Case Studies

The following is a list of case studies, which have not been featured in the DPC's Annual Reports. These case studies provide an insight into some of the issues that this Office investigates on a day to day basis.

1. Inaccurate Information held on a banking system
2. Failure to respond fully to an access request
3. Use of CCTV in the workplace
4. Access to CCTV footage
5. Obligation to give reasons when refusing to provide access to personal data
6. Processing of Special Category Data
7. Further processing for a compatible purpose
8. Appropriate security measures when processing medical data
9. Appropriate security measures
10. Processing that is necessary for the purpose of legitimate interests pursued by a controller
11. Processing that is necessary for the purpose of performance of a contract
12. Confidential expressions of opinion and subject access requests
13. Processing of health data
14. Access requests and legally privileged material
15. Processing in the context of a workplace investigation
16. Amicable resolution - proof of identification and data minimisation
17. Amicable resolution - Right to erasure and user generated content
18. Amicable resolution in cross-border complaint - right to erasure
19. Amicable resolution - right to erasure
20. Disclosure and unauthorised publication of a photograph
21. Legal basis for processing and security of processing
22. Erasure request and reliance on Consumer Protection Code
23. Debt collector involvement
24. Appropriate security measures for emailed health data
25. Access to employee's email on a corporate email service
26. Disclosure by a credit union of a member's personal data to a private investigations firm
27. Data accuracy
28. Retention of data by a bank relating to a withdrawn loan application
29. Access to information relating to a bank's credit assessment
30. Use of employee's swipe-card data for disciplinary purposes
31. Disclosure of a journalist's name and mobile phone number by a public figure
32. Further processing for a compatible purpose
33. Fair and lawful processing of CCTV images of a customer
34. Disclosure of personal and financial data to a third party and erasure request
35. Unlawful processing and disclosure of special category data
36. Unlawful processing and erasure request

1) Case Study 1: 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.

2) Case Study 2: 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.

3) Case Study 3: 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).

4) Case Study 4: 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).

5) Case Study 5: 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.

6) Case Study 6: 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 (i.e. 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.

7) Case Study 7: 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.

8) Case Study 8: Appropriate security measures when processing medical data

The background to this complaint was that the complainant's wife made a Freedom of Information ("FOI") request to a GP who had been involved in the care of the complainant's son. The GP subsequently wrote to another doctor who had also treated the complainant's son, and had separately also treated the complainant, to inform them of the FOI request. That doctor replied to the GP's letter and, in the reply, disclosed medical information concerning the complainant, who was not a patient of the GP.

In order to determine who the data controller was, the DPC sought confirmation of the capacity in which the complainant had consulted the doctor who disclosed the information in question. It was confirmed that the doctor only saw patients publicly and, on this basis, the DPC determined that the data controller was the HSE.

In response to the complaint, the data controller admitted that the personal data regarding the complainant was disclosed in error because the doctor mistakenly believed the complainant was also a patient of the GP. However, the HSE advised that the GP recipient would have been bound by confidentiality obligations in respect of the data received. The data controller also indicated that, because the doctor in question had retired, the issue could not be addressed with them personally. The HSE confirmed that its internal policies regarding data processing had been updated and improved since the incident involving the complainant.

The DPC noted that, when 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 were the obligations to process the personal data fairly and to have appropriate security measures in place to protect against unauthorised processing (disclosure). The DPC further noted that, because the personal data was of a medical nature (and thus benefitted from increased protection under the legislation), the standard to be met in terms of what was appropriate security was higher than that applicable to personal data generally." In addition, the DPC confirmed that, because of the increased protection afforded to health data under data protection legislation, it can be processed only if certain specified conditions are met.

It was apparent that appropriate security measures were not in place when the unauthorised disclosure to the GP took place. The DPC noted that the disclosure was to a GP who was not involved in the complainant's medical care, and further, that the letter in which the disclosure was made had a heading referring to the complainant's son but contained medical information relating to the complainant in the body of the letter. The mistake was therefore evident on the face of the letter itself. The DPC noted the data controller's argument that the GP was bound by confidentiality obligations; however, it held that while this was relevant in terms of the consequences of the unauthorised disclosure, it did not address whether the data controller had appropriate security measures in place. The DPC also highlighted that the data controller was not able to address control measures related to the disclosure as the doctor in question had retired. The DPC held that this was suggestive of the fact that a general framework related to security of personal data was not in place at the time of the disclosure.

The DPC then looked at whether the requisite conditions to permit the processing of data regarding health had been met. The DPC decided that, because the data controller had failed to put forward any lawful basis for disclosing the personal data, it had also contravened data protection legislation in this regard.

The obligation to ensure security of personal data is evident in Article 5(1)(f) of the GDPR and is further specified in Article 32, which requires that a controller and a processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In considering appropriate security measures, data controllers and processors must take into account, amongst other things, the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for data subjects. In this regard, the GDPR recognises that health data, which is a "special category of personal data" under Article 9 of the GDPR, are by their nature particularly sensitive in relation to fundamental rights and freedoms and merit specific protection.

Data controllers should also be aware that, where a breach of security occurs leading to the accidental or unlawful unauthorised disclosure of personal data (a "personal data breach"), it must be notified to the DPC without undue delay in accordance with Article 33 of the GDPR. Where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, it must also be communicated to the data subject without undue delay.

9) Case Study 9: Appropriate security measures

This complaint concerned the alleged loss by the complainant's bank of several items of correspondence relating to the complainant's bank account, which had been hand-delivered to the bank by the complainant's partner.

It was established that the bank was the data controller as it controlled the contents and use of the complainant's personal data in connection with its provision of banking services to the complainant. The data in question consisted of (amongst other things) the complainant's name, address and bank account information and 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 examination of the complaint, the data controller maintained that the relevant documents had been misplaced within the bank and not externally and therefore argued that no personal data breach had occurred. The DPC noted that maintaining appropriate security measures for personal data is a key requirement under data protection law. It considered the nature of the personal data that was contained in the correspondence that went missing (the complainant's name, address and bank account information) and noted that misplacing this information had the potential to cause significant risk to the complainant and the complainant's financial affairs. The security measures that were in place in the data controller were not sufficient to ensure an appropriate level of security, given the nature of the personal data being processed. As regards the data controller's argument that the correspondence was lost internally, the DPC's view was that a data controller's technical and organisational measures to safeguard the security of personal data must take account of the fact that internal as well as external loss of personal data, or unauthorised access to it, can give rise to risks to people like the complainant.

Based on the above, it was considered that there had been a failure of the data controller to have appropriate security and organisational measures in place, to safeguard the complainant's personal data, and that the data controller had therefore failed to act in accordance with the data protection legislation.

Under Article 5(1)(f) of the GDPR, personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful disclosure, using appropriate technical or organisational measures. The obligation to ensure security of personal data is further specified in Article 32, which requires that a controller and a processor implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. In considering appropriate security measures, data controllers and processors must take into account, amongst other things, the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for data subjects.

Data controllers should also be aware that, where a breach of security occurs leading to the accidental or unlawful unauthorised disclosure of personal data (a "personal data breach"), this must be notified to the DPC without undue delay in accordance with Article 33 of the GDPR. Where the personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, it must also be communicated to the data subject without undue delay.

10) Case Study 10: 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.

11) Case Study 11: 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.

12) Case Study 12: 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.

13) Case Study 13: 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.

14) Case Study 14: 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.

15) Case Study 15: 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.

16) Case study 16: 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.

17) Case study 17: 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.

18) Case study 18: 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.

19) Case study 19: 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.

20) Case study 20: 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.

21) Case study 21: 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.

22) Case study 22: 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.

23) Case study 23: 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.

24) Case Study 24: 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.

25) Case study 25: Access to employee's email on a corporate email service

The complainant was an employee who maintained that their employer had infringed their data protection rights by searching for, retrieving and reviewing a number of emails on their corporate account.

During an investigation involving other persons, the employer had come across emails that raised concerns regarding several employees, including the complainant. The employer then searched its corporate servers for emails of the complainant dating to a particular four-week period and involving specific individuals. The employer then monitored the complainant's use of corporate email for communication with a specific person and retrieved several further emails. Based on these, the employer started disciplinary proceedings against the complainant on grounds that the complainant's use of the corporate email service had breached applicable rules and policies.

It was not disputed that the emails comprised personal data, that the employer was the data controller, or that the employer's actions in searching for, retrieving and viewing them constituted processing. The employer maintained that the processing was fair, lawful and proportionate, and that it had balanced the legitimate interests of both itself and the complainant in doing so.

The complainant's employment contract expressly required the complainant to comply with the employer's resolutions, regulations and directions. The employer's corporate policies included an 'Acceptable Use Policy' relating to the corporate email service, a disciplinary policy that outlined types of conduct that could lead to disciplinary proceedings, and a 'Code of Conduct' that dealt with topics such as loyalty, ethics and integrity. All were in effect when the relevant emails were sent.

The Acceptable Use Policy allowed occasional and limited personal use of corporate email that was in line with the employer's values and did not contravene its corporate policies. It said that the employer could and would monitor email for compliance with the Acceptable Use Policy and for other legitimate business purposes. Further, the employer reserved the right to examine information stored on its systems or networks, and it said that the employer "may monitor information stored on [its] systems or equipment, whether created for business or personal purposes, at any time".

The DPC examined whether the processing was fair and whether the employer had a legal basis for processing the data in the way it did.

In relation to fairness of processing, the DPC first considered the controller's obligation to give data subjects sufficient information to make clear the types of data that will be processed and the purposes of the processing. The DPC took the view that the Acceptable Use Policy made clear that all information on the employer's systems, including employees' personal emails, were liable to be examined to ensure compliance with the Acceptable Use Policy and for other legitimate purposes. In that regard, the DPC considered that ensuring compliance with the employer's disciplinary procedures and Code of Conduct were legitimate purposes. Based on this, the DPC's position was that the purposes had been made clear to the complainant.

The DPC then considered whether the processing in this case had in fact been for the purposes provided to the complainant. The DPC noted that the search of the complainant's corporate email account had been prompted by a separate investigation that had raised concerns about the complainant relevant to the Acceptable Use Policy, the Code of Conduct and the disciplinary policy. The resulting search of the complainant's email account was limited both as to the period covered and the individuals involved, as was the subsequent monitoring of the complainant's use of email.

The DPC's view was that the employer's processing of the complainant's emails during the initial investigation (which was not focused on the complainant) fell within the purposes stated in the Acceptable Use Policy. Similarly, its search for, retrieval and reading of emails from the four-week period, and its subsequent monitoring and reading of the complainant's emails, all came within those purposes. Because the period and range of persons specified in the search and the monitoring were limited to those relevant to the investigation, the stated purposes were not exceeded.

The employer relied on its legitimate interest as the legal basis of the processing. The DPC noted that this required three elements: the processing must be for the pursuit of the legitimate interest, it must be necessary for that purpose, and the fundamental rights and freedoms of the person concerned – the complainant in this case – must not take precedence over the processor's interest.

Concerning the first element, the DPC considered the terms of the Acceptable Use Policy, the Code of Conduct and the disciplinary policy. The DPC's view was that these were legitimate and that the initial investigation fell within the interest of the employer in upholding them. In light of information disclosed by the initial investigation, it was within the employer's legitimate interest to search for emails created during the four-week period and to monitor and retrieve certain specific emails.

Regarding the second element – that the processing be necessary for the pursuit of the legitimate interest – the DPC's view was that the Acceptable Use Policy expressly concerned use of the corporate email service, and it would not be possible to investigate a potential breach and enforce its terms without the types of processing carried out in this case. The DPC noted in this regard that the employer's search and monitoring of email was strictly limited in terms of the period and individuals involved.

The third element of the legitimate interest basis of processing was balancing of the processor's interest against the rights and freedoms of the person concerned. The DPC noted that the complainant considered the relevant emails to be personal, and that the Acceptable Use Policy allowed limited and occasional use the email service for personal email. Further, the complainant did not consent to the monitoring and had not been informed of it until the employer notified them of the investigation. Against that, the DPC noted that the emails concerned aspects of the employer's business and so could be considered relevant to the complainant's work. The complainant had stated to the DPC that the contents of the emails were not inappropriate and, had the employer asked, the complainant would have allowed access to them. The employer considered the emails to be evidence of potential

breaches by the complainant of the Acceptable Use Policy and Code of Conduct, and the possibility of monitoring had been notified in that Policy. The DPC's view was that, on balance, the processing by the employer was limited in nature and did not infringe on respect for the complainant's private life.

The DPC's position was, in conclusion, that the processing was fair and that the employer had a legal basis for performing it.

This case demonstrates a number of important points. Employers may have a legitimate interest that justifies monitoring, retrieving or reading employees' personal data on their systems, whether created for personal or work purposes. However, it is not enough just to inform employees that their employer reserves the right to monitor communications: processing must conform to the principles of data protection set out in Article 5 of the GDPR, and controllers such as employers must observe the transparency requirements of Chapter III (Articles 12 to 23). They must also consider the legal basis for processing on which they rely: Article 6 imposes a 'necessity' test for all but one of the available legal bases. This means in essence that the processing must be the only practical way to achieve the desired purpose, not just a more convenient means of doing so. (The exception is consent, and controllers should bear in mind that a data subject may withdraw consent no less easily than they gave it.)

Accordingly, before invoking a power to monitor employees' communications, employers must consider carefully whether all data protection principles have been and will be observed, the precise legal basis relied on, and the nature and amount of processing required. The necessity of the processing and the effects on the rights and freedoms of data subjects must be carefully evaluated.

Employees should be aware of how their employer may collect and process their personal data, and the legal basis on which they rely. (Articles 12 to 15 of the GDPR provide for data controllers to provide information about these matters to data subjects.) Policy statements, employee handbooks and similar documents can provide important information about data protection rights.

26) Case study 26: 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 an unambiguous 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.

27) Case study 27: 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.

28) Case study 28: 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.

29) Case study 29: 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.

30) Case study 30: 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.

31) Case study 31: 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.

32) Case study 32: Further processing for a compatible purpose

This complainant owned a rental property that was managed by a letting agency on the complainant's behalf. The building in which the complainant's rental property was located was managed by a management company which was responsible for the collection of management fees from the owners of the properties in the buildings. The management company sent an email to the complainant's letting agent regarding management fees outstanding on the complainant's property. However, the letting agent did not act on the complainant's behalf in relation to the payment of management fees.

The Commission determined that the data controller was the management company because it controlled the contents and use of the complainant's personal data for the purposes of acting as the management company of the building where the complainant's property was located. The data in question was deemed to be personal data consisting of the status of payment on the complainant's account, because the complainant could be identified from it and it related to the complainant as an individual. Therefore, the Commission was satisfied that an investigation should be carried out to determine if a breach of the relevant legislation had occurred.

In response to the complaint, the data controller argued that it acted as a management company in respect of many properties and many developments and that the role of letting agents varies considerably from property to property. It indicated that, in some cases, the letting agent is appointed on behalf of a property owner to collect management fees and, on this basis, it thought it was appropriate to contact the complainant's letting agent regarding outstanding fees.

The Commission noted that when personal data is processed by a data controller, there are certain legal obligations that the data controller must comply with. Of particular relevance to this complaint were the obligations: (1) To obtain such data for specific purposes and not to further process it in a manner that is incompatible with those purposes, (2) that the data must be relevant and adequate and the data controller must not process more of the data than is necessary to achieve the purpose for which it was collected, and (3) to have appropriate security measures in place to protect the personal data. In addition, the Commission noted that the legislation also requires that there must be a lawful basis for processing the personal data.

In relation to the first obligation (not to process personal data in a manner that is incompatible with the reasons for which it was collected), the Commission noted that personal data regarding the payment of the complainant's management fee was collected for the purposes of financial record keeping and the collection of fees. However, because the letting agent didn't have a role in the payment of the management fees, the data controller shared the complainant's personal data with a party who it had no reason to share it with. On this basis, the Commission held that the disclosure of the complainant's personal data was for a purpose that was incompatible with the purpose for which it was collected.

In circumstances where it was not necessary for the data controller to share the personal data in question with the letting company, the Commission determined that the personal data was not relevant or adequate and was excessive for the purposes for which it was processed.

In relation to whether appropriate security measures were in place, the Commission held that because there was an absence of understanding on the part of the data controller in relation to the letting agent's role, (and the complainant's personal data were disclosed as a result) the data controller had failed to meet its obligations in this regard.

Finally, the Commission determined that the data controller had no lawful basis for making the disclosure to the letting agent, because none of the legal bases for processing could be said to apply. This meant that the data controller had committed a further breach of the legislation in this regard.

Under Article 6 of the GDPR, a data controller must have a valid legal basis for collecting personal data. 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 addition, under Article 5(1)(c) of the GDPR, personal data which are processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and under Articles 5(1)(f) and 32 of the GDPR, personal data must be processed in a manner that ensures appropriate security of the data, including security against unauthorised disclosure. For this purpose, data controllers are required to have in place appropriate technical and organisational measures to ensure the confidentiality of personal data.

33) Case study 33: 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.

34) Case study 34: 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.

35) Case study 35: 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.

36) Case study 36: 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.

37) Case study 37: 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.

38) Case study 38: 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.

39) Case study 39: Disclosure of personal data (Applicable Law – GDPR & 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.

40) Case study 40: Fair processing of personal data (Applicable Law – GDPR & 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.

41) Case study 41: Unlawful processing of photograph and erasure request under Article 17 of GDPR (Applicable Law – GDPR & 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 or 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.