring them to verify their identity by way of electronic submission of a copy of a national identity card, in the context of a request they had made for erasure of personal data pursuant to Article 17 of the GDPR, constituted an infringement of the principle of data minimisation as set out in Article 5(1) (c) of the GDPR, in circumstances where there was no requirement to provide an identity document when a Groupon account was created. In addition, the complainant alleged that Groupon's subsequent failure to act on the erasure request (in circumstances where the individual objected to providing a copy of their national identity card) constituted an infringement of their right to erasure under Article 17.

The DPC commenced an examination of the complaint upon receipt of same. In the course of its correspondence with Groupon on the matter, it became clear that Groupon's policy of requiring a requester to provide a copy of a national identity card, which had been in place since before the GDPR came into force (and which was in place at the time of the complainant's erasure request), had been discontinued since October 2018. In its place, Groupon had implemented an email authentication system which allowed Groupon users to verify their account ownership. The DPC attempted to amicably resolve the complaint (pursuant to section 109(2) of the Data Protection Act 2018), but the complainant was unwilling to accept Groupon's proposals in respect of same. As such, the matter fell to be decided by way of a decision under Article 60 of the GDPR.

(i) Initial Draft Decision

The first step in the Article 60 process entailed the DPC preparing a draft decision in respect of the complaint. In its initial draft decision, the DPC made findings of infringements of Articles 5(1)(c) and 12(2) of the GDPR by Groupon. The DPC provided the draft decision to Groupon to allow it to make submissions. Groupon subsequently provided a number of submissions, which (along with the DPC's analysis thereof) were taken into account in a further version of the draft decision.

(ii) Provision of Initial Draft Decision to Concerned Supervisory Authorities

The second stage in the Article 60 process involved the DPC's initial draft decision being uploaded to the IMI to be circulated amongst the Concerned Supervisory Authorities (CSAs), pursuant to Article 60(3) of the GDPR. The DPC's draft decision was uploaded to the IMI on 25 May 2020 and, pursuant to Article 60(4) of the GDPR, CSAs were thereafter entitled to four weeks in which to submit any relevant and reasoned objections to the decision. The DPC subsequently received a number of relevant and reasoned objections and comments on its decision from CSAs. In particular, certain CSAs argued that additional infringements of the GDPR ought to have been found, and in addition that a reprimand and/or administrative fine ought to have been imposed.

(iii) Revised Draft Decision

The next stage of the Article 60 process required the DPC to carefully consider each relevant and reasoned objection and comment received in respect of its draft decision, and incorporate its analysis of same into a revised draft decision. In revising its draft decision, the DPC followed certain relevant and reasoned objections received,

and declined to follow certain relevant and reasoned objections. The DPC's revised draft decision, taking into account its analysis of the relevant and reasoned objections and comments in respect of its draft decision, found additional infringements of Articles 17(1)(a) and 6(1) of the GDPR by Groupon. In addition, the DPC proposed in its revised draft decision to issue a reprimand to Groupon, pursuant to Article 58(2)(b) of the GDPR. The DPC provided its revised draft decision to Groupon to allow it to make final submissions. A number of final submissions were received from Groupon, which (along with the DPC's analysis thereof) were taken into account in the DPC's revised draft decision.

(iv) Provision of Revised Draft Decision to Concerned Supervisory Authorities

The next stage of the Article 60 process entailed the DPC uploading its revised draft decision to the IMI, for circulation among the CSAs. Under Article 60(5) of the GDPR, CSAs were entitled to two further weeks in which to indicate if they planned to maintain their objections. This raised the prospect that the Dispute Resolution procedure under Article 65 of the GDPR would have to be engaged, which would have involved the European Data Protection Board (EDPB) adjudicating on the point(s) of disagreement, and which would have extended further the time in which the decision in respect of the case could be completed. However, the additional query was subsequently withdrawn.

(v) Adoption of Final Decision

Upon the withdrawal of the final relevant and reasoned objection, and the passing of the deadline for receipt of any further objections, the last stage of the Article 60 process entailed the DPC adopting the final decision, which was uploaded to the IMI and communicated to Groupon. The final decision was uploaded on 16 December 2020. As per Article 60(6) of the GDPR, the CSAs were deemed at this point to be in agreement with the decision and to be bound by it. Pursuant to Article 60(7), the Polish data protection authority with which the complaint was initially lodged was responsible for informing the complainant of the decision.

In summary, the DPC found infringements of the following Articles of the GDPR in respect of this case: Articles 5(1)(c), 12(2), 17(1)(a) and 6(1). This case study demonstrates that, where a cross-border data protection complaint cannot be amicably resolved, the Article 60 procedure that follows as a result is particularly involved, complex and time-consuming, especially as the views of other supervisory authorities across the EU/EEA must be taken into account and carefully considered in all such cases. In this case, following the completion of the investigation of the complaint, the initial draft of the DPC's decision was uploaded to the IMI on 25 May 2020, and the final decision — incorporating submissions from Groupon, relevant and reasoned objections and comments from CSAs, and the DPC's analysis thereof — was adopted on 16 December 2020, some seven months later.

CASE STUDY 27

Amicable Resolution in Cross-Border Complaints: MTCH

The DPC received a complaint in June 2020, via its complaint webforms, against MTCH Technology Services Limited (Tinder). Although the complaint was made directly to the DPC, from an Irish resident, upon assessment it was deemed to constitute a cross-border complaint because it related to Tinder's general operational policies and, as Tinder is available throughout the EU, the processing complained of was therefore deemed to be of a kind "….which substantially affects or is likely to substantially affect data subjects in more than one Member State" (as per the definition of cross border processing under Article 4(23) of the GDPR).

The complaint related to the banning of the complainant from the Tinder platform, subsequent to which the complainant had made a request to Tinder for the erasure of his personal data under Article 17 of the GDPR. In response to his request for erasure, the complainant was referred by Tinder to its privacy policy for information in relation to its retention policies in respect of personal data. In particular, Tinder informed the complainant that "after an account is closed, whatever the reason (deletion by the user, account banned etc.), the user's data is not visible on the service anymore (subject to allowing for a reasonable delay) and the data is disposed on in accordance with [Tinder's] privacy policy". The complainant was dissatisfied with this response and followed up with Tinder again requesting the erasure of his personal data. Tinder responded by reiterating that "…personal data is generally deleted "upon deletion of the corresponding account", further noting that deletion of such personal data is "only subject to legitimate and lawful grounds to retain it, including to comply with our statutory data

retention obligations and for the establishment, exercise or defence of legal claims, as permitted under Art. 17(3) of GDPR." The complainant subsequently made his complaint to the DPC.

Upon the DPC's engagement with Tinder in respect of this complaint, Tinder informed the DPC that the complainant had been banned from the platform as his login information was tied to another banned profile. Also, Tinder identified eleven other accounts associated with the complainant's device ID. All these accounts had been banned from the Tinder platform as it appeared that an unofficial client was being used to access Tinder (a violation of Tinder's terms of service). The DPC reverted to the complainant with this information, and the complainant advised that he had used the official Tinder client for Android and the official Tinder web site on Firefox. However, it transpired that he had been using a custom Android build on his phone with various security and privacy add-ons. As a result, his phone had a different device ID after each update/ reboot. In the complainant's view, this was the likely cause of the issue that resulted in his being banned from Tinder. In light of such a ban, as per Tinder's policy on data retention, his personal data would have been retained for an extended period of time. However, in the circumstances, by way of a proposed amicable resolution, Tinder offered to immediately delete the complainant's personal data so that he could open a new account.

The complainant had certain residual concerns regarding the manner in which Tinder responds to erasure requests. Upon being informed that such matters were being examined by the DPC by way of a separate statutory inquiry, the complainant agreed to accept Tinder's proposal for the amicable resolution of the complaint. As such, the matter was amicably resolved pursuant to section 109(3) of the Data Protection Act 2018 (the Act), and under section 109(3) of the Act the complaint was deemed to have been withdrawn.

This case study demonstrates that a thorough examination of a seemingly intractable complaint can bring about its amicable resolution, which will often result in a fair and efficacious solution for the affected individual in a timely manner. In this case, the information gleaned by the DPC when it probed in more depth into the circumstances of the complainant's ban from Tinder — namely the fact that the complainant used a custom Android build with security and privacy add-ons — contributed to a greater understanding between the parties and led to Tinder making its proposal for the resolution of the case, which the complainant accepted.

CASE STUDY 28

Amicable Resolution in Cross-Border Complaints: Facebook Ireland

The DPC received a multi-faceted complaint in April 2019 relating to requests for access (under Article 15 of the GDPR), rectification (under Article 16 of the GDPR) and erasure (under Article 17 of the GDPR) that the complainant had made to Facebook Ireland Limited ("Facebook"). The complaint was made directly to the DPC, from a data subject based in the UK. Upon assessment in the DPC, the complaint was deemed to be cross border because it related to Facebook's general operational policies and, as Facebook is available throughout the EU, the processing complained of was therefore deemed to be of a kind "....which substantially affects or is likely to substantially affect data subjects in more than one Member State" (as per the definition of cross border processing under Article 4(23) of the GDPR).

The complainant initially made his requests to Facebook because his Facebook account had been locked for over a year, without reason in the view of the complainant, and he believed Facebook held inaccurate personal data relating to him. Wishing to ultimately erase all the personal data that Facebook held in relation to him, the complainant was of the view that this inaccurate information was preventing him from being successfully able to log into his Facebook account to begin the erasure process. He had therefore made an access request to Facebook, but had been unable to verify his identity to Facebook's satisfaction. The complainant subsequently made his complaint to the DPC.

After a considerable amount of engagement by the DPC with both Facebook and the complainant with a view to amicably resolving the complaint, in the course of which the complainant was able to verify his identity to Facebook's satisfaction, Facebook agreed to provide the complainant with a link containing the personal data that

it held in relation to him. The complainant accessed the material at the link, but remained dissatisfied because he claimed that the material provided was insufficient. In particular, the complainant indicated that he wished to be advised of any personal data held in relation to him by Facebook beyond that which was processed in order to operate his Facebook profile. Facebook responded to the DPC indicating that the material provided to the complainant via the link was the totality of the account data that it held in relation to him. The complainant remained dissatisfied with this response, indicating that he wished to obtain information regarding any personal data that Facebook held in relation to him that was not related to his Facebook account. He also reiterated his belief that some of this personal data, allegedly held by Facebook but not related to his Facebook account, may be inaccurate, in which case he wished to have it rectified.

In response, Facebook advised the DPC that, since the commencement of the complaint, it had made certain enhancements to its 'Download Your Information' tool. Following this update to its access tools, it had determined that a very small amount of additional personal data existed in relation to the complainant's Facebook account, and provided the complainant with a new link containing all of the personal data it held in relation to the complainant, including this additional data. The complainant accessed this additional material and, with a view to resolving his complaint, sought confirmation that, once the deletion of his account was effected, Facebook would no longer hold any personal data in relation to him. Facebook reverted to indicate that the material it had provided to the complainant was the totality of the data it held in relation to him that fell within the scope of Article 15, and indicated that it would proceed with the erasure of the complainant's personal data once he had indicated that he was now satisfied for it to do so.

The complainant was content to conclude the matter on this basis and, as such, the matter was amicably resolved pursuant to section 109(3) of the Data Protection Act 2018 (the Act), and under section 109(3) of the Act the complaint was deemed to have been withdrawn.

This case study demonstrates the benefits — to individual complainants — of the DPC's intervention by way of the amicable resolution process. In this case, the DPC's involvement led to the complainant being able to verify his identity to Facebook's satisfaction, and to Facebook providing him with links containing his personal data on two occasions. The DPC's engagement with the controller also resulted in it confirming, to the complainant's satisfaction, that all the personal data that fell to be released in response to an Article 15 request had been provided to him. This resulted in a fair outcome that was satisfactory to both parties to the complaint. This case study also illustrates the intense resource- investment necessary on the part of Data Protection Authorities (DPA) to resolve issues of this nature. The complainant in this case raises an issue of concern to themselves and is entitled to have that addressed. The question the case raises is whether the controller in this case should have been capable of resolving this matter without the requirement for extensive DPA-resources to mediate the outcome.

CASE STUDY 29

Article 60 Non-response to an Access Request by Ryanair

In this case, the complainant initially submitted their complaint to the Information Commissioner's Office (ICO) of the UK, which was thereafter received by the DPC, on 2 March 2019. The complaint related to the alleged failure by the Ryanair DAC (Ryanair) to comply with a subject access request submitted to it by the complainant on 26 September 2018 in accordance with Article 15 of the GDPR. The ICO provided the DPC with a copy of the complaint form submitted to the ICO by the complainant, a copy of the acknowledgement, dated 26 September 2018, that the complainant had received from the data controller when submitting the access request, and a copy of the complainant's follow up email to the data controller requesting an update in relation to their request.

Acting in its capacity as Lead Supervisory Authority, the DPC commenced an examination of the complaint by contacting the data controller, outlining the details of the complaint and instructing the data controller to respond to the access request in full and to provide the DPC with a copy of the cover letter that issued to the complainant. Ryanair provided the complainant with access to copies of their personal data relating to the specific booking reference that the complainant had provided to the ICO and data relating to a separate complaint. Ryanair advised that it could not provide the complainant with a copy of the call recording they had requested as, due to the delay on Ryanair's part in processing the request, the call

recording had been deleted in accordance with company policy and they had been unable to retrieve it. Ryanair advised the DPC that it had previously informed the complainant of this via its online portal. Ryanair stated that at the time the request was submitted, due to the volume of data subjects who did not verify their email address, access requests were not assigned to the relevant department until the email was verified by the data subject. Ryanair advised the DPC that the complainant responded to the request, verifying their email address, but the agent who was working on the request had ceased working on the online portal and therefore the request had not been assigned to the relevant department. Ryanair asserted that this error was not discovered until sometime later, when the request was then assigned to the customer services department to provide the necessary data, including the call recording, at which point the call record had been deleted in accordance with Ryanair's retention policy. Ryanair provided the DPC with a copy of its retention policy, in which it states that call recordings are retained for a period of 90 days from the date of the call. Ryanair advised that, as the complainant's call had been made on 5 September 2018, it would have been automatically deleted on 4 December 2018. Ryanair further stated that it does not have the functionality to retrieve deleted call recordings. Pursuant to Section 109(2) of the Data Protection Act 2018, the DPC attempted to facilitate the amicable resolution of the complaint. However, the complainant was unwilling to accept Ryanair's proposals in respect of same. As such, the matter fell to be decided by way of a decision under Article 60 of the GDPR.

(i) Initial Draft Decision

As the complaint related to cross-border processing, the DPC was obliged, in accordance with the Article 60 process, to make a draft decision in respect of the complaint. In its initial version of the draft decision, the DPC made a finding of infringement of Article 15 of the GDPR in that Ryanair failed to provide the complainant with a copy their personal data that was undergoing processing at the time of the request. The DPC also found an infringement of Article 12(3) of the GDPR in that Ryanair failed to provide the complainant information on action taken on their request under Article 15 within the statutory timeframe of one month. The DPC provided the draft decision to Ryanair to allow it to make submissions. Ryanair subsequently provided a number of submissions, which (along with the DPC's analysis thereof) were taken into account in the draft decision.

(ii) Provision of Draft Decision to Concerned Supervisory Authorities

In accordance with the Article 60 process, the DPC proceeded to submit its draft decision to the IMI to be circulated amongst the Concerned Supervisory Authorities (CSAs), pursuant to Article 60(3) of the GDPR. The DPC's draft decision was uploaded to the IMI on 25 May 2020 and, pursuant to Article 60(4) of the GDPR, the CSAs were thereafter entitled to four weeks in which to submit any relevant and reasoned objections to the decision.

The DPC subsequently received a number of relevant and reasoned objections and comments in relation to its draft decision from the CSAs. In particular, certain CSAs argued that additional infringements of the GDPR ought to have been found, and in addition that a reprimand ought to have been imposed.

(iii) Revised Draft Decision

In accordance with Article 60(3) of the GDPR, the DPC is obliged to take due account of the CSAs' views. In light of the objections and comments received from the CSAs, the DPC carefully considered each relevant and reasoned objection and comment received in respect of its draft decision. The DPC revised its draft decision to include a summary and analysis of the objections and comments expressed by the CSAs. In revising its initial draft, the DPC followed certain relevant and reasoned objections received, and declined to follow others. In the its revised draft decision, the DPC proposed to issue a reprimand to Ryanair, pursuant to Article 58(2) (b) of the GDPR. The DPC provided its revised draft decision to Ryanair to allow it to make final submissions. Ryanair noted that the DPC had found that it had infringed the GDPR, and that the DPC had exercised its powers in this case in line with Recital 129 and the due process requirements in Article 58 of the GDPR. Ryanair advised the DPC that it accepted the findings and the associated reprimand and did not wish to make any further submissions.

(iv) Provision of Revised Draft Decision to Concerned Supervisory Authorities

In accordance with Article 60(5) of the GDPR, once the DPC submitted its revised draft decision to the CSAs for their views, the CSAs were entitled to two further weeks in which to submit any further objections to the decision.

Pursuant to Article 60(5) of the GDPR, the DPC submitted its revised draft decision to the CSAs for their opinion on 20 October 2020. As the DPC received no further objections or comments in relation to the revised draft decision from the CSAs within the statutory period, the CSAs were deemed to be in agreement with the revised draft decision of the DPC and bound by it in accordance with Article 60(6) of the GDPR.

(v) Adoption of Final Decision

Upon the passing of the deadline for receipt of any further objections, the DPC proceeded to adopt the final decision,

in accordance with Article 60(7) of the GDPR. The DPC then uploaded its final decision to the IMI and communicated it to Ryanair. The final decision was uploaded on 11 November 2020. Pursuant to Article 60(7), the ICO, with whom the complaint was initially lodged, was responsible for informing the complainant of the decision.

In summary, the DPC found infringements of Articles 12(3) and Article 15 of the GDPR in respect of this complaint.

This case study demonstrates that, where a complaint relating to the cross-border processing of personal data cannot be amicably resolved, the Article 60 procedure that follows as a result is particularly involved, complex and time-consuming. In this case, the initial draft of the DPC's decision was uploaded to the IMI on 25 May 2020, and the final decision was not adopted until 11 November 2020, some six months later.

This case study also demonstrates — once again — the intensity of DPA resources consumed in delivering outcomes on issues that could have been resolved by the controller without recourse to the DPC, raising again the question of unwarranted DPA resource-drainage away from resolving wider systemic issues which would achieve improved outcomes for the maximum number of individuals.

CASE STUDY 30

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

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

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

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

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

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

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

CASE STUDY 31

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

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

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

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

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

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

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

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

CASE STUDY 32

Amicable resolution in cross-border complaints — Yahoo EMEA Limited

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

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

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

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

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

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

CASE STUDY 33

TikTok and cooperation with other EU data protection authorities

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

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

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

CASE STUDY 34

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

This case study concerns a complaint the DPC received via the One Stop Shop (OSS) mechanism created by the GDPR from an individual regarding an erasure request made by them to MTCH Technology Services Limited (Tinder). As way of background, the individual's account was the subject of a suspension by Tinder. Following this suspension, the individual submitted a request to Tinder, under Article 17 of the GDPR, seeking the erasure of all personal data held in relation to them. When contacting Tinder, the individual also raised an issue with the lack of a direct channel for contacting Tinder's DPO. As the individual was not satisfied with the response they received from Tinder, they made a complaint to the Greek Supervisory Authority.

The individual asserted that neither their request for erasure nor their concerns about accessing the DPO channels, had been properly addressed by Tinder. As the DPC is the Lead Supervisory Authority (LSA) for Tinder, the Greek Supervisory Authority forwarded the complaint to the DPC for handling. The DPC intervened to seek a swift and informal resolution of the matter in the first instance. The DPC put the substance of the complaint to Tinder and engaged with it. In response and by way of a proposed amicable resolution, Tinder offered to conduct a fresh review of the ban at the centre of this case. Following this review, Tinder decided to lift the ban. The lifting of a ban by Tinder allows an individual to be then in a position to access their account on the platform. The individual can then decide if they wish to use the self-delete tools to erase their account from within the Tinder platform. In addition to the above, Tinder provided information for the individual in relation to its retention policies.

In relation to the matter of individuals being able to contact its DPO, on foot of the DPC's engagement with Tinder, the platform agreed to strengthen its existing processes by posting a dedicated Frequently Asked Questions (FAQ) page on its platform. This page now provides enhanced information to individuals on specific issues relating to the processing of personal data and exercising those rights directly with Tinder's DPO. Through the Greek Supervisory Authority, the DPC informed the individual of the actions taken by Tinder. In their response the individual confirmed that they were content to conclude the matter and, as such, the matter was amicably

resolved pursuant to section 109(3) of the Data Protection Act 2018 (the Act), and the complaint was deemed to have been withdrawn. This case study again demonstrates the benefits — to individual complainants — of the DPC's intervention by way of the amicable resolution process. The DPC's engagement with the controller also resulted in Tinder improving the information that it makes available to all of its users on its platform.

CASE STUDY 35

Cross-border complaint resolved through EU cooperation procedure

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

The details of the complaint were as follows:

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

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

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

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

1. The data controller agreed to comply with the erasure request; and
2. The data controller sincerely apologised for the error.

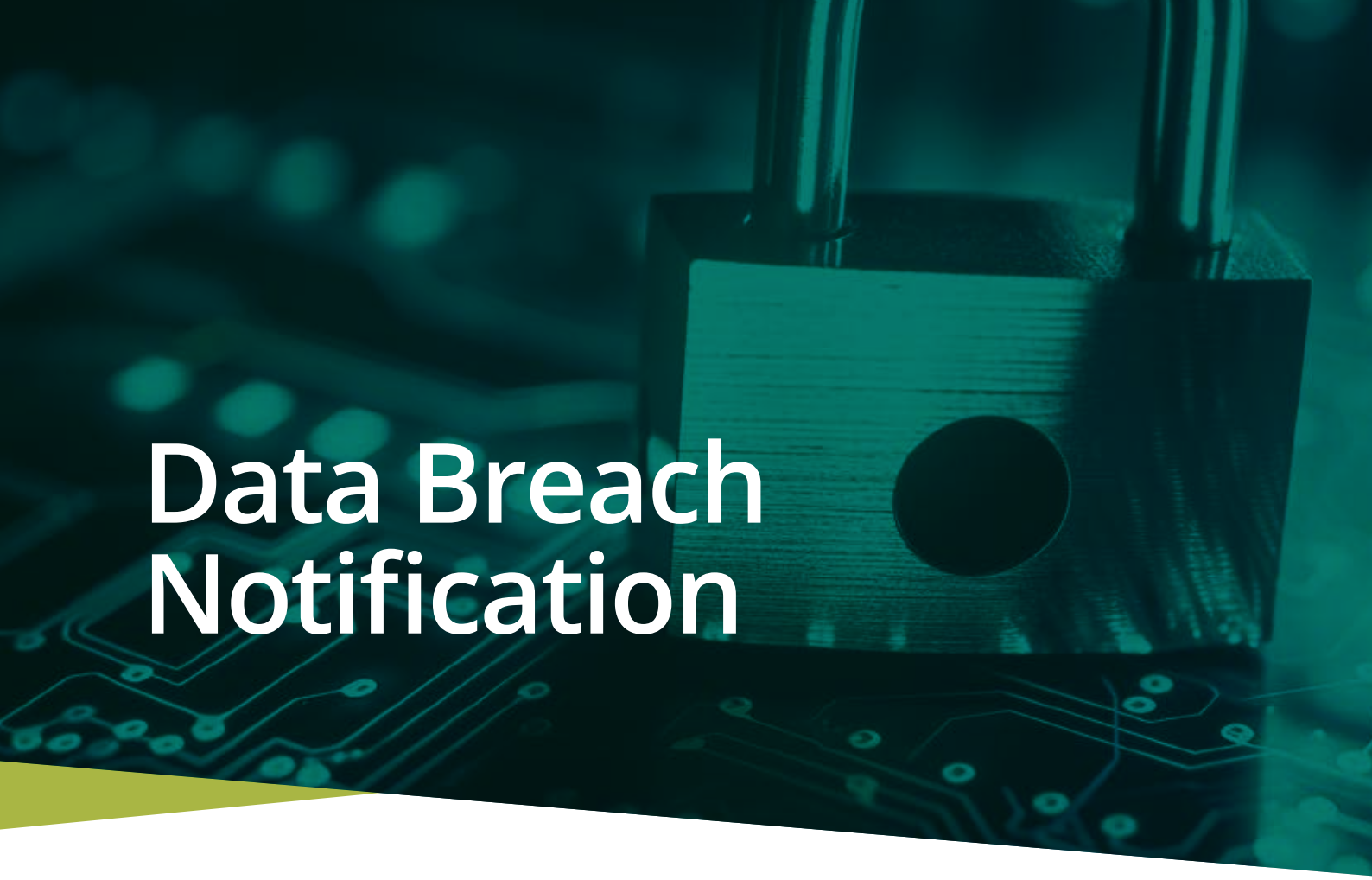
In January 2022, the DPC informed the data subject by email of the final outcome of its engagement with the data controller. When doing so, the DPC noted that the actions now taken by the data controller appeared to adequately deal with the concerns raised in his complaint. In the circumstances, the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

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

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

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

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



Data Breach Notification

CASE STUDY 36

Failure to implement the data protection policies in place

An employee of the data controller, a public-sector body, lost an unencrypted USB device containing personal information belonging to a number of colleagues and service users.

The public controller had the appropriate policy and procedures in place prohibiting the removal and storage of personal data from its central IT system by way of unencrypted devices. However, it lacked the appropriate oversight and supervision necessary to ensure that its rules were complied with, and the employee appeared not to have been aware of the policy regarding the use of unencrypted devices. The breach could have been prevented had the organisation fully implemented the policy and made staff aware of it

CASE STUDY 37

Unencrypted USB device lost in the post

A private-sector data controller notified the DPC that a package containing consent forms and an unencrypted USB device had been sent using standard postal services.

However, the package was damaged in transit, causing the USB device to fall out and become lost. The USB device contained pictures of minors participating in an organised educational event. The potential loss/disclosure of the personal data contained on the USB device could have been prevented/mitigated had the data controller had in place and implemented an encryption policy surrounding the used of portable memory devices and an adequate policy concerning sending sensitive material through the post, for example registered post/courier service.

CASE STUDY 38

Website phishing

A private sector (educational) data controller reported an incident of phishing, where a staff member had clicked on a suspicious website link and entered their credentials resulting in their email account becoming compromised.

The data controller had not enabled multi-factor authentication on its email accounts. Had this technical measure and appropriate cyber security training been in place from the outset this data breach may have been preventable.

CASE STUDY 39

Loss of paper files in transit

The data controller, a public body, notified the Data Protection Commission (DPC) about an incident involving the transportation of hard-copy legal files containing special-category personal data.

The controller had contracted a courier company to transport the files to another department but the files went missing in transit. It transpired that the controller did not retain a backup of the original files, resulting in a loss of personal data. The controller did not have sufficient procedures in place for the secure removal and storage of hard-copy files that contained special-category personal data. The breach could have been prevented had the organisation properly considered its requirements when transporting such materials to another location and the inherent risks involved in such activities, and implemented more secure measures to ensure the protection of personal data.

CASE STUDY 40

SIM swap attack

A data subject notified the data controller (a mobile-phone network operator) that a SIM card swap was requested and authorised on her mobile-phone account by an unauthorised third party.

The data subject was concerned because her mobile-phone number had been used to receive text messages for two-factor authentication from her bank in relation to her banking service. Further investigation undertaken by the data controller indicated that an unknown third party had obtained limited personal data belonging to the data subject by some external means and had managed to pass the controller's identity-validation processes.

The customer-service agent for the data controller did not follow the validation process fully, and facilitated a SIM card swap on the customer's account contrary to the controller's policy. The breach would not have occurred had the controller had more robust processes preventing access to key account information and the customer-service agent had received sufficient data protection training, including on the risks posed to customer personal data by deviating from the company's validation policy.

CASE STUDY 41

Loss of control of paper files

A public sector health service provider notified the DPC that a number of files containing patient medical information had been found in a storage cabinet on a hospital premises which was no longer occupied.

The records were discovered by a person who had gained illegally accessed a restricted premises and subsequently posted photographs of the cabinet containing the files on social media. The public sector organisation in question informed the DPC that, having become aware of the breach, a representative of the organisation was sent to locate and secure the files. The files were removed from the premises and secured.

This breach highlights the importance of having appropriate records management policies; including mechanisms for tracking files, appropriate secure storage facilities and full procedures for the retention or deletion of records. The DPC issued a number of recommendations to the organisations to improve their personal data processing practices.

CASE STUDY 42

Ransomeware Attack

An organisation operating in the leisure industry notified the DPC that it had been the victim of a ransomware attack, which potentially encrypted/ disclosed the personal data of up to 500 customers and staff stored on the organisations server. The route of the infiltration was traced to a modem router that had been compromised (back up data was however stored securely via a cloud server).

Following examination of the incident, the DPC issued a number of recommendations to the organisation.

The DPC recommended that the organisation conduct an analysis of its ICT infrastructure to establish if further malware was present, to review and implement appropriate measures to ensure there is an adequate level of security surrounding the processing of personal data, and to conduct employee training to encompass cyber security risks. The DPC has received regular updates from the organisation and is satisfied that significant steps to improve and implement both organisational and technical measures concerning shortfalls in the security of their ICT infrastructure have been taken, including the development of a training plan for all staff in this area.

CASE STUDY 43

Disclosure of CCTV footage via social media

A commercial and residential property management company notified the DPC that an employee of a security company whose services they retained had used their personal mobile phone to record CCTV footage of two members of the public engaged in an intimate act, which had been captured by the management company's security cameras.

The video taken was subsequently shared via WhatsApp to a limited number of individuals. The business advised the DPC that they communicated to staff who may have received the footage that they must delete it and requested no further dissemination of the video.

Both the property management company and the security company were able to demonstrate that adequate policies and procedures did exist, however appropriate oversight

and supervision to ensure compliance with these policies and procedures were lacking.

Following recommendations made by the DPC to the property management company, the company has subsequently engaged with its staff to deliver further data protection training with an emphasis on personal data breaches. In addition, further signage was displayed prohibiting the use of personal mobile devices within the confines of the CCTV control room.

CASE STUDY 44

Breach Notification (Voluntary Sector) — Ransomware Attack

In May 2020, the DPC received a breach notification from an Irish data processor and subsequently a notification from an Irish data controller operating in the voluntary sector who had engaged this processor to provide webhosting and data management services.

The breach related to a ransomware attack that occurred in the data centre utilised by the data processor, and which was the result of malware gaining access via a Remote Desktop Protocol (RDP) 1 port to the server.

The DPC engaged with both the controller and processor and through a number of communications — including the issuing of technical and organisational questionnaires focusing on areas of potential non-compliance with data protection regulation. These areas included the processor's use of a data centre within the US to store back-up data without adequate agreements — and sufficient oversight by the controller over its processor — as required under Article 28 of the GDPR. The DPC engaged intensively with both parties and the DPC concluded this case by issuing recommendations to both controller and processor. Thereafter the DPC continued to engage with both parties to ensure that implementation of the DPC recommendations had occurred.

CASE STUDY 45

Breach Notification (Public Sector) Erroneous Publication on Twitter

A public sector organisation notified the DPC that they had inadvertently published personal data via their social media platform (Twitter).

The personal data was posted in violation of its policy to anonymise all content, which could potentially identify an individual data subject. The organisation in question informed the DPC that the root cause of this incident was human error and the offending tweet was removed without undue delay. Based on the action the data controller had taken to mitigate against the risk of this type of incident reoccurring, the DPC concluded its examination of this matter and issued a number of further recommendations to the organisation centring on the appropriate use of its social media platforms and how its social media accounts should be secured and limited to a specified number of authorised personnel.

CASE STUDY 46

Breach Notification (Financial Sector) Bank Details sent by WhatsApp

A private financial sector organisation notified the DPC that a customer had made a request to obtain their IBAN and BIC numbers, which were held on file. The customer making the request was personally known to the member of staff dealing with the request. The member of staff, deviating from approved practices, used their personal mobile phone to send a picture of what they believed to be the requested information over a messaging platform (WhatsApp). However, the staff member erroneously sent details pertaining to another customer to the requesting customer.

The customer who received this information contacted the organisation to advise that the information received did not relate to their account and that they had undertaken to delete all offending material from their device. The organisation communicated with staff to remind them that only authorised methods of communication should be utilised when handling future requests of this nature. The organisation has also issued an apology to all affected data subjects.

The DPC issued a number of recommendations encompassing the use of only approved organisational communication tools, making staff fully aware of acceptable and non-acceptable behaviour when using organisational communications tools, and to ensure staff have undergone appropriate training in terms of their obligations/responsibilities under the provisions of the GDPR and the Data Protection Act 2018.

CASE STUDY 47

Breach Notification (12 Credit Unions) Processor Coding Error

The DPC received separate breach reports from 12 credit unions that employed the services of the same processor, which was based in the UK. The breach by the processor arose from a coding error made by the processor when implementing measures introduced in response to the Covid-19 pandemic.

Credit unions are required to report information to the Central Bank of Ireland concerning their borrowers and the performance of their loans. The Central Bank utilises this information to maintain the Central Credit Register (or CCR). Lenders and credit rating agencies in turn use this information to verify borrowers' debts and credit histories. A large number of lenders, particularly credit unions, use the services of data processing companies to prepare such CCR returns and forward them to the Central Bank.

During 2020, the Irish Government introduced a series of measures to mitigate financial distress caused by the pandemic and resulting lockdowns. These included measures allowing financial institutions to pause loan repayments without adversely affecting borrowers' credit ratings. Lenders were instructed to use particular codes in the CCR returns to flag paused loans. This was intended to prevent those loans being interpreted as delinquent or otherwise suggesting that the relevant borrowers' credit-worthiness had deteriorated.

In this incident the processor employed by the 12 credit unions used incorrect codes on CCR returns dealing with paused loans. The incorrect codes indicated that the borrowers affected had undergone a 'restructuring event' — a restructuring event typically occurs when a borrower is unable to repay a loan over the agreed period, and the lender agrees to change the loan's terms to improve the borrower's ability to repay. This can greatly reduce a borrower's credit rating, so an inaccurate CCR record of a restructuring event could have serious consequences for the persons affected.

The credit unions in question became aware of the processor's coding error in relation to their CCR returns several weeks after the processor first sent CCR returns for them using the incorrect codes to the Central Bank.

The issue was reported to the DPC as a breach and credit unions took the matter up with the processor directly and through a user group. This allowed affected records to be identified, the appropriate coding procedures to be worked out, and corrected CCR returns to be sent to the Central Bank.

These cases illustrate the importance of processing contracts that properly implement the requirements of Article 28 of the GDPR. Most relevantly to these cases, processing contracts must provide for the processor to assist the controller in meeting its obligations for security of processing, and for reporting and responding to breaches.

CASE STUDY 48

Repeated similar breaches

Over a period of 12 months, the DPC received notifications of a series of similar breaches from a data controller involved in financial matters. The controller sold services through a nationwide retail network owned and operated by a third party, which acted as its processor. The breaches occurred when existing customers of the controller made purchases at the processor's outlets, but used an address different from the address they had previously registered with the controller.

Recent changes to the controller's customer database systems had not been fully coordinated with those for sales, resulting in sales documents containing personal data being sent to customers' old addresses rather than their new ones. The controller had instructed the processor not to accept purchase requests until changes of address had been registered, but some counter staff did not consistently follow the correct procedures.

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

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

CASE STUDY 49

Unauthorised disclosure arising from video conferencing

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

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

the institution's server. As a result, students gained access to lecturers' discussion of other students' work, which included personal remarks about some of the students.

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

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

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

CASE STUDY 50

Disclosure due to misdirected email

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

The nature of the personal data and the context all indicated a high risk to data subjects. The DPC accordingly confirmed that all affected persons had been notified of the breach, the risks and measures being taken in response to them, as required by Article 34 of the GDPR. The DPC reminded the organisation of its continuing obligation to secure personal data that was accidentally disclosed, and of the importance of ensuring security when emailing personal data. The statutory body has undertaken a review of all its data protection processes, policies and procedures.

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

CASE STUDY 51

Inappropriate disposal of materials by an educational institution

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

In concluding its examination of the breach, the DPC made a number of recommendations. These focused not just on the work practices of employees, but most importantly on the technical and organisational measures of the controller. While it is important for staff to understand and implement good data protection practices, it is the responsibility of the controller to ensure that they do so and have the means — including, where appropriate, devices such as shredders — of delivering the required standard of protection.

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

CASE STUDY 52

Email addresses disclosed via group mail

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

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

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

CASE STUDY 53

Social Engineering Attack

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

Through its DPC engagement with the firm, the DPC established that the firm used a widely used cloud email service which was managed by a contractor. Basic security settings such as strong passwords were not properly enforced and multi-factor authentication was not implemented. Upon becoming aware of the incident, the firm immediately commissioned a full investigation to establish the root cause and the extent of the breach. Based on the findings of the investigation, the firm responded promptly and implemented further technical security measures as well as additional cyber security and data protection training to all staff. The

DPC requested that updates be provided on the implementation of appropriate organisational and technical

security measures to prevent a reoccurrence of a similar breach.

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

CASE STUDY 54

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

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

The individual experienced difficulty obtaining a loan because their CCR record, which is visible to other lending institutions, had been reported in error by the controller as live and in arrears. The risk to the rights and freedoms of the individual was assessed as high and the breach was accordingly communicated by the controller to the individual under Article 34 of the GDPR. The DPC confirmed with the controller that the individual's CCR record had been amended. By way of mitigation, the controller introduced measures which require sellers of portfolios to disclose information on individuals such as bankruptcies. This case highlights the importance of having systems in place to ensure the security and integrity of personal data under Article 5(1)(f) GDPR. Controllers should be aware of the personal data they hold on individuals and have measures in place to validate and understand the data when acquiring it from other parties. The case also demonstrates that controllers have a duty to prevent any alteration to or unauthorised disclosure of personal data, incorrect or otherwise to the CCR which poses risk to individuals.

CASE STUDY 55

Hacking of third-party email

A Hospice Care Centre (data controller) utilises the services of Microsoft Office 365, a cloud-based email service and also engaged third-party IT consultants. An Office 365 Audit was conducted by the IT provider every quarter, where a number of recommendations by the service provider were identified including, but not limited to, all user accounts to have multi-factor authentication (MFA) and the disabling of forwarding rules on all accounts. A user's credentials were subsequently compromised and the IT consultants established that the credentials were obtained as a result of a brute-force attack, which may have been prevented had the controller introduced multi-factor authentication as recommended at the time of the audit. On the advice of the IT consultants, the compromised user password was reset and MFA introduced for this user. The controller has now commenced the introduction of MFA to all users. This breach could likely have been prevented if the recommendations of the audit were introduced in a timely manner.

Disclosure / Unauthorised Disclosure

CASE STUDY 56

Financial information erroneously cc'd to a restaurant (Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

We received a complaint concerning the alleged disclosure by a motor dealership of the complainants' personal data to a third party. The complainants had provided the dealership with copies of their driver's licences and bank details, including bank statements and full account details, in order to purchase a car through a Personal Contract Plan. They were subsequently copied in on an email from the dealership to a third-party email address, believed to be an address associated with a bank, which contained the complainants' driver's licences and bank details. The complainants were concerned that the third-party address was that of a restaurant and contacted the dealership about this, but were assured that the email address in question pertained to a bank and was secure.

The complainants remained concerned over the ownership of the email address, conducted online research into the matter, and were confident the email address was that of a restaurant. In order to confirm their suspicions, a friend of the complainants sent an email to the address in question and the response received confirmed it was that of a restaurant.

In the course of our examination, the dealership accepted that the email had been sent in error to the wrong address. Notwithstanding this acknowledgment, it was clear that no attempt had been subsequently made to contact the restaurant in order to request that the information erroneously sent be deleted by the unintended recipient. Upon instruction from this office, we received confirmation that the dealership had contacted the restaurant and requested that the email, including the documents, be deleted. The dealership put forward a proposal for amicable resolution that was accepted by the complainants.

This case demonstrates that it is vital for data controllers (and their employees) to implement and ensure a practice of precautionary measures when electronically transmitting personal data, particularly financial information. A large proportion of the data-breach notifications that the Data Protection Commission (DPC) receives are of the unauthorised-disclosure variety, with a common cause being emails sent in error to the wrong address. Where a data controller identifies that such an incident occurs, it is not enough to acknowledge it, whether to the data subject or

to the DPC. Instead, it is incumbent on the data controller to take all reasonable steps to remedy such a breach. This includes recalling the email from the sender, asking the unintended recipient to confirm they have deleted the email, and thereafter putting in place measures to prevent a recurrence. Human error by staff presents a high risk of data breaches on an ongoing basis and it is critically important that efforts are made to mitigate those risks by driving data protection awareness throughout the organisation, particularly in regard to new staff.

CASE STUDY 57

CSO data breach — Disclosure of P45 data (Applicable law — Data Protection Acts 1988 and 2003)

We received several complaints in late 2017 against the Central Statistics Office (the CSO), each alleging that the CSO had disclosed the respective complainants' personal data without their consent or knowledge. The complaints related to a data breach that the CSO had previously reported to us (under the voluntary Personal Data Breach Code of Practice) and to the affected individuals.

The data breach originated from actions taken by the CSO in response to three requests over a five-day period from separate former census enumerators seeking their P45 information. Emails with PDF attachments containing their own P45 and P45s of thousands of third parties were sent to the requesting enumerators. The CSO informed us that the data breach had been identified when a member of CSO staff had reviewed the relevant CSO sent-items mailbox, as part of the CSO's standard due-diligence practices. The CSO confirmed that the disclosed third-party P45 information contained personal data including PPSNs, dates of birth, addresses and details of earnings from employment as census enumerators.

During our investigation, the CSO informed us that upon discovering the breach it had notified the recipients of the error, who had subsequently confirmed in writing that they had deleted the files. The CSO told us that it had also notified the affected individuals of the facts of the breach as they pertained to each individual. The CSO also informed us that following the data breach it had implemented a range of new procedures for handling P45 requests, including a rule that P45 requests were to be answered only by post going forward.

This data breach had impacted on the thousands of individuals whose personal data was contained in the files that were unlawfully disclosed to the three former enumerators. The incident essentially occurred in triplicate because the erroneously disclosed files had been attached to three separate outgoing communications. This incident would have been preventable had the CSO had the appropriate processes in place for the oversight of releasing tax-related personal data.

The DPC issued a number of individual decisions in respect of complaints in relation to this breach, finding in each case that a contravention of Section 2A(1) of the Data Protection Acts 1988 and 2003 had occurred, in that personal data had been processed without a legal basis, as was clear from the breach report submitted to the DPC from the CSO. Having examined the new measures implemented by the CSO to guard against a recurrence, the DPC was satisfied that they comprehensively addressed the failings that had brought about this incident. However, from the perspective of ensuring the lawfulness of the processing and the security and confidentiality of personal data held by the CSO, those new organisational procedures only served to underline the inadequacy of the previous measures for responding to requests for tax-related information.

CASE STUDY 58

Ryanair webchat transcript sent to another customer (Applicable law — GDPR and Data Protection Act 2018)

We received a complaint from a data subject whose webchat with a Ryanair employee was accidentally disclosed by Ryanair in an email to another individual who had also used the Ryanair webchat service. The transcript of the webchat contained details of the complainant's name and that of his partner, his email address, phone number and flight plans. The complainant told us that he had been alerted to the disclosure by the individual who had been erroneously sent the transcript of his webchat.

In our examination of the complaint, we established that Ryanair's live webchat service is provided by a third party, which is a data processor for Ryanair. We also established that the system that sends the webchat transcripts by email has an auto-fill function that populates the recipient field with the email address of the last customer emailed. On the date in question, the data processor received requests from four Ryanair customers for transcripts of their webchats, all of which were processed by the same agent. However, the agent did not correctly change the recipient email address when sending each transcript so that they were sent to the wrong recipients. Ryanair informed us that in order to prevent a recurrence of this issue the auto-fill function in the live webchat system has been disabled by the data processor and refresher GDPR training has been provided to staff.

Many of the complaints that the DPC receives relating to unauthorised disclosure of personal data in an electronic context — for example, emails containing personal data sent to the wrong recipient — stem from use of the auto-fill functions in software. While data controllers may consider this a useful timesaver tool in a data-entry context, it has inherent risks when it is used to populate recipient details for the purposes of transmitting personal data. Auto-fill functions should therefore be used with caution, and where controllers decide to integrate such a function into their software for data-processing purposes, at a minimum other safeguards should be deployed, such as dummy addresses at the start of the address book, or on-screen prompts to double-check recipient details. The principle of safeguarding the security and confidentiality of personal data goes hand in hand with data protection by design and default so that when data controllers and processors are devising steps in a personal-data-processing programme or software, the highest standards of protection for the personal data are built in, particularly with regard to assuring the integrity, security and confidentiality of personal data.

CASE STUDY 59

Transmission of data by a Government Department via WhatsApp (Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

We received a complaint against the Department of Foreign Affairs and Trade (the DFAT), alleging that the mission in Cairo, Egypt, had shared the complainant's personal data with a third party (his employer) without his knowledge or consent, and that it had failed to keep the complainant's personal data safe and secure, having transmitted it via WhatsApp to his employer. This related to processing of the complainant's personal data contained in a short-term visa application that the complainant had submitted in order to sit an exam in Ireland.

During our investigation, the DFAT informed us that it was standard practice in processing visa applications to check for accuracy, completeness and the validity of supporting documents. According to DFAT, a suspicion had arisen as to the veracity of a supporting document submitted by the complainant, which had purportedly been signed by his employer. In order to verify its validity, a staff member in the Cairo mission had contacted the employer (an official of an Egyptian government agency, whose name and signature appeared on the document) by telephone as he was best placed to verify the authenticity of the document. The employer confirmed that he would need to see the

document to verify it, but that as he did not have an official email address, the only way to receive it was via WhatsApp. The DFAT informed us that prior to sending the data via WhatsApp it had carried out a local risk assessment, including looking at the security/ encryption associated with WhatsApp. It had concluded that in light of the end-to-end encryption on WhatsApp, this was the most secure means of transmission available, given the urgency of the visa application, as outlined by the complainant in his application. In this context, DFAT informed us that many government officials and civil servants in Egypt do not have access to official email accounts/ systems and often use services like Gmail, Hotmail, WhatsApp and Viber to carry out official business. In this case, the government official in question had confirmed that this was the only method of communication available to him.

The documents had been sent by using the mobile phone of the only staff member of the Cairo mission with WhatsApp and had been deleted from the device immediately after being sent. Ultimately, the official informed the Cairo mission that the documents were fraudulent and the visa application was denied. During our investigation, the complainant informed us that he was seeking €3,000 in compensation from the DFAT, as the lost cost of sitting the exam in Ireland. Upon the DPC informing the complainant that it did not have the power to award compensation, the complainant requested a formal decision from the DPC. In considering whether a contravention of the Acts had occurred when the complainant's personal data was sent by DFAT, via WhatsApp to the official in question, the DPC sought to establish the facts in relation to, first, whether the transmission in question was necessary, and, second, whether it was secure, including whether there were more secure methods available to DFAT to transmit the data. On the first issue, the DPC was satisfied that it was necessary for the DFAT to share the complainant's personal data with the official who, in the application for the short-term visa, was stated to be his employer and who, according to the application documents, had purportedly signed certain supporting documents. We noted in this regard that the relevant privacy policy (for the Irish Naturalisation and Immigration Services) explicitly states that burden of proof in a visa application is on the applicant and that the visa officer may verify any evidence submitted in support of an application. The policy also states that any information provided in an application form can be disclosed to, among others, foreign governments and other bodies for immigration purposes.

The DPC was satisfied that given the lack of any other secure means to contact the official in question, the transmission via WhatsApp was necessary to process the personal data for the purpose provided (visa eligibility) and that the complainant was on notice that supporting documentation could be shared with third parties to verify authenticity. The DPC also took account of the fact that the local risk assessment carried out by DFAT had established that, in the circumstances, sending the personal data via WhatsApp was the most secure means of transmission. Accordingly, the DPC found that DFAT had complied with the Acts.

This was an exceptional case arising from the particular on-the-ground circumstances of the country in question. Here, transmission of information for official purposes via WhatsApp was in fact the most secure method available and the complainant's employer, while a government official, had no access to an official communications system through which the personal data could have been transmitted. In this case, the key data protection principles of necessity and proportionality, applied against the unique context of the processing in question, resulted in the DPC reaching a finding of compliance with the Acts. Such a finding would likely not have prevailed had the complaint arisen in an equivalent case where other official communication channels had been available to transmit the personal data contained in the supporting documents.

CASE STUDY 60

HSE Hospital/Healthcare Agency

In 2019, the DPC received a complaint about the disclosure of a patient's data via Facebook messenger by a hospital porter regarding her attendance at the Early Pregnancy Unit of a hospital. Upon examination of the complaint, the HSE clarified to the DPC that the hospital porter who disclosed the personal information of the patient was in fact employed by a healthcare agency contracted by the HSE. The DPC contacted the agency and sought an update in relation to its internal investigation, details of any remedial action as well as details of any disciplinary action taken against the employee in question. At the same time, the DPC advised the HSE that, as it contracts the company concerned to provide agency staff to work in the hospital, ultimately the HSE is the data controller for the personal data in this instance.

The complaint was subsequently withdrawn by the solicitor acting on behalf of the woman following a settlement being agreed between the affected party and the hospital/ healthcare agency. Data controllers/data processors may be liable under Section 117 of the Data Protection Act 2018 to an individual for damages if they fail to observe the duty of care they owe in relation to personal data in their possession.

The DPC has no role whatsoever in dealing with compensation claims and no function in relation to the taking of any such proceedings under Section 117 of the 2018 Act or in the provision of any such legal advice.

What this case illustrates is that ongoing training is necessary for all staff in relation to their obligations under data protection law and that controllers must do due diligence and satisfy themselves that any contractors/ processors they engage are fully trained and prepared to comply with data protection laws.

CASE STUDY 61

Unauthorised disclosure of mobile phone e-billing records, containing personal data, by a telecommunications company, to the data subject's former employer (Applicable law: Data Protection Acts 1988 and 2003 ("the Acts"))

The complainant, during a previous employment, asked the telecommunications company to link her personal mobile phone number to her (then) employer's account. This enabled the complainant to avail of a discount associated with her (then) employer. While this step resulted in the name on the complainant's account changing to that of her (then) employer, the complainant's home address remained associated with the account and the complainant remained responsible for payment of any bills. Following termination of the employment relationship, the complainant contacted the telecommunications company to ask that it (i) restrict her former employer's access to her mobile phone records; and (ii) separate the account from that of her former employer. Following this request, an account manager took a number of steps in the mistaken belief that this would result in the separation of the complainant's account from that of her former employer. The complainant, however, became aware that, subsequent to her request, her former employer continued to access her account records. On foot of further inquiries from the complainant, the telecommunications company discovered its error and the complainant's account was eventually separated from that of her former employer.

The complainant subsequently submitted a complaint to the telecommunications company. Having investigated the complaint, the company informed the complainant that it did not have a record of the original account restriction request. In the circumstances, the complainant referred a complaint to this office.

During our investigation, the telecommunications company acknowledged that the initial action taken by its account manager was insufficient as it did not separate the complainant's account from that of her former employer and neither did it prevent her former employer from accessing her e-billing records. The company further acknowledged that its records were incomplete when it investigated the complainant's complaint. It confirmed, in this regard, that it had since located the complainant's initial restriction/separation request.

The issues for determination, therefore, were whether the telecommunication company, as data controller:

1. implemented appropriate security measures, having regard to Sections 2(1)(d) and 2C(1) of the acts in order to protect the complainant's personal data against unauthorised access by, and disclosure to, a third party (i.e. the complainant's former employer); and
2. kept the complainant's data accurate, complete and up to date, as required by Section 2(1)(b) of the Acts.

This office found that the telecommunications company did not implement appropriate security measures to protect the complainant's personal data from unauthorised access by, and disclosure to, her former employer. This was self evident from the fact that the complainant's former employer continued to access her e-billing records despite the initial actions taken by the telecommunications company.

This office further noted the obligation, set out in Section 2C(2) of the Acts, for a data controller to "... take all reasonable steps to ensure that — (a) persons employed by him or her ... are aware of and comply with the relevant security measures aforesaid ...". This office found that the telecommunications company had not complied with its obligations in this regard. Again, this was self evident from the fact that the account manager who initially actioned the complainant's request was operating on the mistaken belief that the actions taken were sufficient to achieve separation of the complainant's account from that of her former employer.

This office also considered the fact that, at the time when the complainant referred her complaint to the telecommunications company, the company could not locate her initial account restriction request. The result of this was that the outcome of the company's own investigation into the individual's complaint was incorrect. Accordingly, and notwithstanding the subsequent rectification of the position, this office found that the telecommunications company failed to comply with its obligations under Section 2(1)(b) of the Acts in circumstances where the complainant's records, at the relevant time, were inaccurate, incomplete and not up to date.

Key Takeaways

The above case study highlights the fact that the obligation to keep personal data safe and secure is an ongoing one. Data controllers must ensure that they continuously monitor and assess the effectiveness of their security measures, taking account of the possibility that the circumstances or arrangements surrounding its data processing activities may change from time to time. In this case, the data controller failed to take the required action to reflect the change in circumstances that was notified to it by the complainant when she requested the restriction and separation of her account from that of her former employer. The case study further highlights the importance of effective training for employees in relation to any internal protocols.

CASE STUDY 62

Alleged disclosure of the complainant's personal data by a local authority (Data Breach Complaint)

The DPC received a complaint from an individual concerning an alleged disclosure of the complainant's personal data by a local authority. The complainant alleged that the local authority had disclosed the complainant's name, postal address and information relating to the housing assistance payment in error to a third party. The individual had been informed by the local authority that this disclosure had occurred. However, the individual was dissatisfied with the actions taken by the local authority in response to the disclosure and did not wish to engage further with the local authority with a view to seeking an amicable resolution of the complaint.

The DPC examined the complaint and contacted the local authority in order to seek further information regarding the individual's allegations. The local authority confirmed to the DPC that a personal data breach had occurred when the complainant's personal data was included, in error, in a Freedom of Information request response to a third party. In addition to the information provided by the local authority to the DPC in the context of its examination of the complaint, the incident in question was notified to the DPC by the local authority as a personal data breach, as required by Article 33 of the GDPR. In that context, the DPC engaged extensively with the local authority regarding the circumstances of the personal data breach, the data security measures in place at the time the personal data breach occurred and the mitigating measures taken by the local authority, including the local authority's ongoing efforts to retrieve the data from the recipient.

On the basis of this information, the DPC concluded its examination of the complaint by advising the individual that the DPC was satisfied that the complainant's personal data were not processed by the local authority in a manner that ensured appropriate security of the personal data and that an unauthorised disclosure of the complainant's personal data, constituting a personal data breach, had occurred. On the basis of the actions that had been taken by the local authority in response to the personal data breach and, in particular, the fact that the recipient of the complainant's personal data had returned the data to the local authority, the DPC did not consider that any further action against the local authority was warranted in relation to the subject matter of the complaint.

CASE STUDY 63

Unauthorised disclosure in a workplace setting

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

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

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

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

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

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

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

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

However, the company had failed to properly anticipate and mitigate the risk of human error in storing such documents, as had happened to the WRC submission. The DPC also reminded the company of the need to ensure that relevant personnel are aware of the need to handle personal data in accordance with applicable security measures, and to respond to breaches accordingly. This case illustrates how data controllers must consider all risks that can arise when they process personal data, including the risk of human error. The measures that they adopt to address those risks must reflect not just the possible causes of loss or harm, but also the consequences of a breach, and the ways in which those consequences can be minimised or remedied.

CASE STUDY 64

Lack of appropriate security measures unauthorised disclosure in a workplace setting

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

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

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

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

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

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

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

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

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

CASE STUDY 65

Disclosure Without Consent

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

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

CASE STUDY 66

Disclosure of Sensitive Data

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

CASE STUDY 67

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

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

During the course of the DPC's handling of this complaint, the bank set out its position that any joint account holder is entitled to access the details and transaction information of the joint account as a whole. The bank further took the view that, in relation to solicitors who are acting for its customers, it is sufficient for it to accept written confirmation from a solicitor on their headed paper that the solicitor acts for the customer as authority for the bank to engage with the solicitor in their capacity as a representative of the bank's customer. Data protection law requires that personal data be collected or obtained for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes (the "purpose limitation" principle). In this case, the DPC noted that the bank had obtained the complainant's personal data in order to administer the joint account which the complainant held with the other account holder, including the making of payments, the collection of transaction information and the preparation of bank statements. It appeared to the DPC that it was consistent with the bank's terms and conditions for the joint account, and the account holder's signing instructions on the account (which allowed either party to sign for transactions without the consent of the other account holder), that the administration of the account could be completed by one account holder without the consent of the other. In the light of this, the DPC considered that the disclosure of bank statements to the solicitors of the other joint account holder was not incompatible with the specified, explicit and legitimate purpose for which the complainant's personal data had been obtained by the bank, that is, for the administration of the joint account.

Second, the DPC considered whether the bank had a lawful basis for the disclosure of the complainant's personal data, as required under data protection law. In this regard, the DPC was satisfied that the bank was entitled to rely on the "legitimate interests" lawful basis, which permits the processing of personal data where that processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party. In this case, the bank had disclosed the complainant's personal data on the basis that the solicitor was acting for the other joint account holder and was seeking the statements for legitimate purposes, namely to carry out an audit of the other account holder's financial affairs. In circumstances where, in accordance with the signing instructions on the account, the other account holder would have been entitled to administer the account, the DPC was satisfied that the bank would not have had any reason to suspect that the disclosure would be unwarranted by reason of any prejudice to the complainant's fundamental rights or freedoms. Accordingly, the DPC considered that the bank had a lawful basis for the disclosure, regardless of whether the complainant had provided consent.

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

CASE STUDY 68

Disclosure and unauthorised publication of a photograph

A data subject made a complaint to the DPC regarding the publication of their child's image, name and partial address in a religious newspaper. The image used in the publication was originally obtained from a religious group's Facebook page. The data subject informed the DPC that consent was not given for the wider use of the image through the publication in the newspaper. The concern was for the child's privacy arising from the use of the image, name and partial address by the newspaper. In correspondence sent directly between the data subject and the newspaper the data subject cited Article 9 of the GDPR concerning special category personal data applies to their complaint because the image disclosed information regarding the child's religious beliefs.

As part of its examination, the DPC engaged with the data controller and asked for a response to the complaint. The data controller informed the DPC they never intended any distress to the data subject or their family. A reporter had seen the image on the group's Facebook page and asked permission to use it from a leading member of the religious group, subsequently this member granted permission for its usage. The newspaper stated the image was already available online through the group's Facebook page and was taken at a public event and the address used was that of the religious group and not the child's personal address.

In further response to the DPC's queries, the newspaper informed the DPC that it was their normal practice to seek consent to take and use images and although in this circumstance the image was available on an open Facebook page the newspaper still contacted the religious group and queried if permission had been obtained to use the image. The leading member of the religious group they had contacted advised them that another person in loco parentis (acting in the place of a parent) had given permission. The newspaper stated to the DPC, that this person "was acting in loco parentis as far as [the newspaper] was concerned and consent had been therefore given." The newspaper also informed the DPC they rely on Article 9(2)(a) and 9(2)(e) of the GDPR for the processing of special category personal data. The newspaper concluded that they had the required legitimate interest in publishing the photograph, the photograph was in a public domain through the open Facebook page, they took steps to ensure that consent was obtained to publish the photograph and the consent furnished was adequate and they were entitled to rely on same. The newspaper said they were satisfied they had complied with their obligations but they had reviewed and amended their internal policies on this issue.

The DPC provided the data subject with the response to the complaint and asked the data subject whether they considered their data protection concerns adequately addressed and amicably resolved. In addition to this the data subject was invited to make their observations on the response from the data controller. The data subject responded to inform the DPC the matter was not amicably resolved and that explicit consent should have been obtained. The DPC proceeded to conclude the examination and provide an outcome to both parties as required under section 109(5) of the Data Protection Act 2018 (the 2018 Act).

The DPC advised the data subject under section 109(5)(c) of the 2018 Act that the explanation put forward by the data controller concerning the processing of the child's personal data in the circumstances of this complaint was reasonable. In saying this, the DPC wrote to the religious newspaper and under section 109(5)(f) of the 2018 Act recommended that it considers the Code of Practice from the Press Council, in particular principle 9 therein, ensuring that the principle of data minimisation is respected, and to conduct and record the balancing exercise between public interest in publication and the rights and interests of data subjects.

CASE STUDY 69

Disclosure by a credit union of a member's personal data to a private investigations firm

The complainant in this case was a borrower from a credit union and was alleged to be in arrears on a loan. The credit union claimed to be unable to contact the complainant. The credit union disclosed personal data of the complainant to a private investigations firm with the intention of locating and communicating with the complainant. The data disclosed included the complainant's name, address, former address, family status and employment status. Approximately four years later, the complainant became aware of that disclosure and complained to the DPC.

The private investigations firm had ceased to trade several years before the complaint and so was not in a position to assist the DPC's investigation. The DPC asked the credit union to explain the legal basis on which it had disclosed the data, and why it considered it necessary to do so. The credit union informed the DPC that it did not have a written contract with the private investigations firm, so the DPC asked it to provide details of any internal policy or procedure concerning when it was appropriate to liaise with that firm.

Concerning the legal basis for the disclosure, the credit union claimed that the disclosure was necessary for the purposes of pursuing a legitimate interest and for the performance of its contract with the complainant. It also referred to a provision of section 71(2) of the Credit Union Act 1997 that allows a credit union to disclose a member's account information where the Central Bank of Ireland (previously, the Registrar of Credit Unions) is of the opinion that doing so is necessary to protect shareholder or depositor funds or to safeguard the interests of the credit union. (The credit union was unable to say whether the Central Bank had expressed such an opinion in relation to this case.)

The credit union maintained that the disclosure was necessary because it had been unable to communicate with the complainant by letter, telephone or through the complainant's solicitor. In its view, the complainant was seeking to evade its efforts to update its records and discuss the outstanding loan. (The complainant strongly disputed that, pointing out that they had made repayments shortly before the credit union contacted the private investigations firm.)

The credit union told DPC that its credit control policy dealt with cases where it was proposed that a member's non-performing loan should be written off as a bad debt. Before doing so, the relevant provisions directed that the credit union should make "every effort…to communicate with the member, including the assistance of a third party" to try and continue with agreed arrangements and assist collection of the debt.

The DPC assessed that the legal basis for the disclosure and the existence of a data processing contract as the central issues in the complaint.

In light of all the facts presented, and on the basis of applicable legislation, the DPC concluded that the credit union had a legitimate interest in seeking to obtain up-to-date contact details in order to re-establish contact with the complainant with a view to discussing the repayment of the loan. The processing of personal data was necessary for the purposes of pursuing that legitimate interest. The DPC accepted that the disclosure could affect the complainant's fundamental rights and legitimate interests. Against that, however, fulfilling the important social function provided by credit unions required that they be able to take action to engage with members whose loans fall into arrears. For that reason, the disclosure was warranted despite the potential prejudice to the complainant's fundamental rights and freedoms or legitimate interests. The credit union therefore assert the pursuit of its legitimate interest in contacting the complainant and seeking repayment of the loan as the legal basis for disclosing personal data to the private investigations firm.

The DPC also considered whether section 71(2) of the Credit Union Act 1997 provided a legal basis for the disclosure in this case. The DPC noted that compliance with a legal obligation, such as under a court order or provision of a statute, can provide a legal basis for processing. However, section 71(2) (including the provision mentioned by the credit union in its submissions to the DPC) was permissive rather than mandatory in its effect: while it allowed credit unions to disclose information in certain circumstances, it did not require them to do so. Accordingly, the section did not justify the disclosure for the purposes of applicable data protection legislation.

The DPC noted that processing by a processor on behalf of a controller must be conducted under the terms of a contract in writing or in equivalent form that complies with

applicable data protection legislation, and in particular ensures that the processing meets the obligations imposed on the controller. In the DPC's opinion, the credit union's credit control policy was not sufficient to meet this requirement, so the credit union had failed to meet its statutory obligation in this regard.

This case highlights several important issues for data controllers. Whenever a controller engages a processor to process data on its behalf, there is a clear requirement to have a processing contract or equivalent measure that complies with Article 28(3) of the GDPR or other applicable legislation. These contracts benefit both controllers and processors by making clear what processing is required and how it is to be done. They also protect data subject by providing clarity on how and by whom their data is being processed, and for what purposes.

The case also shows the importance of being clear as to the legal basis for processing. Where the basis claimed is a legal obligation, it is not sufficient to simply show that the controller can legally choose to act in a particular way: the processing must be required by law for this legal basis to apply. Where a processor claims that processing is for the purpose of pursuing a legitimate interest, they must be able to show that the processing is necessary for that purpose, and that they have carefully balanced that interest against the rights and freedoms of persons who may be affected by it. If the interest does not outweigh those rights and freedoms, it does not provide a legal basis for the processing.

CASE STUDY 70

Disclosure of a journalist's name and mobile phone number by a public figure

The complainant in this case was a journalist who emailed a public figure to ask questions about decisions that the public figure had taken in relation to their work. The public figure used their Twitter account to publish a copy of the email. The journalist's name, work email address and mobile phone number were legible in the published copy of the email. The journalist reported receiving a number of threatening text messages afterwards.

The journalist asked the public figure to delete the published copy of the email. The public figure did so, but also published a Tweet saying that the journalist's mobile phone number was available online. This included a link to a discussion board message posted by the journalist six years previously, while a student, which included the same mobile number. The journalist complained to the DPC.

As part of its investigation, the DPC asked the public figure to identify the legal basis for disclosing the journalist's data. The public figure's response queried whether the journalist's name and contact details constituted personal data. It also asserted that, because the journalist had previously made that information available on the internet, the journalist had impliedly consented to its publication by the public figure. The journalist rejected that assertion.

The DPC took the position that the journalist's name, email address and mobile phone number were personal data because the journalist was clearly identifiable by them. Concerning the legal basis for disclosing them, the DPC noted that, while data protection law provided for several possible legal bases for processing, the only basis raised by the public figure had been consent. The DPC's view was that a media enquiry to a public figure from a journalist acting in that capacity did not amount to valid consent to the sharing of any personal data in the enquiry. For those reasons, the public figure's disclosure of the data breached data protection law.

This case highlights several important issues. Article 6 of the GDPR provides for six legal bases on which a processor can justify processing personal data. Consent is one of these, but the GDPR sets out important requirements including as to how consent is given, the right to withdraw consent and the need for controllers to be able to demonstrate that data subjects have given consent. While other legal bases exist, controllers must bear in mind that these are all subject to a 'necessity' test and their own specific requirements.

CASE STUDY 71

Disclosure of personal and financial data to a third party and erasure request

A data subject provided their personal and financial data to an organisation (the data controller) as part of their relative's application for a scheme. The application was unsuccessful and the applicant was issued with a refusal letter, which included a breakdown of the data subject's personal and financial data. The data subject made a complaint to the Data Protection Commission (DPC) regarding the lack of transparency in the application process and the disclosure of their personal and financial data to their relative. The data subject requested the return of their personal data from the data controller. The data subject also requested that their personal data be erased by the data controller under Article 17 of the General Data Protection Regulation (GDPR), and if erasure was not an option, their legal basis for retaining their data.

Prior to the commencement of an examination by the DPC, the data subject made suggestions to amicably resolve their complaint, which included, among other things, a 'goodwill gesture' from the data controller. However, due to the role of the organisation, the data controller was not in a position to facilitate this request.

As part of its examination, the DPC engaged with the data controller and requested a response to the data subject's complaint. The data controller stated that while it is part of their procedure to inform applicants of their reasons for refusal, only a partial disclosure should be made in their decision letters where information was gathered from a third party. With regards to the data subject's erasure request, the data controller advised that the personal data provided would be retained for the lifetime of the applicant plus 10 years. The data controller explained that the data is retained for this period as the data in question may affect any future applications by the applicant.

Subsequently the data subject's erasure request was refused by the data controller as they advised they are relying on Article 17(3)(b) of the GDPR, which restricts the obligations on data controllers to erase personal data where the personal data is required for compliance with a legal obligation. Also, the data controller relied on Article 23(1)(e) of the GDPR, which states that a data subject's rights may be restricted for:

"Important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security."

An apology was issued to the data subject by the data controller, as a result of the disclosure of their personal data in the refusal letter issued to their relative, the applicant. The data subject queried if this disclosure was reported to the DPC as a breach. Under Article 33 of the GDPR, a data controller is required to report a personal data breach to the relevant competent authority without undue delay, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. A data breach is described in Article 4(12) of the GDPR as: "A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". The DPC found that the disclosure was a result of human error and not identified as a systemic issue.

Through its examination, the DPC found that the refusal letter which resulted in the disclosure of the data subject's personal data, could be distinguished from other records retained by the data controller as it did not directly follow their guidelines. As such, the DPC invited the data controller to erase or redact the data subject's personal data from the decision letter held on file. In addition, an amended letter could be issued to the applicant redacting the data subject's personal data. The data controller advised they would reissue the refusal letter and request the applicant return the initial letter sent. The data controller also advised they would delete the initial letter from their records.

Under section 109(5)(c) of the 2018 Act, the DPC advised the data subject that the explanation put forward by the data controller in the circumstances of their complaint was reasonable. While the data controller acknowledged the disclosure of the data subject's personal data to their relative, the applicant, they issued an apology for same, and indicated that the original refusal letter will be amended on their system, while an updated letter will issue to the applicant.

Further, under section 109(5)(f) of the 2018 Act, the DPC recommended the data controller provide updated training to their staff regarding their guidance for decision letters.

CASE STUDY 72

Disclosure of personal data (Applicable Law — GDPR and Data Protection Act 2018)

A data subject issued a complaint to the Data Protection Commission (DPC) against their owner management company (data controller) regarding the disclosure of their personal data under the General Data Protection Regulation (GDPR). The data subject explained to the DPC that an email containing their personal data was circulated by a property management company on behalf of an owner management company (OMC) and contained information regarding the payment of annual services charges.

Before contacting the DPC the data subject contacted the OMC to address their concerns of the disclosure of their personal data. The OMC responded that its policy was to include such personal data in emails to all clients. The data subject confirmed that it had not seen, nor signed this policy.

Following the engagement of the DPC the data controller cited a clause in its OMC Memorandum of Association, which allowed for the disclosure of payment or non-payment of service charges to other unit owners.

The DPC provided both parties with guidance from this office for consideration, "Data Protection Considerations Relating to Multi-Unit Developments and Owners' Management Companies". The guidance indicated that the disclosure must be justified as both necessary and proportionate to achieve a specific, explicit and legitimate purpose, in accordance with data protection law.

The data controller informed the DPC that a balancing test was conducted and highlighted that the processing of the personal data was necessary to achieve the legitimate interest of the management company to obtain payment of service charges.

Under section 109(5)(c) of the 2018 Act the DPC advised that the data controller had not been able to provide an adequate lawful basis for the processing of personal data as outlined in the complaint.

The outcome reminded the data controller of their obligations as a data controller under Articles 5, 6 and 24 of the GDPR and under section 109(5)(f) of the 2018 Act, the DPC recommended that the data controller review their Memorandum of Association to ensure compliance with the DPC guidance; consider alternative methods to resolve the non-payment of service charges and consider and balance any legal obligation or legitimate interest against the rights and interests of the data subject.

CASE STUDY 73

Appropriate security measures for emailed health data

The DPC received a complaint from the parent of a child whose health data was mistakenly disclosed to an unknown third party. The data was contained in a document attached to a misaddressed email that had been sent by an employee of a public body.

The child was the subject of a health-related assessment by a therapist employed by the public body. The therapist prepared a draft report, which was to be sent to a senior professional. Before sending it, the therapist decided to ask a colleague for a second opinion. The colleague was not in the office, so the therapist chose to send the draft report to the colleague's personal email address. Soon after doing so, the therapist realised that the email address was incorrect. The public body's IT service was not able to recall the misaddressed email. The recipient's email service provider confirmed that the recipient's account was active, but emails from the public body asking the recipient to delete the misaddressed email were not answered. The public body contacted the parent by telephone, in person and in writing to inform them of the error and apologise for it. It also notified the DPC of a personal data breach. The parent subsequently lodged a complaint with the DPC.

As part of its examination of the complaint, the DPC asked the public authority to explain the steps taken to secure deletion of the misaddressed email, its policy concerning the sending of work-related emails to staff members' personal addresses, and the measures being adopted to prevent a recurrence of the breach.

In its response, the public body confirmed the sequence of events described above, including its attempts to recall the email and its interactions with the email service provider. It advised the DPC that it had reissued a copy of its data protection policy to all members of the team on which the therapist worked, and wrote to it reminding it that it is not permitted to send any information to personal email addresses, regardless of whether they were asked to do so. It was made clear that this included reports and other work-related documentation. Data protection was added as a fixed item on the agenda of the team's bi-monthly meetings, and all team members were scheduled for data protection awareness training.

In assessing the matter, the central issue identified by the DPC was the obligation of a data controller to take appropriate security measures against risks including unauthorised disclosure of personal data. Appropriate security measures were to be identified having regard to factors including the technology available, the harm that could be caused by disclosure, and the nature of the data. Further, controllers must take all reasonable steps to ensure that their employees are aware of and comply with those measures.

The DPC's view was that sending a draft report to a personal email address was clearly inappropriate having regard to the required level of security, and was contrary to the public body's own data protection policies. However, the mere existence of those policies was not enough to satisfy the obligation to take reasonable steps to ensure its employees were aware of and complied with them. The public body had done so only after the breach had occurred.

This case highlights the risk-based approach of data protection legislation. Article 32 of the GDPR requires controllers (and, where applicable, processors) to implement technical and organisational measures to ensure appropriate security of the personal data they process. Persons who process personal data on behalf of the controller must do so only on the controller's instructions, and therefore must be aware of relevant technical and organisational measures.

The appropriateness of security measures will be determined by reference to risks: the risk that a breach could pose to individuals' right and freedoms, and the possibility of various types of breach, such as the loss, disclosure or unauthorised access to the data. Special category data, such as health data, has heightened protection under Article 9 of the GDPR. Security measures that are appropriate for these categories of data are therefore likely be more stringent. Controller must also bear in mind that risks often change over time; security measures must likewise be adapted to the circumstances.

Electronic Direct Marketing

CASE STUDY 74

Prosecution of Viking Direct (Ireland) Limited

In April 2017, we received a complaint from a business owner regarding unsolicited marketing emails that the business email address was receiving from Viking Direct (Ireland) Limited. The complainant indicated that she had previously contacted the company to ask for her business email address to be removed from the marketing list but, despite this, further marketing emails continued to be sent.

During our investigation, Viking Direct (Ireland) Limited confirmed that the complainant had asked to be removed from its mailing list several times. It explained that the internal processes of moving the data to the suppression list had failed and the data remained on the mailing list. The company stated that the systems had now been corrected and tested, such that the situation should not recur. It apologised for any inconvenience caused to the complainant. Our investigation found evidence of three opt-out requests sent by the complainant to Viking Direct (Ireland) Limited by email between 30 March 2017 and 11 April 2017.

Viking Direct (Ireland) Limited had been the subject of an investigation in 2012 on foot of a complaint made to the DPC about unsolicited marketing emails. At that time, we concluded that investigation with a warning to the company. In light of that warning, the DPC decided to prosecute the company in respect of the 2017 complaint.

At Dublin Metropolitan District Court on 14 May 2018, the company entered a guilty plea to one charge of sending an unsolicited marketing email to a business email address in contravention of Regulation 13(4) of S.I. No. 336 of 2011. Under this regulation, it is an offence to send an unsolicited direct-marketing communication by electronic mail to a subscriber (which includes business subscribers) where that subscriber has notified the sender that it does not consent to the receipt of such a communication. The case was adjourned for sentencing until 11 June 2018. At the sentencing hearing, the court applied Section 1(1) of the Probation of Offenders Act in lieu of a conviction and fine. The company agreed to cover the prosecution costs incurred by the DPC.

CASE STUDY 75

Prosecution of Clydaville Investments Limited, T/A The Kilkenny Group

Annual Report 2018 May–December Case Study 16

In November 2017, we received a complaint from an individual who received a marketing email from the Kilkenny Group. The email, which was personally addressed to him, promoted a pre-Christmas sale and informed him that there was up to 50% off and that everything was reduced. The complainant informed us that he did not believe that he had opted into receiving marketing emails.

During our investigation, it emerged that a previous marketing email had been sent to the same complainant one year earlier, in November 2016, inviting him to a corporate event in the company's Cork store. The complainant subsequently advised us that he recalled replying to that email, asking that his email address be deleted. In September 2012, arising from our investigation of a complaint about unsolicited marketing text messages sent by the Kilkenny Group to a different complainant, we had issued a warning to the company. In light of that, the DPC decided to prosecute the company in respect of the 2017 complaint.

The matter came before Tralee District Court on 15 October 2018. The defendant faced a total of four charges. Two related to alleged contraventions of Regulation 13(1) of S.I. No. 336 of 2011 for the sending of unsolicited marketing emails to the complainant in November 2016 and November 2017 without his consent. Two further charges related to alleged contraventions of Regulation 13(12) (c) of S.I. No. 336 of 2011. This regulation provides that a person shall not send electronic marketing mail that does not have a valid address to which the recipient may send a request that such a communication shall cease. As guilty pleas were not entered to any of the charges, the matter went to a full hearing involving three defence witnesses and two prosecution witnesses, including the complainant. At the end of the proceedings, the court found the facts were proven in relation to two contraventions of Regulation 13(1) in relation to the sending of two marketing emails without consent. On the understanding that the defendant would discharge the prosecution costs of €1,850, the court applied Section 1(1) of the Probation of Offenders Act in respect of both charges instead of a conviction and fine. The court dismissed the two charges in respect of Regulation 13(12)(c).

CASE STUDY 76

Prosecution of DSG Retail Ireland Limited

DSG Retail Ireland Limited operates under various trading names and registered business names such as Dixons, Currys, PC World and Currys PC World. In November 2017, we received a complaint from a woman who had purchased a television from Currys a year previously. She informed us that she gave her email address to the company for the purposes of receiving a receipt and that she did not consent to receiving marketing emails. She stated she had unsubscribed from receiving further emails but the unsolicited emails continued.

During our investigation, the company told us that the customer had successfully unsubscribed from its mailing list in November 2016. However, when she made a new purchase in January 2017 and once again opted out of receiving marketing communications, a duplicate record was created following the customer's second transaction. According to the company, this duplicate record, coupled with a system bug arising during an update to its systems in May 2017, resulted in an error regarding the recording of the customer's marketing preferences. As a result, there was a period between August and November 2017 during which marketing emails were sent to her.

As we had previously issued a warning to the company in November 2014 on foot of a previous complaint from a member of the public concerning an alleged contravention of the regulations in relation to unsolicited marketing emails, the DPC decided to prosecute the company in respect of the latest suspected contravention.

At Dublin Metropolitan District Court on 22 October 2018 the company entered a guilty plea in relation to a charge for contravention of Regulation 13(1) of S.I. No. 336 of 2011 for the sending of an unsolicited marketing email to the complainant without her consent. In lieu of a conviction and fine, the court ordered the company to make a charitable donation of €1,500 to the Peter McVerry Trust. The defendant company agreed to cover the prosecution costs of the DPC. Confirmation of the charitable donation was subsequently provided to the court on 26 November 2018 and the matter was struck out.

CASE STUDY 77

Prosecution of Vodafone Ireland Limited

In May 2018, we received a complaint from an individual who stated he was receiving frequent unsolicited calls from Vodafone's marketing team. He claimed that Vodafone initially called him on 10 May 2018, at which point he said he was not interested in their offer; since then the company had called him every day. He ignored the communications.

During our investigation, we confirmed that a recording of the marketing telephone call on 10 May 2018 included the complainant advising the calling agent that he was not interested in Vodafone's broadband service. Vodafone told us that the agent should have then removed the telephone number from the marketing campaign by using an appropriate code when closing the call. Human error had led to the phone call being closed with an incorrect code for a call-back — meaning the complainant's phone number remained, leading to the further calls.

We received a separate complaint in July 2018 from a Vodafone customer. He reported that he had received an unsolicited marketing telephone call from Vodafone in June 2018 despite having opted out of receiving marketing telephone calls during a previous unsolicited marketing telephone call in May 2018, confirmation of which had been sent to him by email shortly afterwards.

In response to our enquiries, Vodafone referred to a data-breach report that it had submitted to the DPC on 21 June 2018. This report notified the DPC that several customers who had opted out of marketing between 18 May and 11 June 2018 had erroneously received marketing communications due to difficulties in the implementation of system changes as part of its GDPR-compliance programme. This resulted in recently changed marketing preferences not being read clearly on all its systems and, accordingly, the customers concerned were wrongly included in marketing campaigns.

The DPC decided to prosecute Vodafone in relation to both cases. At Dublin Metropolitan District Court on 22 October 2018, the company entered guilty pleas in relation to two charges for contraventions of Regulation 13(6) (a) of S.I. No. 336 of 2011 for the making of unsolicited marketing telephone calls to the mobile telephones of the two complainants without their consent. The court convicted Vodafone on the two charges and imposed fines of €1,000 in respect of each of the two charges (a total fine of €2,000). Vodafone agreed to cover the prosecution costs of the DPC.

CASE STUDY 78

Prosecution of Starrus Eco Holdings Limited, T/A Panda and Greenstar

In April 2018, a customer of the bin-collection service provider, Panda, complained to us that he had received unsolicited marketing SMS and email messages to which he had not consented, advertising Panda's electricity business. He stated that the messages did not provide an unsubscribe option.

During our investigation, we were informed by Panda that the complainant should not have received the marketing messages. It said that due to a human error, a staff member of the marketing department had incorrectly believed that the complainant had consented to receiving direct-marketing messages. It regretted the failure to include an opt-out on the messages and explained that its service provider for marketing emails had failed to act in accordance with its instructions to include an opt-out. In May 2018, we received a complaint from a customer of Greenstar, another bin-collection service provider. This individual had previously complained to us in 2011 about unsolicited marketing text messages sent to him without consent. We concluded that previous complaint by issuing a warning to Greenstar in September 2011. The complainant now reported to us that direct marketing from Greenstar by means of SMS messages had started aggressively once again.

In response to our enquiries, Greenstar informed us that given the lapse of time (which it acknowledged was absolutely no excuse) since the 2011 complaint, its records pertaining to the complainant were not what they should have been with respect to the complainant having previously opted out of receiving marketing from the company — that neither the complainant's details nor details of the 2011 complaint were accurate and up-to-date, insofar as it should not have used the complainant's mobile telephone number for marketing purposes.

In light of our previous warning, the DPC decided to prosecute Starrus Eco Holdings Limited, T/A Panda and Greenstar in respect of offences committed in both cases. At Dublin Metropolitan District Court on 24 October 2018, the company entered guilty pleas in relation to charges for contraventions of Regulation 13(1) of S.I. No. 336 of 2011 for the sending of unsolicited marketing SMS messages to the two complainants without their consent. Instead of a conviction and fine, the court ordered the company to make a charitable donation of €2,000 to the Peter McVerry Trust. The defendant company agreed to cover the prosecution costs of the DPC. Confirmation of the charitable donation was subsequently provided to the court on 15 November 2018 and the matter was struck out.

CASE STUDY 79

Prosecution of Vodafone Ireland Limited

In April 2019, the DPC received two separate complaints from an individual who had received unsolicited direct marketing communications by text and by email from the mobile network operator Vodafone. The individual stated that Vodafone had ignored their customer preference settings, which recorded thatthey did not wish to receive such marketing.

During our investigation, Vodafone confirmed that the complainant had been opted-out of direct marketing contact but that communications were sent to them due to human error in the case of both the text message and the email marketing campaigns.

In the case of the SMS message, Vodafone confirmed that a text offering recipients the chance to win tickets to an Ireland verses France rugby match was sent to approximately 2,436 customers who had previously opted-out of receiving direct marketing by text. This was as a result of a failure to apply a marketing preferences filter to the SMS advertising campaign before it was sent.

In the case of the email received by the complainant, an application that was intended to be used to send direct marketing to prospective customers was used in error and the message was sent to existing Vodafone customers. While Vodafone was unable to definitively confirm the number of customers who were contacted by email contrary to their preference, the marketing email was sent

to 29,289 existing Vodafone customers. The company confirmed that some 2,523 out of 7,615 of these were contacted in error. However, it was unable to link the remaining 21,674 customers who were sent the same email with their marketing preferences in Vodafone's data warehouse to confirm the total number contacted in error.

The DPC had also received a separate complaint in February 2019 from another individual who was a former customer of Vodafone. This customer had ceased to be a Vodafone customer more than five years earlier and they still continued to receive promotional text messages. In the course of our investigation, Vodafone confirmed that the direct marketing messages were sent to the complainant in error. It said that in this exceptional case, the complainant's mobile number was not removed from the platform used to send marketing communications when their number was no longer active on the network. As the DPC had previously prosecuted Vodafone in 2011, 2013 and 2018 in relation to direct electronic marketing offences, we decided to initiate prosecution proceedings in relation to these complaints.

At Dublin Metropolitan District Court on 29 July 2019, Vodafone pleaded guilty to five charges of sending unsolicited direct marketing communications in contravention of S.I. No. 336 of 2011 ('the ePrivacy Regulations'). The company was convicted and fined €1,000 on each of three charges and convicted and fined €750 each in respect of the two remaining charges.

CASE STUDY 80

Prosecution of Just-Eat Ireland Limited

We received a complaint from an individual in November 2018 regarding unsolicited direct marketing emails from Just-Eat Ireland Limited. The complainant had unsubscribed from the company's direct marketing emails but several days later received an unsolicited marketing email. During our investigation of this complaint, the company informed us that the complainant's attempt to unsubscribe was unsuccessful due to a technical issue with its email platform. This issue affected 391 customers in Ireland.

As Just-Eat Ireland Limited had previously been warned by the DPC in 2013 on foot of complaints in relation to unsolicited direct marketing emails, we decided to initiate prosecution proceedings.

At Dublin Metropolitan District Court on 29 July 2019, Just-Eat Ireland Limited pleaded guilty to one charge in relation to sending an unsolicited direct marketing email. The court applied section 1(1) of the Probation of Offenders Act in lieu of a conviction and fine on the basis that the company donate €600 to the Peter McVerry Trust charity.

CASE STUDY 81

Prosecution of Cari's Closet Limited

In May 2018, we received a complaint against the online fashion retailer Cari's Closet from an individual who had in the past placed an online order with the company. The complaint concerned the receipt of three unsolicited direct marketing emails. The same person had previously complained to the DPC in January 2018 about unsolicited emails from that company. On that occasion, the complainant said they had received over forty marketing emails in one month alone. The person had attempted, without success, to unsubscribe on a couple of occasions.

Cari's Closet attributed the failure to properly unsubscribe the complainant from emails to a genuine mistake on its behalf.

As the DPC had issued a warning in April 2018 in relation to the earlier complaint, we decided to initiate prosecution proceedings against the company.

At Dublin Metropolitan District Court on 29 July 2019, Cari's Closet pleaded guilty to one charge of sending an unsolicited direct marketing email to the complainant. Instead of a conviction and fine, the court applied section 1(1) of the Probation of Offenders Act on the basis that the company donate €600 to the Little Flower Penny Dinners charity.

CASE STUDY 82

Prosecution of Shop Direct Ireland Limited T/A Littlewoods Ireland

In May 2019, the DPC received a complaint from an individual who said they had been receiving direct marketing text messages from Littlewoods since March. The complainant stated that they had followed the instructions to unsubscribe by texting the word 'STOP' on five occasions to a designated number known as a short code, but they had not succeeded in opting out and they continued to get marketing text messages.

In the course of our investigations, Shop Direct Ireland Limited (T/A Littlewoods Ireland) confirmed it had a record of the complainant's opt-out from direct marketing texts submitted through their account settings on the Littlewoods website on 8 May 2019. It did not, however, have a record of their attempts to opt-out of direct marketing texts on previous occasions using the SMS short code. This was due to human error in setting up the content for the SMS marketing messages. The company said that the individual responsible for preparing and uploading content relating to marketing texts had mistakenly included the opt-out keyword 'STOP' instead of 'LWISTOP' at the end of the marketing texts.

Shop Direct Ireland Limited had previously been prosecuted by the DPC in 2016 in relation to a similar issue, which resulted in a customer attempting, without success, to unsubscribe from direct marketing emails. On that occasion, the court outcome resulted in the company making a donation of €5,000 to charity instead of a conviction and fine.

The DPC decided to prosecute the company in respect of direct electronic marketing offences in relation to the May 2019 complaint.

At Dublin Metropolitan District Court on 29 July 2019, Shop Direct Ireland Limited (T/A Littlewoods Ireland) entered guilty pleas to two charges relating to sending unsolicited direct marketing text messages. The court ruled that the company would be spared a conviction and fine if it donated €2,000 each to the Peter McVerry Trust and the Little Flower Penny Dinners charities and section 1(1) of the Probation of Offenders Act was applied.

CASE STUDY 83

Vodafone seeks employment details from customers

The DPC received a number of queries regarding new or existing customers being requested by Vodafone to produce their employment details and work phone number as a requirement for the provision of service by that company.

The concerns arising were that the requests were excessive and contrary to the Article 5 principle of lawful, fair and transparent collection as the processing of data relating to their employment status was entirely unrelated to the product or service that they were receiving from the telecommunications company, which was for their personal or domestic use only.

Second, there were concerns that the mandatory request for a customer's occupation/place of work/work phone number was not adequate, relevant or necessary under the "data minimisation" requirement and did not meet the purpose limitation principle as set out in Article 5 of GDPR. Third, there were also concerns amongst customers that the company's data protection/privacy notice did not comply with the transparency requirement of GDPR Article 13(1).

Following engagement with the DPC, Vodafone admitted that it had made an error in the collection of this information. The company stated that the problems were caused by a legacy IT system that had not been updated to remove this requirement and that any access to the data was exceptionally limited and was not used for any additional processing purposes by them. Vodafone immediately commenced a plan to remediate the problems caused and, on the insistence of the DPC, published on its website the details of what had occurred, so that customers would be aware of the issue.

CASE STUDY 84

Prosecution of Three Ireland (Hutchison) Limited (ePrivacy)

In February 2021, the DPC received one complaint from an individual concerning unsolicited marketing electronic mail they had received from the telecommunications company Three Ireland (Hutchison) Limited. The complainant opted out of receiving marketing emails in mid-February 2021.

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

The DPC had previously prosecuted Three Ireland (Hutchison) Limited in 2020 and 2012 for breaching Regulation 13 of the ePrivacy Regulations in relation to previous complaints. Accordingly, the DPC decided to proceed to another prosecution arising from this complaint case.

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

CASE STUDY 85

Prosecution of Vodafone Ireland Limited (ePrivacy)

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

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

In the other case, the complainant completed a transfer of ownership form on which they clearly set out their marketing preferences not to receive any marketing communications from Vodafone Ireland Limited. The agent handling the transaction failed to follow a process to input the customer's marketing preferences. As a result, the customer subsequently received a further 14 unsolicited marketing messages — seven emails and seven text messages.

The DPC had previously prosecuted Vodafone Ireland Limited in 2019, 2018, 2013 and 2011 for breaching Regulation 13 of the ePrivacy Regulations in relation to previous complaints. Accordingly, the DPC decided to proceed to another prosecution arising from these complaint cases.

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

CASE STUDY 86

Prosecution of Guerin Media Limited

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

The DPC had previously prosecuted Guerin Media in 2019 for breaching Regulation 13 of the ePrivacy Regulations in relation to previous complaints regarding similar incidents of unsolicited email marketing. Accordingly, the DPC decided to proceed to another prosecution arising from these complaint cases. At Naas District Court on 5 December 2022, Guerin Media Limited pleaded guilty to three charges under Regulation 13(1) of the ePrivacy Regulations. The District Court convicted Guerin Media Limited on all three charges and it imposed fines totalling €6,000. Guerin Media Limited agreed to pay €1,000 towards the DPC's legal costs.

CASE STUDY 87

Prosecution of Vodafone Ireland Limited

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

The DPC had previously prosecuted Vodafone Ireland Limited in 2021, 2019, 2018, 2013 and 2011 for breaching Regulation 13 of the ePrivacy Regulations in relation to previous complaints. Accordingly, the DPC decided to proceed to another prosecution arising from this complaint case. At Dublin Metropolitan District Court on 27 June 2022, Vodafone Ireland Limited pleaded guilty to one charge under Regulation 13(6) of the ePrivacy Regulations. The District Court applied the Probation of Offenders Act 1907 in this case, on the basis of a charitable donation of €500 to Little Flower Penny Dinners. Vodafone Ireland Limited agreed to discharge the DPC's legal costs.

Erasure

CASE STUDY 88

Retention of a minor's personal data by a State Agency (Amicable Resolution) (Applicable Law — Data Protection Acts, 1988 and 2003)

In this case, the complainants involved had previously requested that an Irish state agency erase a file pertaining to an incident at school involving their young child which had originally been notified to the agency. However while the agency had decided that the incident did not warrant further investigation, it had refused to erase the minor's personal data — indicating that such files are retained until the minor in question reaches the age of 25 years.

The Data Protection Commission (DPC) requested that the state agency outline its lawful basis for the retention of the minor's personal data. The agency provided this and cited its retention policy as stated to the complainants, but the DPC did not consider a blanket retention period applicable in the particular circumstances.

The DPC informed both parties of the amicable resolution process and both expressed a willingness to engage on same. After iterative engagement between the complainants and the controller to discuss the matter, the state agency confirmed to the complainants that the file containing their child's personal data would be deleted.

CASE STUDY 89

Delisting request made to internet search engine (Applicable Law — GDPR and Data Protection Act 2018)

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

The criteria to be applied by search engines is that delisting must occur if the results are irrelevant, inadequate or excessive. A case-by-case balancing

exercise must be conducted by the search engine that balances rights of access and rights of those individuals affected by search results.

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

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

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

Article 17(3)(a) of the GDPR states the right to be forgotten will not apply where the processing of personal data is necessary "for exercising the right of freedom of expression and information". In examining this complaint, the DPC noted the information contained in the webpages — the subject of the individual's complaint — relates to previous business conduct by them relevant to their professional life. The individual continues to engage in the same professional sphere and activities. The individual accepted this by arguing the content was impacting their professional life. The individual argued the content was inaccurate because it was defamatory. The DPC noted that a significant majority of the content the individual said was inaccurate was a blog post and comments of third parties and related to their professional activities; appearing to be the opinions of third-party commentators.

The DPC concluded if a third party were to consider the webpages the subject of this complaint it would be clear that the comments were made as user-generated content and represent third party opinions rather than appearing as verified fact. The role of the search engine in listing is not to challenge or censor the opinions of third parties unless to list results gives rise to personal data processing on the part of the search engine that is irrelevant, inadequate or excessive.

The DPC concluded that given the individual's business role and role in public life arising from their professional life, there is a public interest in accessing information regarding their professional life within the European Union. The DPC wrote to the individual and under section 109(5)(b) of the 2018 Act dismissed the individual's complaint based on the above considerations.

CASE STUDY 90

Right to be Forgotten (Microsoft)

The complaint concerned the individual's dissatisfaction with Microsoft Ireland Operations Limited's (data controller) response to their right to be forgotten request pursuant to Article 17 GDPR. The individual requested the delisting of two URLs that were returning on the data controller's search engine when searching the individual's name. The data controller confirmed to the individual that the URLs were delisted. However, a search of the individual's name, carried out by their legal representative, showed that the URLs continued to be returned. The DPC reviewed the URLs when receiving the complaint and confirmed that the URLs were still being returned.

The DPC intervened to seek to swiftly and informally resolve the matter. The DPC corresponded with the data controller and noted that despite confirmation that the URLs were delisted, they continued to return when searching the individual's name. The data controller investigated the request further and confirmed to the DPC that the URLs had now been delisted. Following further investigation by the DPC, it was determined that while the original URLs requested for delisting no longer appeared, a different URL was now appearing, distinct from the other URLs, redirecting to the same content. The data controller delisted this URL also at the request made by the DPC on behalf of the individual. The DPC wrote to the individual and outlined the data controller's actions. The DPC confirmed that all three URLs had been delisted by the data controller. This case demonstrates the importance

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

CASE STUDY 91

Access and Erasure request (Pinterest)

The complaint concerned the individual's dissatisfaction with Pinterest Europe's (data controller) response to his access and erasure requests pursuant to Article 15 GDPR and Article 17 GDPR, respectively. The individual submitted his requests following the suspension of his account, in order to obtain a copy of all of his personal data and to have it deleted from the data controller's systems. The individual's account was suspended due to a violation of the data controller's policies regarding spam. The data controller responded to the requests via automated response which stated that it had reviewed the account and decided not to reactivate it because it noticed activity that violated its spam policy. As a result, the individual was no longer able to access his personal data stored on their account. The individual maintained that this information could not be correct as they seldom used their account and sought a more substantial response to their access and erasure requests.

The DPC took up the complaint with Pinterest. The DPC outlined the individual's concerns in relation to his access and erasure requests and requesting that the data controller address those concerns more substantively. The DPC also requested that the data controller indicate whether the individual was provided with an opportunity to appeal his account suspension and, if so, describe the procedure for such appeals. The data controller responded to the DPC stating that it had investigated the matter and explained that once an account is suspended on the basis of a spam violation, all correspondence is automatically directed to its Spam Operations team. The data controller further explained the appeal process and noted that the individual corresponded with the Spam Operations team in relation to the appeal of their suspension. The Spam Operations team failed to identify that the correspondence also included the individual's access and erasure requests and therefore this was not addressed in its response. The data controller's response also noted that, although the Spam Operations team had rejected the individual's appeal of their account suspension, it had since carried out another review in light of its updated spam policies. Following this review, the data controller re-activated the individual's account.

The data controller also acknowledged the delay in responding to the individual and confirmed that it had since taken steps to ensure that such delays would not occur in responding to future requests. The data controller confirmed that it had actioned the individual's access and erasure requests. It also confirmed that it had reached out to the individual to inform him of the steps it had taken in response to the DPC's correspondence and provided the individual with the explanations set out above. The actions taken and explanations given by the data controller were also outlined to the individual by the DPC. The individual informed the DPC that they were satisfied with the actions taken by the data controller in response to the DPC's correspondence as it allowed him to download his data and delete his account. This case study illustrates how often simple matters — such as a complaint being forwarded to the wrong unit in an organisation — can become data protection complaints if the matter is not identified appropriately.

CASE STUDY 92

Right to be Forgotten (Microsoft)

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

The DPC intervened on behalf of the complainant. The data controller originally refused the delisting request, stating that the URLs contained information of public relevance, and that the information was published in an official bulletin of a government body; in this case, the Spanish Government. The DPC corresponded with the Spanish Data Protection Authority in relation to the information published in the URLs. The Spanish Data Protection Authority stated that due to the introduction of the GDPR, the Spanish Data Protection law was modified and the Government is no longer permitted to disclose citizens' complete National Identification number alongside their name and surnames when publicising administrative acts. Following clarification from the Spanish Data Protection Authority, the DPC informed the data controller of the change in the Spanish Data Protection law. The data controller stated that based on the update in Spanish Data Protection law, it would delist all requested URLs from being returned against the individual's name in accordance with Article 17 GDPR. This case highlights the importance of communicating with other supervisory authorities during the complaint resolution process. In these circumstances, the DPC was provided with clarification on how Spain has adapted its national legislation to comply with the GDPR. It also allowed the data controller to adapt its current procedure to ensure that requests involving the delisting of URLs containing full National Identity numbers are handled in accordance with the updated national legislation.

CASE STUDY 93

Amicable resolution — right to erasure and user generated content

This complaint concerned an initial refusal by the data controller to comply with an erasure request made by the complainant, pursuant to Article 17 GDPR. The complainant first lodged their complaint via the Spanish Data Protection Authority, the AEPD, who then transferred the complaint to the DPC as the Lead Supervisory Authority.

The complainant stated that they were named, and therefore identified, in a negative review relating to their place of employment. The review, accompanied by a partial image of the complainant, had been posted online. The complainant had sought the removal of their name and any associated images from the review.

During its engagement with the DPC on the matter, the data controller advised that they had reviewed the content in question in the context of their own privacy guidelines for the removal of content from the website and that they considered the content did not infringe upon same.

The DPC requested that the data controller review the matter again, in the spirit of amicably resolving the complaint. The data controller subsequently reverted to advise that after a further assessment of the content in question they had made the decision to remove the review posting in its entirety.

This case study demonstrates the benefits, to individual complainants, of the DPC's intervention by way of the amicable resolution process. In this case, this led to the complainant being able to affect their right of erasure over their personal data, as afforded to individuals under Article 17 of the GDPR.

CASE STUDY 94

Amicable resolution in a cross-border complaint — right to erasure

The DPC received a complaint from an individual regarding an erasure request made by them to a data controller, a platform for booking accommodation, pursuant to Article 17 GDPR. The complainant had begun creating an account on the data controller's platform but chose to abandon the process before it was complete. The complainant then communicated his erasure request to the data controller by email and telephone. In response to the erasure request, the data controller informed the complainant that they required an identity document in order to comply with the erasure request.

The complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018, and the data controller agreed to work with the DPC to attempt to amicably resolve the complaint. The data controller provided the DPC with its replies to the complainant relating to the matters raised in the complaint thus far, and confirmed that, in response to the complainant's erasure request, the data controller had requested an identity document.

In the course of the DPC's investigation of the complaint, the data controller also confirmed that the account in question had never been used to book or host accommodation or to use the service in any way. Following intervention by the DPC, the data controller undertook to delete the complainant's account without requesting that the complainant provide any additional documentation.

The DPC communicated these developments to the complainant. The complainant responded by confirming that they accepted the proposed action and that erasure of the account would resolve their complaint. The DPC engaged further with the data controller, which provided confirmation to the DPC that it had erased the complainant's account. The data controller also conveyed this erasure confirmation to the complainant directly.

The complaint was amicably resolved in accordance with section 109 of the Data Protection Act 2018. This case study demonstrates the benefits, to individuals, of the DPC's intervention by way of the amicable resolution process. In particular, this case study brings to the fore the manner in which the DPC can assist a complainant through the amicable resolution process. This includes explaining the complainant's individual concerns to the data controller, where initial engagement between them and data controller has not led to a resolution of their concerns. In this case, the DPC's involvement resulted in deletion of the complainant's personal data by the data controller, in accordance with Article 17, without requiring any further action on the part of the individual.

CASE STUDY 95

Amicable resolution — right to erasure

This complaint concerned the alleged non-response to an erasure request made by the complainant to a data controller pursuant to Article 17 GDPR.

Following receipt of the complaint from the complainant, the DPC engaged with both parties in relation to the subject matter of the complaint. Further to this engagement, it was established that, during the week in which the complainant sent their erasure request by email to the data controller, a new process to manage personal data erasure requests was being implemented by the data controller.

The data controller informed the DPC that it was during this transitional period from the old system to the new system that the erasure request was received from the data subject. The data controller further advised that while new personnel were being trained on how to manage these types of requests during this period, it appeared a response to the erasure request was missed. The data controller stated that this was an oversight, possibly due to a technical issue or human error and that it regretted the error.

In the circumstances, the data controller agreed to comply with the erasure request and sincerely apologised for the error. The data controller also subsequently confirmed

to the DPC that it had deleted the complainant's personal data.

The DPC informed the complainant of the outcome of its engagement with the data controller, noting that the positive actions taken by the data controller appeared to deal with the concerns raised in their complaint.

The complainant subsequently confirmed to the DPC that they agreed to the amicable resolution of their complaint as their concerns were now resolved and that their complaint was now withdrawn.

In this circumstance, the complaint was deemed to be amicably resolved and withdrawn, in accordance with section 109 of the Data Protection Act 2018.

This case study demonstrates the benefits to both data controllers and to individual complainants of engaging in the amicable resolution process in a meaningful way. In this case, the data controller's detailed explanation of how the oversight occurred, their offering of an apology and an undertaking to resolve the matter for the complainant, resulted in a good outcome for both parties. Most importantly, the complainant was able to exercise their right to obtain from the controller the erasure of personal data concerning them, as afforded to them under the GDPR.

CASE STUDY 96

Erasure request and reliance on Consumer Protection Code

Following an unsuccessful application for a credit card, the data subject in this case sought to have their personal data erased under Article 17 of the General Data Protection Regulation (GDPR). When the erasure request was refused by the data controller, the data subject raised concerns with the DPC that their personal data was being unlawfully retained. The DPC engaged with the data controller in order to assess the reasoning for such refusal.

In response to the data subject's initial erasure request, the data controller stated in line with provision 11.6 of the Consumer Protection Code 2012 and their Privacy Policy and Cookies Statement they had a legal obligation to retain the information provided. The data controller went further to explain that the personal data provided in the application would be retained for a period of six years from the date on which the service was provided.

As part of its examination, the DPC engaged with the data controller and requested a response to the complaint. The data controller stated that they were relying on Article 6(1)(c) of the GDPR to retain the personal data whereby processing is necessary for compliance with a legal obligation to which the data controller is subject. The data controller in this case was also subject to the Consumer Protection Code 2012 (CPC). On this basis, the data controller relied on this lawful basis for the refusal of the erasure request. Under Article 17(3)(b) of the GDPR, a data subject's right to erasure does not apply and may be restricted where the processing is necessary for compliance with a legal obligation.

For reference, the CPC is a set of rules and principles that all regulated financial services firms must follow when providing financial products and services to consumers and was published by the Central Bank of Ireland in compliance with section 117 of the Central Bank Act 1989. Under section 117(4) of the Central Bank Act 1989, it is an offence for a regulated financial firm to fail to provide the Central Bank with information to demonstrate compliance with the CPC.

Provisions 11.5 and 11.6 of the CPC require data controllers to retain the records of a consumer for six years after the date on which a particular transaction is discontinued or completed. The required records include but are not limited to: all documents required for consumer identification; the consumer's contact details; all correspondence with the consumer; all documents completed or signed by the consumer. The data subject contested this reliance as no service was provided, therefore they were of the view they were not a consumer and as such felt the data controller had no legal right to maintain the personal data. The CPC defines a consumer and includes where appropriate, a potential consumer. In addition to this, the data controller stated when the data subject applied for a credit card, the consideration of the application and subsequent decision was deemed a service.

Under section 109(5)(c) of the 2018 Act, the DPC advised the data subject that within the meaning of the CPC they were classified as a potential consumer. As a result the data controller is legally obliged to retain the personal data for a period of six years. The DPC did not consider any further action necessary at the time of issuing the outcome.

CASE STUDY 97

Debt collector involvement

A data subject had contacted the DPC as they were not satisfied with the responses to a data subject access request and erasure request. This case was against a debt collector and the data subject raised concerns about how their personal data was obtained. The data subject explained that the debt had been cleared but they still received a letter from a debt collector. This letter referred to an outstanding amount owed to a third party.

The data subject outlined to the DPC that their subject access request was made through an online platform. The data subject did not receive a response to their Article 15 Access request or their erasure request under Article 17 of the General Data Protection Regulation (GDPR). Prior to the DPC involvement, both parties engaged directly. In their correspondence to the data subject, the debt collector explained that the personal data was obtained from a third party. The personal data was then uploaded to their online system and a letter was issued to the data subject.

As part of its examination, the DPC engaged with the debt collector and requested that they outline their relationship with this third party. The debt collector informed the DPC they were acting as a data processor on behalf of the third party and that a data processor agreement, in line with Article 28(3) of the GDPR, was in place at the time they processed this personal data. The debt collector advised the DPC that this contract was now terminated and they would not be acting on behalf of the third party going forward. The DPC accepted this response and identified the debt collector as a data processor and the third party as the data controller. The data processor, stated that debt collection is in the public interest and as such they had a legitimate interest to process personal data where a data subject's account has been legally assigned to them, or when they are acting under a legal contract. The data processor stated that the processing of the data subject's personal data was necessary to collect the debt and is allowed even where the data subject does not consent to the processing; meaning the data processor relied on Articles 6(1)(b) and 6(1)(f) of the GDPR for processing the personal data.

The data processor in this case accepted that the data subject may have paid the outstanding debt but stated they could not be held responsible if the data subject pays the data controller directly and the data controller fails to notify the data processor to close the outstanding debt on their systems. The DPC highlighted that there appeared to be an error in the letter the data subject received. In this correspondence the debt collector referred to themselves as a data controller. The debt collector accepted this error and stated it should have read data processor, this error was caused by an oversight when using a template letter.

With regard to the subject access request, due to their data processor relationship they did not respond directly to the data subject's access request but did share this with the third party, the data controller. In terms of the erasure request, the data processor informed the data subject that they would be required to retain the personal data for six months for taxation/financial/auditing purposes. The six months had passed prior to the DPC involvement and the data processor assured the DPC that the personal data had now been erased. The data processor apologised directly to the data subject and offered a payment as a gesture of good will.

The DPC advised the data subject under section 109(5)(c) of the 2018 Act that the data processor and data controller had a legitimate interest to collect debts and disclose personal data in order to collect the debts. The DPC acknowledged the errors in the correspondence provided to the data subject and under section 109(5)(f) of the 2018 Act recommended that the data processor engage in regular testing of organisational and technical processes to ensure compliance with the GDPR in order to comply with Article 28 of the GDPR.

CASE STUDY 98

Retention of data by a bank relating to a withdrawn loan application

The complainant in this case had made a loan application to a bank. The complainant subsequently withdrew the loan application and wrote to the bank stating that they were withdrawing consent to the processing of any personal data held by the bank relating to the loan application and requesting the return of all documents containing the complainant's personal data. In response, the bank informed the complainant that it had stopped processing all of the complainant's personal data, with the exception of data contained in records which the bank stated it was required to retain and process under the Central Bank of Ireland's Consumer Protection Code. The complainant was not satisfied with this response, and argued, in their complaint to this Office, that in circumstances where the bank had obtained the complainant's personal data on the basis of the complainant's consent, the bank was not permitted to continue to process these data on a different legal basis (i.e. processing which is necessary for compliance with a legal obligation to which the bank is subject). The complainant also argued that the continued processing by the bank of their personal data was for a purpose which was not compatible with the purpose for which the data were originally obtained, in contravention of data protection legislation.

This office established that the bank was identified as the relevant data controller in relation to the complaint, as it controlled personal data, which the complainant had provided to the bank when making a loan application. The data in question were personal data relating to the complainant (consisting of, amongst other things, a completed loan application form and supporting documentation) as the complainant could be identified from it and the data related to the complainant as an individual. This office was therefore satisfied that the complaint should be investigated to determine if a breach of data protection legislation had occurred.

During the course of the investigation of this complaint, this office reviewed the bank's loan application form, which provided that, by signing the form, a person consented to the bank storing, using and processing their personal data for a range of purposes, including to process applications for credit or financial services. However, this office noted that the purposes for which the complainant had given their consent did not include processing for the purpose of compliance with the bank's legal obligations generally, and specifically did not include the processing of the complainant's personal data for the purpose of compliance with the Consumer Protection Code. Accordingly, this office considered that at the time of collection of the complainant's personal data the bank did not claim to rely on consent as the legal basis for the collection and processing of the complainant's personal data in order to comply with its legal obligations. Rather, this office considered that the bank could validly rely on the lawful basis that the processing was necessary in order to take steps at the request of the data subject prior to entering into a contract.

This office noted that where a loan application is subsequently withdrawn or unsuccessful and the bank does not enter into a contract with the applicant, the retention of personal data relating to the loan application can no longer be on the basis that the processing was necessary in order to take steps at the request of the data subject prior to entering into a contract, as there is no longer the possibility of entering into a contract with the data subject. As such, the bank identified a separate legal basis for the retention of the complainant's personal data relating to the loan application, namely that this processing was necessary for compliance with a legal obligation to which the bank was subject.

This office noted that the Consumer Protection Code obliged regulated entities to retain details of "individual transactions" for six years after the date on which the particular transaction is discontinued or complete. This Office considered, however, that a loan application which is subsequently withdrawn or ultimately unsuccessful is not a 'transaction' for the purpose of the Consumer Protection Code. This office then noted that the Consumer Protection Code also obliged regulated entities to retain "all other records" for six years from the date on which the regulated entity ceased to provide any product or service to the consumer, including potential consumer, concerned. However, this office did not consider that records relating to a loan application which is subsequently withdrawn to fall within the scope of this requirement under the Consumer Protection Code either. Accordingly,

this office considered that it was not necessary for the bank to retain personal data relating to the complainant's withdrawn loan application for the purpose of compliance with its legal obligations under the Consumer Protection Code, and considered that the bank had not identified a lawful basis under data protection legislation for the retention of the complainant's personal data relating to their loan application.

Under Article 6 of the GDPR, data controllers must have a lawful basis for any processing of personal data. The available lawful bases include that the data subject has given consent to the processing of their personal data for one or more specific purposes, that the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract, and that the processing is necessary for compliance with a legal obligation to which the data controller is subject. Data controllers should note also that the processing of personal data for purposes other than those for which the personal data were originally collected is only allowed where the processing is compatible with the purposes for which the data were initially collected.

CASE STUDY 99

Unlawful processing and erasure request

Following their trip to a leisure facility (the data controller), a data subject submitted a complaint to the Data Protection Commission (DPC) as they were unhappy with how the data controller processed their personal data. The data subject also wanted to exercise their rights under Article 17 of the General Data Protection Regulation (GDPR) and have their, and their families, data deleted by the organisation. Prior to contacting the DPC, the data subject requested the erasure of their data directly from the data controller and this request was refused.

The data subject explained to the DPC that, during their stay at the leisure facility, they believed their personal data was processed unlawfully as they were repeatedly asked to provide details of their booking to staff, in order to gain access to facilities on site such as restaurants and activities. The data subject believed this to be excessive processing and stated at the time they were not given a choice to object to such processing or they could not receive full access to the facilities.

In line with their examination of the complaint, the DPC contacted the data controller and shared the details of the data subject's complaint. The data controller advised the DPC that their lawful basis for processing personal data is Article 6(1)(f) of the General Data Protection Regulation (GDPR) also commonly referred to as, legitimate interest. The data controller further explained that they request customer's details prior to accessing facilities or making a purchase in order "to understand patterns and to improve the range of services and facilities available to guests". This is also detailed in their privacy policy, which is available on their website.

On foot of the data subject's complaint, the data controller reviewed their policies and identified a training gap with their staff. Following this identification, the data controller briefed their staff to ensure that they were aware that customers were not obliged to provide details of their booking when accessing certain facilities. The data controller also advised that they updated their Data Protection Regulation Department Operating Procedure to reflect this procedure more clearly.

In regards to the data subject's erasure request, the data controller advised the DPC that they have removed the data subject for all direct marketing communications. However, they were unable to erase any other personal data relating to the data subject, and their family, as it is held in accordance with their retention policy. The data controller's retention policy states that all personal data is held on file as it may be required in defence of a legal claim and only deleted after the youngest member of the booking reaches the age of 21 years, in accordance with statutory limitation periods.

Under section 109(5)(f) of the 2018 Act the DPC recommended that the data controller continue to provide training to all its employees on its obligations and the rights of data subjects under data protection legislation and to keep this training up to date.

The DPC further recommended under section 109(5)(f) of the 2018 Act that the data controller delete all personal data in accordance with their retention period.

The DPC did not consider any further action necessary at the time of issuing the outcome as they noted that the data controller had retrained all staff, apologised to the data subject and offered them compensation as a result of their complaint.

CASE STUDY 100

Unlawful processing of photograph and erasure request under Article 17 of GDPR (Applicable Law — GDPR and Data Protection Act 2018)

A data subject submitted a complaint to the Data Protection Commission (DPC) regarding the publication of their historical image in a newspaper (data controller). The data subject explained to the DPC that the article was published without their knowledge and without their consent. Before contacting the DPC the data subject contacted the data controller to address their concerns that they felt their personal data had been unlawfully processed and requesting erasure of the image from the newspaper under Article 17 of the General Data Protection Regulation (GDPR); however, the data controller rejected all elements of the data subject's request.

As part of its examination, the DPC engaged with the data controller and asked for a lawful basis under Article 6 of the GDPR for processing the data subject's personal data in the manner outlined in this complaint. The data controller informed the DPC that it is not relying on Article 6 of the GDPR for processing the data subject's personal data and it advised that it is relying on section 43 of the Data Protection Act 2018, (the 2018 Act), (data processing and freedom of expression and information), namely that processing of personal data for the purpose of exercising the right to freedom of expression and information, including processing for journalistic purposes for for the purposes of academic, artistic or literary expression, shall be exempt. The data controller further explained that the data subject was not the subject of the news article in question, that a significant number of years have passed since the photograph was taken and as such, the data subject was not readily identified.

In relation to the data subject's erasure request, the data controller relied on Section 43 of the 2018 Act as their basis for refusing to erase the image from the article.

Having considered all the elements of this complaint, the DPC found that the newspaper had a lawful basis under Section 43 of the 2018 Act and Article 85 of the GDPR to publish the data subject's historical image in a news article.

The DPC notes that the journalistic exemption does not exempt a data controller from the whole of the GDPR and data protection acts. A data controller must have consideration for their remaining obligations under the GDPR and the 2018 Act. The DPC found the processing of the data subject's personal data by the data controller to be proportionate, considering that the image in question is a historical image in which it can be reasonably assumed that the data subject is no longer readily identifiable from same. The DPC acknowledges that a third party is the main person of interest and directly quoted within the article and therefore the data subject is not the subject of discussion.

The DPC advised the data subject under section 109(5)(c) of the 2018 Act that the explanation put forward by the data controller concerning the processing of their personal data in the circumstances of this complaint was reasonable.

CASE STUDY 101

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

A complaint was lodged directly with the DPC on 2 July 2019 against Twitter International Company ("Twitter"), and accordingly was handled by the DPC in its role as lead supervisory authority. The complainant alleged that, following the suspension of their Twitter account, Twitter failed to comply within the statutory timeframe with an erasure request they had submitted to it. Further, the complainant alleged that Twitter had requested a copy of their photographic ID in order to action their erasure request without a legal basis to do so. Finally, the complainant alleged that Twitter had retained their personal data following their erasure request without a legal basis to do so.

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

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

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

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

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

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

- Article 5(1)(c): Twitter's requirement that the complainant verify his identity by way of submission of a copy of his photographic ID constituted an infringe-

ment of the principle of data minimisation, pursuant to Article 5(1)(c) of the GDPR;

- Article 6(1): Twitter had not identified a valid lawful basis under Article 6(1) of the GDPR for seeking a copy of the complainant's photographic ID in order to process his erasure request;
- Article 17(1): Twitter infringed Article 17(1) of the GDPR, as there was an undue delay in handling the complainant's request for erasure; and
- Article 12(3): Twitter infringed Article 12(3) of the GDPR by failing to inform the data subject within one month of the action taken on his erasure request pursuant to Article 17 of the GDPR.

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

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

Law Enforcement Directive (LED)

CASE STUDY 102

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

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

The matter related to an individual seeking copies of allegations of abuse made against him with regard to the welfare of his parents. Having examined this matter, it was clear to the DPC that releasing the information would entail the release of third-party data and would reveal the identity of the person making the allegations. The DPC was satisfied on review that the information sought was provided in the strictest of confidence and considered the provisions of Section 91(9)(a) also applied.

CASE STUDY 103

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

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

An Garda Síochána refused to supply the data. The DPC advised the parent that it agreed with the restriction imposed, as the controller in this case had particular knowledge of all of the circumstances pertaining to a shared guardianship arrangement in place and considered that consent of all legal guardians would be required in order to release the data in this case.

CASE STUDY 104

Purpose Limitation — Law Enforcement Directive

The DPC examined a complaint where an individual alleged that data gathered in one particular law enforcement context was being used by the same data controller for another law enforcement purpose. The complaint concerned the prosecution of an individual for offences in the equine and animal remedies area by the Department of Agriculture, Food and the Marine (DAFM) and the separate referral by DAFM of allegations of professional misconduct to the Veterinary Council of Ireland (VCI) in relation to the same person.

Having examined the matters raised, the DPC referred the complainant to Section 71(5) of the Data Protection Act 2018:

Where a controller collects personal data for a purpose specified in section 70 (1)(a), the controller or another controller may process the data for a purpose so specified other than the purpose for which the data were collected, in so far as— (a) the controller is authorised to process such personal data for such a purpose in accordance with the law of the European Union or the law of the State, and (b) the processing is necessary and proportionate to the purpose for which the data are being processed.

With regard to section 70(1)(a) and "the law of the State", the DPC noted the provisions set out in the Veterinary Practice Act 2005 regarding the conduct of inquiries by the VCI into allegations of professional misconduct. In particular, section 76 of the Veterinary Practice Act 2005 outlines that the VCI or any person may apply for an inquiry with regards to the fitness to practice veterinary medicine of a registered person. On this basis, the DPC did not consider data protection legislation to disallow the separate referral by DAFM of allegations of professional misconduct to the VCI in relation to a person, in tandem with prosecution proceedings by DAFM against the same individual for offences in the equine and animal remedies area.

CASE STUDY 105

Data restrictions — prosecutions pending (Law Enforcement Directive)

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

In some cases, An Garda Síochána may supply an individual with a copy of their statement provided by the individuals but will withhold other data on the basis of Section 94(3)(a) of the Act whereby a data controller may restrict access, wholly or partly, for the purposes of "the prevention, detection or investigation of offences, the apprehension or prosecution of offenders or the effectiveness of lawful methods, systems, plans or procedures employed for the purposes of the matters aforesaid."

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

CASE STUDY 106

Access restrictions (Law Enforcement Directive)

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

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

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

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

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

CASE STUDY 107

Law Enforcement Directive (LED)

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

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

Objection to Processing

CASE STUDY 108

Use of location data to verify expense claims

The complainant in this case study was a former employee of a statutory service provider, whose work involved driving to locations assigned by his employer. Where this gave rise to claims for overtime or subsistence, the complainant would complete forms provided by the employer, detailing items such as relevant dates and places, dispatch reference numbers, and the amounts claimed. The employer made use of a dispatch system intended to ensure the most efficient use of drivers and vehicles, particularly as they provided response in emergency situations. This system logged the performance and completion of service calls, when vehicles were out on calls or back at base, and when drivers were on or off duty.

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

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

The employer did not have a written policy on the use of the dispatch system. Instead, it relied on the "general awareness" of employees that the system was used for that purpose. The employer pointed out that such use had been noted in an arrangement with its employees' trade unions some years previously. The DPC noted that overtime and subsistence claims required employees to include relevant dispatch reference numbers from the dispatch system. The DPC took the view that the inclusion of relevant dispatch system reference numbers in overtime and subsistence claims indicated that employees were aware that the data was used not just for logistical processing but also to verify their claims. Even if the major purpose of the dispatch system was to aid logistics, its use to verify overtime claims was not incompatible with that purpose, as that data was the only means available to the employer to verify claims.

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

This case is an example of when data collected for one legitimate purpose — in this case, logistical control — may be appropriately processed for another, in this case

verifying overtime claims. However, controllers should bear in mind the overarching requirement to process personal data fairly and must ensure that data subjects are made aware of what data is collected, and the nature and purpose of the processing. Equally important is that the processing have a legal basis, which in most cases will require that the processing is necessary for the stated purpose.

CASE STUDY 109

Fair obtaining complaint made against a Golf Club

An individual made a complaint to the DPC concerning the data controller's use of CCTV footage to investigate an incident in which the individual was involved. The individual had organised an event in a leisure facility (the data controller), and displayed signage in relation to Covid-19 procedures to assist attendees. At the end of the event, the individual inadvertently removed a different sign also in relation to Covid-19 procedures when removing the signage they had installed for the event. The data controller reviewed its CCTV footage to establish who had removed the sign. The complainant was of the opinion that the data controller did not process their personal data in a proportionate or transparent manner, and that it did not comply with its obligations as a data controller in how it investigated the incident. Accordingly, the individual lodged a complaint with the DPC.

The DPC intervened to seek to resolve the matter informally and the parties reached an amicable resolution when the leisure centre agreed to undertake an audit of its use of the CCTV system and to restrict access to review CCTV footage to designated staff members. The individual thanked the DPC for handling their complaint in a professional and helpful manner and further stated that they were reluctant to submit the complaint initially as they are aware of the volume of complaints the DPC deals with and the accompanying constraints on resources. The complainant stated that they felt confident that the issue will not arise in the future as a result of the involvement of the DPC. The individual wished to express their appreciation and acknowledge the DPC's efficiency in dealing with the matter.

CASE STUDY 110

Unlawful processing arising from billing error (Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

In April 2018, we received a complaint from a data subject who had ceased to be a customer of the data controller. However, she had discovered that her data was still being processed as she continued to receive bills from the data controller. The complainant had received verbal and written assurances that she did not owe the amount being billed.

However, he complainant subsequently received a text message from a debt-collection company, asking that she contact them. When the complainant phoned the debt-collection company, it refused to provide her with any information regarding the alleged debt until she provided them with personal data verifying her identity, which she refused to do. Later the same day, the complainant received a letter from the debt-collection company confirming that it was seeking to recover monies owed by her to the data controller.

This complaint was identified as potentially capable of amicable resolution under Section 109 of the Data Protection Act 2018, with both the complainant and data controller agreeing to work with the DPC to try to amicably resolve the matter. Company A confirmed with the DPC that an error had caused the complainant's account balance to appear outstanding but that when

the error was identified by the data controller, the outstanding balance was removed from the account. The data controller also confirmed that it had instructed the debt-collection company to cease any collection activities, and also to delete any data associated with the complainant.

While the complainant was satisfied with the ultimate outcome, the DPC emphasised to the data controller that the complainant had previously been informed on at least two occasions that the matter had been resolved. Despite this, her data had been unfairly processed by being passed to a debt-collection company without there being any justification for such disclosure.

In recognition of its failings, the data controller apologised to the complainant, provided certain assurances to her that the matter would have no effect on her credit rating, and made donations to charities of her choice.

For a controller to lawfully engage a processor to process personal data, there must be a justification for the processing of the personal data in the first place. In this case, the controller had disregarded previous concerns raised by the complainant that bills were being issued to her despite her no longer receiving services from the controller and had failed to look into the continued use of her personal data for billing purposes in circumstances where she was no longer a customer. The DPC encourages individuals to raise data protection concerns directly with the controller in the first instance so that they can address them.

However, data controllers frequently ignore or disregard direct attempts made by a data subject to raise complaints until the DPC becomes involved. This is unacceptable and, as part of each organisation's accountability obligations, it should have meaningful and efficient measures in place to deal with and address data protection complaints when raised directly by a data subject, without the need for the data subject to resort to DPC intervention.

CASE STUDY 111

Receivers and fair processing

We received a complaint against a private receiver who was appointed by a financial institution over the complainant's property.

The complaint alleged infringements of the Acts on the basis that the receiver:

- Was not registered as a controller pursuant to section 16 of the Acts;
- Had no lawful basis for obtaining the complainant's personal data from the financial institution;
- Further processed personal data unlawfully by disclosing information to a company appointed by the receiver to manage the receivership (the receiver's "managing agent");
- Opened a bank account in the complainant's name;
- Obtained the property ID and PIN from Revenue which gave the receiver access to the complainant's personal online Revenue account; and
- Insured the property in the complainant's name.

Following an investigation pursuant to section 10 of the Acts, the DPC established that the receiver was appointed by the financial institution on foot of a Deed of Appointment of Receiver (DOA), which granted the receiver powers pursuant to the Conveyancing Act 1881, and pursuant to the mortgage deed between the complainant and the financial institution. On being appointed, the receiver wrote to the complainant informing them of their appointment as the receiver over the complainant's property and provided a copy of the DOA. The receiver appointed a separate company as their managing agent to assist in the managing of the property. During the receivership, the receiver liaised with Revenue in order to pay any outstanding taxes on the property, such as the Local Property Tax (LPT). It was also established that the receiver opened a bank account for the purpose of managing the income from the property. The bank account name included the name of the complainant. It was further established that an insurance policy was taken out, in respect of the property. This insurance policy referred to the complainant's name.

The DPC first considered whether a receiver was required to register as a data controller in accordance with section 16 the Acts, and whether the exemptions listed in the Data Protection Act 1988 (Section 16(1)) Regulations 2007 (the "Registration Regulations") applied. The DPC held that a receiver was not required to register, as the exemption under regulation 3(1)(g) of the Registration Regulations applied to the receiver. Regulation 3(1)(g) exempted data controllers who were processing data in relation to its customers. Having considered the relationship between the complainant and the receiver, the DPC held that the

exemption applied in respect of the receiver's activities regarding the complainant.

Next the DPC considered whether the receiver had a lawful basis for obtaining the personal data from the financial institution, disclosing it to the managing agent, and whether such processing constituted further processing incompatible with the original purpose it was obtained pursuant to section 2(1)(c)(ii) of the Acts. The complainant had a mortgage with the financial institution, which had fallen into arrears. Under section 19(1)(ii) of the Conveyancing Act 1881, the financial institution could appoint a receiver once the debt on the mortgage had come due. Section 2A(1)(b)(i) of the Acts permits processing of personal data where the processing is necessary "for the performance of a contract to which the data subject is party". The mortgage deed was a contract between the data subject and the financial institution, and in circumstances where the terms of the contract were not being adhered to, the appointment of the receiver by the financial institution was necessary for the performance of the contact. The DPC held that the receiver had a lawful basis for obtaining the complainant's personal data from the financial institution.

The DPC also found that the receiver had a lawful basis pursuant to section 2A(1)(b)(i) of the Acts to disclose personal data to its managing agent, to assist in the day to day managing of the receivership. The DPC found that the financial institution obtained the complainant's personal data for the purposes of entering into a loan agreement. This was specific, explicit and a legitimate purpose. The disclosure of the complainant's personal data by the financial institution to the receiver, and by the receiver to the managing agent was in accordance with the initial purpose for which the personal data was obtained. This processing during the receivership did not constitute further processing pursuant to section 2(1)(c)(ii) of the Acts. The DPC assessed whether the receiver had a lawful basis to open a bank account in the complainant's name. The complainant submitted that this account was opened without their knowledge or consent. Consent is one of the lawful bases for processing personal data under the Acts. The DPC considered whether the receiver otherwise had a lawful basis for processing under section 2A(1)(d) of the Acts, on the basis of legitimate interests. To assess this lawful basis, the DPC took account of the Court of Justice of the European Union (CJEU) case in Rīgas C-13/16(1) which sets out a three step test for processing on the basis of legitimate interests, as follows:

Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme' Case C-13/16

- The processing of personal data must be for the pursuit of a legitimate interest of the controller or a third party;
- The processing must be necessary for the purpose and legitimate interests pursued; and
- The fundamental rights and freedoms of the individual concerned do not take precedence.

The DPC held that the opening of the bank account was a reasonable measure to manage the income and expenditure during a receivership. The receiver submitted that referring to complainant's name as part of the bank account name was necessary to ensure the receivership was carried out efficiently and to avoid confusion between different receiverships. While it would have been possible to open an account without using the complainant's name, the DPC took account of the CJEU's judgment in Huber v Bundesrepublik C-524/062 where the Court held that processing could be considered necessary where it allowed the relevant objective to be more effectively achieved. The DPC held that the reference to the complainant's name on the bank account was therefore necessary, as it allowed for the more effective pursuit of the receiver's legitimate interests.

With regard the third element of the legitimate interests test (which requires a balancing exercise, taking into account the fundamental rights and freedoms of the data subject), the DPC held that the reference to the complainant's name on the account would have identified them to individuals who had access to the bank account or been supplied with the bank account name. The DPC balanced these concerns against the administrative and financial costs, which would result from the need for the receiver to implement an alternative procedure for naming accounts. On balance, the DPC did not find that the complainant's fundamental rights took precedence over the legitimate interests of the receiver and as a result, the receiver had a lawful basis for processing the complainant's name, for the purpose of the receiver's legitimate interests.

With regard to the allegation that the receiver had gained access to the personal Revenue account of the complainant, the DPC found that the receiver did not gain access to the complainant's personal online Revenue account as alleged. The receiver was acting as a tax agent in relation to the LPT and this did not allow access to a personal Revenue account. In relation to the insurance policy being taken out in the complainant's name the DPC held that the receiver did not process personal data in this instance.

During the course of the investigation, the DPC also examined whether the receiver had complied with the data protection principles under section 2 of the Acts. In this regard, the DPC examined the initial correspondence the receiver had sent to the complainant notifying them of their appointment. This correspondence consisted of a cover letter and a copy of the DOA. The cover letter and DOA were assessed in order to determine whether the

receiver had met their obligation to process the personal data fairly. Section 2D of the Acts required an organisation in control of personal data to provide information on the identity of the data controller, information on the intended purposes for which the data may be processed, the categories of the data concerned as well as any other information necessary to enable fair processing. The DPC held that the correspondence was sufficient in informing the complainant of the identity of the data controller (and original data controller). However, the DPC held that, while a receiver was not required to provide granular information on each purpose for which personal data was to be processed, the receiver should have given a broad outline of the purposes for which the personal data was intended to be processed, and this was not done in this case. It was also held that the receiver should have provided the categories of personal data they held in relation to the complainant, but this was not done. In light of this, the DPC held that the receiver had not complied with section 2D of the Acts.

This decision of the DPC demonstrates that private receivers and their agents may lawfully process personal data of borrowers, where such processing is necessary in order to manage and realise secured assets. Individuals should be aware that their information may be processed without their consent in circumstances where a deed of mortgage provides for the appointment of a receiver. At the same time, receivers must comply with their obligations under the Acts and GDPR to provide individuals with information on processing at the outset of the receivership. The decision is currently the subject of an appeal by the complainant to the Circuit Court.

1. Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme' Case C-13/16

2. Heinz Huber v Bundesrepublik Deutschland Case C-524/06

3. The processing of personal data was considered in a similar case where the same complainant made a complaint against the managing agent in this case. In that decision the DPC held that the managing agent had legitimate interest in processing the complainant's personal data for the purposes of insuring the property.

CASE STUDY 112

Unauthorised publication of a photograph (Amicable Resolution)

The DPC received a complaint from an individual regarding the publication of their photograph in an article contained in a workplace newsletter without their consent. The data controller, who was the individual's public sector employer, informed the individual that it should have obtained consent to use the photograph in the workplace newsletter as this was not the purpose for which the photograph was obtained. The data controller also informed the individual that a data breach had occurred in this instance.

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

The data controller engaged with the DPC on the matter, and advised that it had conducted an internal investigation and determined that a data breach did occur and that consent should have been obtained to use the individual's photograph in the workplace newsletter. The purpose(s) for which the photograph was initial obtained did not include publication in a newsletter. An apology from the employer was issued to the individual. However, the complainant did not deem this to be an appropriate resolution to the complaint at hand.

The DPC provided recommendations that a consent information leaflet be distributed to staff in advance of using photography, audio and/or video, and that a consent form for photography, audio and video be completed and signed prior to images or recordings being obtained, which the controller subsequently implemented.

Article 5(1)(b) of the GDPR states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation') The DPC was satisfied that the data controller further processed the individual's personal data without their consent (or other legal basis) for doing so when it published the employee photograph in the workplace newsletter. The DPC issued an outcome letter advising the complainant of same. The

DPC was satisfied with the organisational measures subsequently introduced and as such no further actions by the controller in this case was warranted.

In this case study, the risks to the fundamental rights and freedoms of the individual could not be deemed significant, but nonetheless the personal data processing upset the individual and is an infringement of GDPR in the circumstances. This underlines the need for all organisations to train staff — at all levels and in all roles — to be aware of the GDPR and take account of its principles.

CASE STUDY 113

Processing of footage of funeral service by parish church (Amicable Resolution)

Annual Report 2021 Case Study 3 (Applicable Law — GDPR and Data Protection Act 2018)

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

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

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

CASE STUDY 114

Further processing for a compatible purpose

The complainant was a solicitor who engaged another solicitor to represent them in legal proceedings. The relationship between the complainant and the solicitor engaged by the complainant broke down and the solicitor raised a grievance about the complainant's behaviour to the Law Society. In this context, the solicitor provided certain information about the complainant to the Law Society. The complainant referred the matter to the DPC, alleging that the solicitor had contravened data protection legislation.

It was established that the complainant's solicitor was the data controller, as it controlled the contents and use of the complainant's personal data for the purpose of providing legal services to the complainant. The data in question consisted of (amongst other things) information relating to the complainant's legal proceedings and was personal data because the complainant could be identified from it and it related to the complainant as an individual.

The DPC noted Law Society's jurisdiction to handle grievances relating to the misconduct of solicitors (by virtue of the Solicitors Acts 1954-2015). It also accepted that the type of misconduct that the Law Society may investigate includes any conduct that might damage the reputation of the profession. The DPC also noted that the Law Society accepts jurisdiction to investigate complaints made by solicitors about other solicitors (and not just complaints made by or on behalf of clients) and its code of conduct requires that, if a solicitor believes another solicitor is engaged in misconduct, it should be reported to the Law Society. The DPC therefore considered that the complaint made by the data controller to the Law Society was properly made and that it was for the Law Society to adjudicate on the merit of the complaint.

The DPC then considered whether the data controller had committed a breach of data protection legislation. In this regard, the DPC noted that data controllers must comply with certain legal principles that are set out in the relevant legislation. Of particular relevance to this complaint was the requirement that data must be obtained for specified purposes and not further processed in a manner that is incompatible with those purposes. The DPC established that the reason the complainant's personal data was initially collected/processed was for the purpose of providing the complainant with legal services. The DPC pointed out that when the data controller made a complaint to the Law Society, it conducted further processing of the complainant's personal data. As the further processing was for a purpose that was different to the purpose for which it was collected, the DPC had to consider whether the purpose underlying the further processing was incompatible with the original purpose.

The DPC confirmed that a different purpose is not necessarily an incompatible purpose and that incompatibility should always be assessed on a case-by-case basis. In this case, the DPC held that, because there is a public interest in ensuring the proper regulation of the legal profession, the purpose for which the complainant's data was further processed was not incompatible with the purpose for which it was originally collected. On this basis, the data controller had acted in accordance with data protection legislation.

The DPC then noted that, in addition to other legal requirements, a data controller must have a lawful basis for processing personal data. The lawful basis that the data controller sought to rely on in this case was that the processing was necessary for the purposes of the legitimate interests pursued by the data controller. In this regard, the DPC held that the data controller had a legitimate interest in disclosing to the Law Society any behaviour that could bring the reputation of the legal profession into disrepute. Further, the data controller was required by the Law Society's Code of Conduct to report serious misconduct to the Law Society). As a result, the DPC was of the view that the data controller had a valid legal basis for disclosing the complainant's personal data and had not contravened the legislation.

Under Article 6 of the GDPR, a data controller must have a valid legal basis for processing personal data. One such legal basis, in Article 6(1)(f) of the GDPR, provides that processing is lawful if and to the extent that it is necessary for the purpose of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights or freedoms of the data subject. However, Article 6(4) of the GDPR provides that where processing of personal data is carried out for a purpose other than that for which the data were initially collected, this is only permitted where that further processing is compatible with the purposes for which the personal data were initially collected.

In considering whether processing for another purpose is compatible with the purpose for which the personal data were initially collected, data controllers should take

into account (i) any link between the purposes for which the data were collected and the purposes of the intended further processing, (ii) the context in which the data were collected, (iii) the nature of the personal data, (iv) the possible consequences of the intended further processing for data subjects, and (v) the existence of appropriate safeguards.

CASE STUDY 115

Processing that is necessary for the purpose of legitimate interests pursued by a controller

This complainant was an employee of a shop located in a shopping centre and was involved in an incident in the shopping centre car park regarding payment of the car park fee. After the incident, the manager of the car park made a complaint to the complainant's employer and images from the CCTV footage were provided to the complainant's employer. The complainant referred the matter to the DPC to examine whether the disclosure of the CCTV images was lawful.

It was established that the shopping centre was the data controller as it controlled the contents and use of the complainant's personal information for the purposes of disclosing the CCTV stills to the complainant's employer. The data in question consisted of images of the complainant and was personal data because it related to the complainant as an individual and the complainant could be identified from it.

The data controller argued that it had a legitimate interest in disclosing the CCTV images to the complainant's employer, for example, to prevent people from exiting the car park without paying and to withdraw the agreement it had with the complainant's employer regarding its staff parking in the car park. The DPC noted that a data controller must have a lawful basis on which to process a person's personal data. One of the legal bases that can be relied on by a data controller is that the processing is necessary for the purposes of legitimate interests pursued by the data controller. (This was the legal basis that the data controller sought to rely on here.) The DPC acknowledged that the data controller had in principle a legitimate interest, in disclosing the complainant's personal data for the reasons that it put forward. However, it was not "necessary" for the data controller to disclose the CCTV stills to the complainant's employer for the purposes of pursuing those legitimate interests. This was because the car park attendant employed by the data controller had discretion to take steps against the complainant, in pursuit of the legitimate interests, without the need to involve the complainant's employer. For example, the car park attendant had discretion to ban the complainant from using the car park without involving the complainant's employer. On this basis, the DPC determined that it was not necessary for the data controller to notify the complainant's employer of the incident and provide it with CCTV stills. Accordingly, the data controller had no legal basis for doing so and had contravened data protection legislation.

Under Article 6 of the GDPR, personal data can be processed only where there is a lawful basis for doing so. One such legal basis is under Article 6(1)(f), which provides that processing is lawful if and to the extent that it is necessary for the purpose of the legitimate interests pursued by the controller or by a third-party, except where such interests are overridden by the interests or fundamental rights or freedoms of the data subject. Data controllers should be aware, however, that it is not sufficient merely to show that there is a legitimate interest in processing the personal data; Articles 5(1)(c) and 6(1)(f) require data controllers to be able to show that the processing in question is limited to what is "necessary" for the purpose of those legitimate interests.

CASE STUDY 116

Processing that is necessary for the purpose of performance of a contract

This complainant was involved in an incident in a carpark of a building in which they worked. A complaint was made by the manager of the car park to the complainant's employer and images from the CCTV footage of the incident were subsequently obtained by the complainant's employer. Disciplinary proceedings were then taken against the complainant arising out of the car park incident. The complainant's manager and other colleagues of the complainant viewed the CCTV stills in the context of the disciplinary proceedings.

The complainant's employer was the data controller in relation to the complaint, because it controlled the contents and use of the complainant's personal data for the purposes of managing the complainant's employment and conducting the disciplinary proceedings. The data in question consisted of images of the complainant and was personal data because it related to the complainant as an individual and the complainant was identifiable from it.

In response to the complaint, the data controller maintained that it had a lawful basis for processing the complainant's personal data under the legislation because the CCTV images were used to enforce the employee code of conduct, which formed part of the complainant's contract of employment. It also stated that, because of the serious nature of the incident involving the complainant, it was necessary for the data controller to investigate the incident in accordance with the company disciplinary policy, which was referred to in the complainant's employment contract. The data controller also argued that the CCTV stills were limited to the incident in question and that only a limited number of personnel involved in the disciplinary process viewed them.

The DPC noted that data protection legislation permits the processing of a person's personal data where the processing is necessary for the performance of a contract to which the data subject (the person whose personal data is being processed) is a party. The DPC noted the data controller here sought to argue that the use of the CCTV images was necessary for the performance of the complainant's employment contract. However, the DPC was of the view that it was not 'necessary' for the data controller to process the complainant's personal data contained in the CCTV images to perform that contract. For this argument to succeed, the data controller would have had to show that it could not have performed the complainant's employment contract without processing the complainant's personal data. As the data controller had failed to satisfy the DPC that this was the case, the data controller was judged to have infringed the data protection legislation.

The DPC also noted that, in addition to the requirement to have a lawful basis for processing, there are also certain legal principles that a data controller must comply with, when processing personal data. It highlighted that the processing must be adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed. The DPC noted the data controller's argument that the CCTV stills were limited to the incident in question and that only a limited number of personnel involved in the disciplinary process viewed the stills. However, the DPC was of the view that the data controller had failed to show why it was necessary to use the CCTV images. On this basis, there had been a further infringement of the legislation by the data controller.

Under Article 6 of the GDPR, personal data can be processed only where there is a lawful basis for doing so. One such legal basis is under Article 6(1)(b), which provides that processing is lawful if and to the extent that it is necessary for the performance of a contract to which the data subject is a party. Data controllers should be aware, however, that it is not sufficient merely to show that there is a contractual basis for processing the personal data; Articles 5(1)(c) and 6(1)(b) require data controllers to be able to show that the processing in question is limited to what is "necessary" for the purpose of performance of the contract.

CASE STUDY 117

Fair and lawful processing of CCTV images of a customer

This complaint concerned the processing of the complainant's personal data in the form of a still image from CCTV footage taken in a betting shop, by distributing that image to various betting shops in the chain with a warning note to staff in order to prevent the complainant from placing bets.

The Commission determined that the betting shop was the data controller because it controlled and processed the personal data in question. The data were (amongst other things) an image of the complainant and internal notes circulated to staff of the data controller about the complainant. The data were personal data because they related to the complainant as an individual and the complainant could be identified from the data.

In response to the complaint, the data controller put forward a number of reasons for processing the complainant's personal data and sought to argue that there was a valid legal basis for each purpose, as provided for in data protection legislation.

The reasons and corresponding legal bases presented by the data controller included the following:

1. Legal and Regulatory Obligations: The data controller argued that it is required to retain and use personal data in order to comply with certain legal and regulatory obligations, such as to detect suspicious betting activity and fraudulent transactions under applicable criminal justice legislation. The legal basis put forward by the data controller was that the processing was lawful because it was necessary for the data controller to comply with a legal obligation.
2. Risk Management: The data controller claimed that it records personal data relating to customers for commercial risk management. The legal basis put forward in this regard was that the processing was lawful because it was necessary for the purposes of the legitimate interests pursued by the data controller.
3. Profiling: The data controller confirmed that it carries out profiling of customer betting activity to (amongst other things) improve customer experience. The data controller argued that such processing is lawful as it is necessary for compliance with legal obligations and for the purposes of the legitimate interests pursued by the data controller.

The Commission decided that the data controller had identified an appropriate lawful basis for each purpose for which it processed personal data relating to its customers.

The Commission then considered whether the obligation to process personal data fairly had been complied with by the data controller. In this context, the Commission noted that the data controller is obliged to provide the complainant with information in relation to the key elements of the collection and use of the complainant's personal data. The data controller here had provided the complainant with an internal company document and confirmed that the complainant's personal data had been processed in accordance with this document. However, the document was dated after the date on which the complainant's personal data was processed. On this basis, the Commission noted that it was not clear that the required information had been provided to the complainant and therefore the data controller had failed to process the complainant's personal data fairly.

Finally the Commission considered the period of time the personal data had been retained for. In this regard, it noted that the relevant legislation requires that a data controller keep personal data for no longer than is necessary for the purposes for which the data are processed. The complainant's personal data had been kept for approximately seven years. The Commission considered that because the data controller had a legitimate interest in retaining the complainant's data (for commercial risk management), the data controller had acted in accordance with the legislation in this regard.

Under Article 6 of the GDPR, a data controller must have a valid lawful basis for processing personal data. Amongst the available lawful bases are that the processing of personal data is necessary for the purpose of the legitimate interests pursued by the data controller or that the processing is necessary for compliance with a legal obligation to which the data controller is subject. The data controller must have a lawful basis not just for the initial obtaining of the personal data, but also for their ongoing processing, including storage, and the data must not be kept for longer than is necessary for the purpose for which they are processed (Article 5(1)(e) GDPR).

In addition to having a valid lawful basis for processing of personal data, however, a data controller must comply with a number of further obligations in relation to personal data being processed. In particular, personal data must be processed fairly and transparently. To this end, a data controller is required to provide a data subject with certain information under Article 13 of 14 of the GDPR, in accordance with the requirements of Article 12 GDPR. The information required to be provided to the

data subject includes the identity and contact details of the controller and the controller's data protection officer, where applicable, the purposes of the processing, and the recipients or categories of recipients of the data, if any. The information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

CASE STUDY 118

Unlawful processing and disclosure of special category data

A data subject submitted a complaint to the Data Protection Commission (DPC) against their bank (the data controller) as they believed their personal data was processed unlawfully. The data subject explained that they held a mortgage with the data controller, and this mortgage was sold to another bank, as part of a loan sale agreement. The data subject complained that this sale was processed without their prior knowledge or consent and was specifically concerned about the data controller sharing their personal email address and mobile phone number with another bank as they deemed this as an excessive disclosure of personal data. While the data subject did not object to their name, address or landline number being shared, they believed their email address and mobile phone number were "sensitive" personal data and the disclosure of same was disproportionate.

Prior to contacting the DPC, the data subject engaged with the data controller directly regarding their complaint. The data controller responded to the data subject and advised that their lawful basis for processing their personal data was Article 6(1)(f) of the General Data Protection Regulation (GDPR) which states: "Processing is necessary for the purposes of the legitimate interests pursued by the controller."

Upon commencing their examination, the DPC shared the data subject's complaint with the data controller and requested a detailed response. The data controller informed the DPC that as part of their Data Privacy Notice, a copy of which is provided to their customers, details that the data controller may sell assets of the company in order to manage their business. This is also further detailed in the loan offer letter to mortgage applicants.

In relation to the sharing of excessive personal data, the data controller outlined that they do not consider an email address or a mobile phone number to be sensitive information nor do they fall under special categories of personal data under Article 9 of the GDPR.

The DPC advised that while consent is one of six lawful basis for processing personal data, it is lawful to process personal data without prior consent once one of the five other bases, which are listed in Article 6 of the GDPR, are met. In this instance the data controller was relying on Article 6(1)(f) and as such, they are required to conduct a balancing test to ensure that the legitimate interest that are pursued by the controller are not overridden by the interests, rights, or fundamental freedoms of the data subject. The data controller confirmed to the DPC that they had conducted a balancing test and it was confirmed that the processing of personal data, in this instance, did not override the interests, rights or fundamental freedoms of the data subject.

The data controller further explained that it was necessary for the data controller to share the data subject's contact information with the other bank as they were the new data controllers for the data subject's loan. The data controller also clarified that they do not differentiate between different types of contact information, i.e. landline and mobile numbers as this information was provided to the data controller for the purpose of contacting customers. As such, this information is required by the bank managing the loan.

Article 9 of the GDPR describes special category personal data as:

"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

As such, the DPC clarified to the data subject that mobile numbers and email addresses do not fall into this category. Under section 109(5)(c) of the 2018 Act the DPC advised the data subject that, having examined their complaint, the DPC found no evidence that their personal data was processed unlawfully. While the data controller relied on a legitimate basis to process data, they did so in a transparent manner, and kept the data subject fully informed at all key stages of the sale, so it was conducted with the data subject's prior knowledge. The DPC did not consider any further action necessary at the time of issuing the outcome.

CASE STUDY 119

Unlawful processing of special category data

A data subject issued a complaint to the Data Protection Commission (DPC) against their employer (data controller) regarding the processing of their health data under Article 9 of the General Data Protection Regulation (GDPR). The data subject explained to the DPC that they had been signed off work by their GP and so, presented their medical certificate to their employer, in an envelope addressed to the organisation's Medical Officer. A staff member in an acting-up manager role, opened the medical cert; however, this person's role was not as a medical officer. Before contacting the DPC the data subject contacted their employer to address their concerns that they felt their sensitive personal data had been unlawfully processed; however, they did not receive a response to their complaint.

As part of its examination, the DPC engaged with the data controller and shared the details of the data subject's complaint. The data controller responded to the DPC and explained that, as per their organisation's Standard Operating Procedures, as there was no medical officer on duty on the day in question, the responsibility and authority for granting leave, sick or otherwise, automatically falls to the manager on the day, who in this instance was the manager who processed the medical certificate.

The data subject did not accept the explanation provided by the data controller and contested that a medical certificate should not be processed by anyone who is not the designated medical officer.

Through its examination, the DPC found that, under section 109(5)(c) of the 2018 Act, the data controller had a legitimate basis to process the data subject's sensitive personal data under the GDPR and so no unlawful processing had occurred. No further action against the data controller was considered necessary in relation to the data subject's complaint.

CASE STUDY 120

Fair processing of personal data (Applicable Law — GDPR and Data Protection Act 2018)

A data subject issued a complaint to the Data Protection Commission (DPC) against their employer (data controller) regarding the processing of their personal data under the General Data Protection Regulation (GDPR). The data subject explained to the DPC that details of a confidential matter as part of a reference was given to a third party (a prospective employer). Before contacting the DPC the data subject contacted the data controller to address their concerns as they felt their personal data had been unlawfully processed; however, they did not receive a satisfactory response to their complaint.

The DPC notes that the provision of a reference about a staff member from a present/former employer, to a third party, such as a prospective employer, will generally involve the disclosure of personal data. The data subject mentioned that the data controller disclosed a confidential matter in the reference provided to the prospective employer.

As part of its examination, the DPC engaged with the data controller and shared the details of the data subject's complaint. The data controller responded to the DPC and explained that, it is relying on consent and legitimate interest for disclosing the confidential matter. The data controller outlined that in balancing the data subject's rights against the interests of the third party (and those to whom it provides care) it determined that it had a duty of care to ensure that the recipient of the reference (prospective employer) received a reference which was true, accurate, fair and relevant to the role which the data subject had applied for.

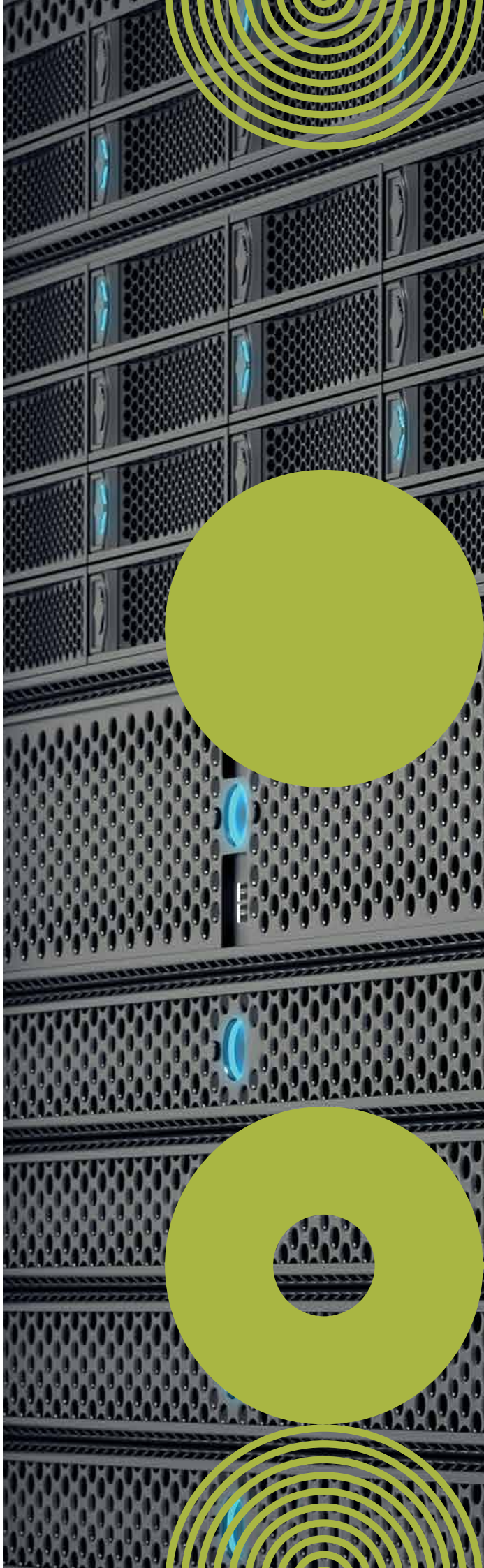
The data controller was satisfied that the data was processed, fairly and in a transparent manner. It further stated that due to the nature of the employment it had a

duty of care not only to the people they support, the staff members, but also to prospective employers who provide support services to same category of clients.

It is important to consider whether the status of the data controller, the applicable legal or contractual obligations (or other assurances made at the time of collection) could give rise to reasonable expectations of stricter confidentiality and stricter limitations on further use. The DPC has taken into consideration whether the data controller could have achieved the same result without disclosing the confidential details to the prospective employer. The statements made in the reference were based on facts, which could be proven and were necessary to achieve the legitimate interests of and the duty of care of the data controller's clients.

The DPC is satisfied that despite the duty of confidence, and in circumstances where the data subject nominated the data controller to provide the reference, thus consented to the sharing of the data subject's relevant personal data to a prospective employer, the prospective employer's legitimate interest and the wider public interest justifies the disclosure of the confidential matter.

Having examined the matter thoroughly, under section 109(5)(c) of the 2018 Act the DPC advised the data subject that the explanation put forward by the data controller in the circumstances of this complaint are reasonable and no unlawful processing had occurred. Accordingly, no further action against the data controller was considered necessary in relation to the data subject's complaint.



Purpose Limitation

CASE STUDY 121

Use of CCTV in the workplace

We received a complaint that concerned the use of CCTV cameras by the data controller in the complainant's work premises, and the viewing of that CCTV footage (which contained personal data of the complainant, consisting of, among other things, images of the complainant) for the purpose of monitoring the complainant's performance in the course of his employment with the data controller.

At the time of the complaint, the data controller had a CCTV policy in place, which stated that the reason for the CCTV system was for security and safety. This was also stated on signage in place in areas where the CCTV cameras were in operation. The facts indicated that the purposes for which the complainant's personal data was initially collected were security and safety. However, during a meeting with the complainant, a manager informed the complainant that CCTV footage containing the complainant's personal data had been reviewed solely for the purposes of monitoring the complainant's performance in the course of the complainant's employment with the data controller. This purpose was not one of the specified purposes of processing set out in the CCTV policy and signage. The controller acknowledged that the use of the complainant's personal data in this way was a contravention of its policies.

Where personal data is processed for a purpose that is different from the one for which it was collected, the purposes underlying such further processing must not be incompatible with the original purposes. In relation to the use of the complainant's personal data, the purpose of monitoring their performance was separate and distinct from the original purposes of security and safety for which the CCTV footage was collected. On that basis, the processing of the complainant's personal data contained in the CCTV footage for the purpose of monitoring performance was further processing for a purpose that was incompatible with the original purposes of its collection.

A further issue arose regarding the security around the manner in which the CCTV system and CCTV logs were accessed. In written responses to the DPC, the controller stated that, at the time of the complaint, access to CCTV footage was available on a standalone PC in the department, which did not require log-in information. The responses from the controller indicated that access to CCTV footage was not logged either manually or automatically. The absence of an access log for the CCTV footage was a deficiency in data security generally. Data controllers must implement appropriate security and organisational measures, in line with Article 32 of the GDPR, in relation to conditions around access to personal data.

The CCTV policy has since been substantially revised and replaced by a new policy. The controller confirmed that the PC utilised has now been deactivated and removed. Access to CCTV recordings is now limited to a single individual in the specific unit and recordings are reviewed only in the event of a security incident or accident.

Of particular relevance in this type of situation are the obligations to process personal data fairly (Article 5(1)(a)), and to obtain such data for specific purposes and not further process it in a manner that is incompatible with those purposes (Article 5(1)(b)). Further, appropriate security measures should be in place to ensure the security of the personal data (Article 5(1)(f) and Article 32).

CASE STUDY 122

Processing of Special Category Data

This complaint concerned the processing of the complainant's personal data (in this case, details about the nature of the complainant's medical condition) by his employer, for the purpose of administering the complainant's sick leave and related payments. In particular, the complainant raised concerns regarding the sharing of his medical records by the data controller (the employer), including with staff at the local office of the data controller where the complainant worked. The complainant highlighted his concerns to a senior official in the organisation. However, the view of the senior official was that the minimum amount of information necessary had been shared.

When a person's personal data is being processed by a data controller, there are certain legal requirements that the data controller must meet. Of particular relevance to this complaint are the obligations (1) to process personal data fairly; (2) to obtain such data for specific purposes and to not further process it in a manner that is incompatible with those purposes; (3) that the data be relevant and adequate and the data controller not process more of it than is necessary to achieve the purpose for which it was collected; and (4) to maintain appropriate security of the personal data. As well as the rules that apply when personal data is being processed, because the personal data in this case concerned medical information, (which is afforded even more protection under data protection legislation), there were additional requirements that had to be met by the data controller.

It was considered that the initial purpose of the processing of this personal data by the data controller was the administration of a statutory illness payment scheme. This office also found that the further processing of complainant's personal data for the purpose of managing employees with work-related stress or long-term sick leave and the monitoring of sick pay levels was not incompatible with the purpose for which the data was initially collected. Moreover, the DPC concluded that processing for the purpose of managing work-related stress and long-term sick leave and monitoring sick pay was necessary for the performance of a contract to which the data subject was a party, for compliance with a legal obligation to which the controller was subject, and for the purpose of exercising or performing a right or obligation which is conferred or imposed by law on the data controller in connection with employment.

It was, however, considered that the data processed by the local HR office (that is, the specific nature of the complainant's medical illness) was excessive for the purpose of managing long-term sick leave and work-related stress leave and for monitoring sick-pay levels. Moreover, the DPC concluded that, on the basis that excessive personal data was disclosed by the shared services provider to the local HR office and further within that office, the level of security around the complainant's personal data was not appropriate. Finally, it was considered that, in these circumstances, the data controller did not process the complainant's personal data fairly. Therefore, the data controller was found to have contravened its data protection obligations.

Under the GDPR, special category personal data (such as health data) must be processed fairly in line with Article 5(1)(a). It must be collected for a specified, explicit and legitimate purpose and not further processed in a manner incompatible with those purposes in line with Article 5(1)(b). It may be processed only in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, in line with Article 5(1)(f). When processing special category data, controllers need to be conscious of the additional requirements set out in Article 9 of the GDPR.

Transparency

CASE STUDY 123

Provision of CCTV footage by a bar to an employer (Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

We received a complaint against a city-centre bar, alleging that it had disclosed the complainant's personal data, contained in CCTV footage, to his employer without his knowledge or consent and that it did not have proper CCTV signage notifying the public that CCTV recording was taking place.

During our investigation, we established that a workplace social event had been hosted by an employer organisation in the bar on the night in question. The complainant was an employee of that organisation and had attended the workplace social event in the bar. An incident involving the complainant and another employee had taken place in the context of that workplace social event and there was an allegation of a serious assault having occurred. An Garda Síochána had been called to the premises on the night in question and the incident had been reported for a second time by the then manager and headwaiter to the local Garda station the following day. We established that the employer organisation had become aware of the incident and had contacted the bar to verify the reports it had received. Ultimately the bar manager had allowed an HR officer from the employer organisation to view the CCTV footage on the premises. The HR officer, upon viewing the CCTV footage, considered it a serious incident and requested a copy of the footage so that the employer organisation could address the issue with the complainant. The bar manager allowed the HR officer to take a copy of the footage on their mobile phone as the footage download facility was not working.

The Data Protection Commission (DPC) considered whether there was a legal basis, under the grounds of the 'legitimate interests' of the data controller or a third party under Section 2A(1)(d) of the Acts, for the bar to process the complainant's personal data by providing the CCTV footage to the employer organisation. This provision allows for the processing that is 'necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject'.

In its analysis of this case, the DPC had regard to the judgment of the CJEU in the Riga regional security police case in which the CJEU had considered the application of Article 7(f) of the Data Protection Directive (95/46/EC) on which Section 2A(1)(d) of the Acts is based, and identified three conditions that the processing must meet in order to justify the processing as follows:

a) There must be the existence of a legitimate interest justifying the processing;

b) The processing of the personal data must be necessary for the realisation of the legitimate interest; and

c) That interest must prevail over the rights and interests of the data subject.

The DPC established during its investigation that, arising from the incident in question, there was an allegation of a serious assault committed by the complainant against a colleague and the bar had provided a copy of the CCTV footage to the complainant's employer so that the employer could properly investigate that incident and the allegations made. The DPC took into account that as the incident had occurred during the employer organisation's workplace social event, the employer might have been liable for any injuries to any employee that could have occurred during the incident. Accordingly, the CCTV was processed in furtherance of the employer organisation's obligation to protect the health and safety of its employees. As the CJEU has previously held that the protection of health is a legitimate interest, the DPC was satisfied that there was a legitimate interest justifying the processing. The DPC also considered that the disclosure of the CCTV in this instance was necessary for the legitimate interests pursued by the employer organisation so that it could investigate and validate allegations of wrongdoing against the complainant. The DPC considered, in line with the comments of Advocate General Bobek in the Riga regional security police case, that it was important that data protection is not utilised in an obstructive fashion where a limited amount of personal data is concerned. In these circumstances, the DPC considered that it would have been unreasonable to expect the bar to refuse a request by the employer organisation to view and take a copy of the CCTV footage, against a backdrop of allegations of a serious assault on its premises, especially where the personal data had been limited to the incident in question and had not otherwise been disclosed. On the question of balancing the interest of the employer organisation against the complainant's rights and interests, the DPC had primary regard to the context of the processing, where the bar had received a request for the viewing and provision of a serious incident on its premises, which it had deemed grave enough to report to An Garda Síochána. A refusal of the request might have impeded the full investigation of an alleged serious assault, and the employer organisation's ability to protect the health and welfare of its employees. Accordingly, the DPC considered that it was reasonable, justifiable and necessary for the bar to process the CCTV footage by providing it to the employer organisation, and that the legitimate interest of the employer organisation took precedence over the rights and freedoms of the complainant, particularly given that the processing did not involve sensitive personal data and there had not been excessive processing.

On the facts, the DPC was also satisfied that the bar currently had adequate signage alerting patrons to the use of CCTV for the purpose of protecting staff and customers and preventing crime, and that in the absence of any evidence to the contrary offered by the complainant, the complainant had been on notice of the use of CCTV at the time in question.

In many of the complaints that the DPC handles, data subjects hold the mistaken belief that because they have not consented to the processing of their personal data, it is de facto unlawful. However, there are a number of legal bases other than consent that justify processing depending on the particular circumstances. With regard to the legitimate interests justification, the DPC will rigorously interrogate whether the circumstances of the processing satisfy the elements that the CJEU has indicated must be present for controllers to rely on this legal basis. Equally, however, the DPC emphasises that where the circumstances genuinely meet the threshold required for this justification, as per the sentiment of Advocate General Bobek of the CJEU, protection of personal data should not disintegrate into obstruction of genuine legitimate interests by personal data.

CASE STUDY 124

Reliance on consent in the use of child's photograph in the form of promotional material by a State Agency (Applicable law — Data Protection Acts 1988 and 2003)

We received a complaint from a parent in respect of their child. The parent had attended a festival organised by a state agency with their child, where a professional photographer took the child's photograph. The following year the state agency used this photograph in promotional material. The child's parent, while accepting that they had conversed with the photographer, had understood at the time of the photograph that they would be contacted prior to any use of the image.

During the investigation, the state agency indicated that they had relied upon consent pursuant to section 2A(1) (a) of the Acts as the photographer had obtained verbal permission from the child's parent. However, the state agency also accepted that it was not clear to the child's parent that the image would be used for media/PR purposes. The state agency further accepted that the parent was not adequately informed regarding the retention of the image. The DPC welcomed the state agency's indications that it would immediately review their practices and procedures. In conclusion, the DPC found that the state agency had not provided the child's parent with adequate information in order to consent to the processing of the image used in promotional material.

CASE STUDY 125

Processing of health data

The complainant was a member of an income protection insurance scheme and had taken a leave of absence from work due to illness. The income protection scheme was organised by the complainant's employer. In order to claim under the scheme, the complainant was required to attend medical appointments organised by an insurance company. Information relating to the complainant's illness was shared by the complainant with the insurance company only. However, a third-party company (whose involvement in the claim was not known to the complainant) forwarded information to the complainant's employer regarding medical appointments that the complainant was required to attend. The information included the area of specialism of the doctors in question.

It was established that the insurance company was the data controller as it controlled the contents and use of the complainant's personal data for the purposes of managing and administering the complainant's claim under the insurance scheme. The data in question included details of the complainant's illness, scheduled medical appointments and proposed treatment and was deemed to be personal data because the complainant could be identified from it and it related to the complainant as an individual.

During the course of the investigation, the data controller argued that the complainant had signed a form, which contained a statement confirming that the complainant gave consent to the data controller seeking information regarding the complainant's illness. When asked by the DPC to clarify why it had shared the information regarding the complainant's medical appointments with the third-party company (who was the broker of the insurance scheme), the data controller advised it had done so to update the broker and to ensure that matters would progress swiftly.

The data controller stated it had a legislative obligation to provide the complainant with certain information. In particular, that the data controller was obliged to inform the complainant as to the recipients or categories of recipients of the complainant's personal data. The DPC pointed out that, while the data controller had notified the complainant that it might seek personal data relating to them, it had failed to provide sufficient information to the complainant as regards the recipients of the complainant's personal data.

Data protection legislation also requires that data, which are kept by a data controller, be adequate, relevant and limited to what is necessary in relation to the purposes for which the data were collected. The DPC examined the reason given by the data controller for disclosing information about the nature of the complainant's medical appointments (i.e. to update the broker and to ensure matters progressed smoothly). The DPC was of the view that it was excessive for the data controller to disclose information regarding the specific nature of the medical appointments, including the specialisms of the doctors in question, to the third party company.

The DPC pointed out that, under data protection legislation, data concerning health is afforded additional protection. The DPC was of the view that, because the information disclosed by the data controller included details of the specialisms of the doctors involved, it indicated the possible nature of the complainant's illness and thus benefitted from that additional protection. The DPC confirmed that, because of the additional protection, there was a prohibition on processing the data in question, unless one of a number of specified conditions applied. For example (and of relevance here), the personal data concerning health could be legally processed if the complainant's explicit consent to the processing was provided to the data controller. The DPC then considered whether the complainant signing the claim form (containing the paragraph about consent to the data controller seeking information, as described above) could be said to constitute explicit consent to the

processing (disclosure) of the information relating to the complainant's medical appointments. The DPC noted that it could be said that the complainant's explicit consent had been given to the seeking of such information by the data controller. However, the complainant had not given their explicit consent to the giving of such information by the data controller to third parties. On this basis, the DPC held that a further contravention of the legislation had been committed by the data controller in this regard.

Under Article 13 of the GDPR, where personal data are collected from a data subjects, the data controller is required to provide the data subject with certain information at the time the personal data are obtained, such as the identity and contact details of the data controller and, where applicable, its Data Protection Officer, the purpose and legal basis for the processing and the recipients of the data, if any, as well as information regarding the data subject's rights. This information is intended to ensure that personal data are processed fairly and transparently. Where the personal data have been obtained otherwise than from the data subject themselves, additional information is required to be provided to the data subject under Article 14 of the GDPR. This information must be given in a concise, transparent, intelligible and easily accessible form.

Additionally, the data minimisation principle under Article 5(1)(c) requires that personal data be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means that the period for which personal data are stored should be limited to a strict minimum and that personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Finally, data controllers should note that personal data concerning health is considered a "special category of personal data" under Article 9 of the GDPR and is subject to specific rules, in recognition of its particularly sensitive nature and the particular risk to the fundamental rights and freedoms of data subjects which could be created by the processing of such data. The processing of medical data is only permitted in certain cases as provided for in Article 9(2) of the GDPR and sections 45 to 54 of the Data Protection Act 2018, such as where the data subject has given explicit consent to the processing for one or more specified purposes.

CASE STUDY 126

Use of employee's swipe-card data for disciplinary purposes

The complainant in this case was an employee who was the subject of disciplinary proceedings by their employer. An aspect of those proceedings concerned the complainant's time keeping, and the employer sought to rely on swipe-card data derived from the complainant's entry into and exit from the workplace during the relevant period. As a result of an internal appeal process, the employer subsequently agreed not to use the data for this purpose and removed it from the complainant's disciplinary record. However, the complainant asked the DPC to continue its investigation of the complaint.

The DPC's investigation focused on the data protection principle that data must be obtained and processed fairly. This includes an obligation to give data subjects' information including the purpose or purposes for which the data are intended to be processed.

In this case, the employer had not informed the complainant of the use of swipe-card data for the purpose of disciplinary proceedings. (During the investigation, the employer informed the DPC that the complainant's case was the only one in which it had used swipe-card data for disciplinary purposes.) Similarly, the employer had not informed the complainant or other employees that swipe-card data collected in the workplace was intended to be used for time-keeping purposes.

The employer had failed to inform the complainant about the use of swipe-card data for time-keeping and disciplinary purposes. The DPC therefore concluded that the employer had not obtained and processed that data fairly.

This case demonstrates the importance of fairness and transparency in protecting data protection rights. Controllers such as employers may have valid legal bases for processing personal data, whether on grounds of performance of contract, legitimate interest or otherwise. However, the principles of data protection set out in Article 5 of the GDPR must be observed regardless of the legal basis that is relied on.

Index

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2, D02 RD28
Ireland

www.dataprotection.ie
Email: info@dataprotection.ie
Tel: 01 765 0100
LoCall: 1800 437 737

An Coimisiún um Chosaint Sonraí
Data Protection Commission