LK SHIELDS
YOUR LEGAL COUNSEL

DATA PROTECTION, PRIVACY AND SECURITY

Data Protection Commission's Annual Report 2021

by **Aideen Burke, James Green**

Data Protection Commission's Annual Report 2021

30th March 2022 | by Aideen Burke, James Green

The Irish Data Protection Commission (DPC) published its 2021 Annual Report in February 2022.

It includes over 30 case studies on a range of topics, which are practical and illustrative examples of how the DPC deals with some common issues.

The most useful case studies can be divided into three categories:

1. Dealing with access requests.
2. Using data for a new or additional purpose.
3. Security related case studies.

Dealing with Access Requests

Access requests continue to be one of the top issues to feature in complaints received by DPC. The DPC identified a growing pattern in 2021 of data controllers failing to respond to requests by data subjects or to complaints correspondence from the DPC itself.

Missing content from an access request

The DPC received a complaint from an individual who said they had not received all personal data relating to them. In particular, they were looking for an email they had sent the controller which was relevant a separate appeal they were undertaking. The controller proved to the DPC that the email had never reached any of the intended recipients – it had been quarantined by a spam filter and was automatically deleted. As the email was not in existence at the time the access request was made it did not have to be included in the access request. But the DPC did note that when implementing a quarantine system such as this, the controller must balance the rights and freedoms of individuals against the security requirements of the controller.

Only data available at the time of the access request must be shared and the implementation of any security measures must be measured against the impact on the rights and freedoms of data subjects

Identity verification obligations

A person that submitted an access request to a controller (a hotel) was asked by the hotel to provide a copy of utility bill and a copy of photo ID verified by An Garda Siochana. The DPC asked the controller to set out its particular concerns relating to the identity of the data subject who had submitted the request. The DPC noted that the postal address and email address being used were the same as those provided during the booking process. The DPC felt that the level of verification sought was not proportionate to the categories of data held by the controller and that identify could be verified based on questions of a different nature

when combined with the information the controller already held on file.

A controller should only request the minimum amount of further information necessary and proportionate to prove the identity of a requester.

Using Data for A New Purpose

It is common for controllers to use data collected for a specified purpose, for additional purposes, which were not previously disclosed to data subjects.

Use of data collected for one purpose also being used for a different purpose

The controller (which carried out a statutory function) used a dispatch system for the purpose of ensuring the most efficient use of drivers and vehicles, particularly in emergency situations. The system logged various details which the employer used to verify overtime and substance claims. The employer rejected the complainant's request for overtime due to inconsistencies between the details on the complainant's form and those recorded in the dispatch system. The controller did not have a written policy on the use of the dispatch system, but the requirement for dispatch reference numbers to be included in overtime requests indicated to employees that the system was used for other purposes. The use of the system in this way did comply with the legitimate interests of the controller and it should be noted that the legal obligations of the controller in relation to verifying overtime for payments, etc., were also relevant.

There are steps that must be followed before data collected for one purpose can be used for a different purpose, but it is possible to do so if the new purpose is compatible with the original purpose.

Data Breaches

Under the GDPR it is a mandatory requirement to notify any personal data breaches that occur to the DPC. Unauthorised disclosure of personal data account for up to 71% of data breach notifications. The report contains a number of useful case studies relating to unauthorised disclosure.

Unauthorised disclosure in a workplace setting

A complainant was in a legal dispute with a controller and filed a complaint with the DPC. Approximately one month before the complaint, the DPC received a notification from the controller relating to a data breach where a submission to the Workplace Relations Commission had been inadvertently stored in a folder accessible by all employees.It was corrected two days later. The DPC took the view that there was no evidence that the file had been inappropriately accessed during that period and looked favourably on the fact that the data breach had been disclosed. On security measures, the DPC said the company was clearly aware of the risks of disclosure and had failed to take adequate steps to mitigate those risks.

Ensure steps are taken to secure personal data appropriate to the risk and promptly notify the DPC if a data breach occurs.

Unauthorised disclosure from video conferencing

An educational institution used a video conferencing application for the delivery of presentations by students to their lecturers. The sessions were recorded so that the presentations could be shared with external examiners. It later emerged that the recordings of each student's presentation and the internal deliberations of examiners were available to all the students involved. The controller reported this data breach to the

DPC.

Basic security steps around the implementation of new technology should not be overlooked. The risks stemming from such technology should be clearly documented as part of a data protection impact assessment.

Email misdirect breach

An email containing a sensitive encrypted file was sent to the wrong email address. The file was encrypted, but the mistake was repeated by the controller in sending a separate email to the same incorrect email address with the password.

While encryption is an important step in protecting sensitive information, the protection it provides can be negated if the appropriate steps are not taken. Encryption keys should be shared through a separate medium such as SMS, where possible.

Inappropriate disposal of materials

An educational institution had an employee working from home due to pandemic restrictions. The employee worked on printed copies of a number of job applications and CVs.The employee was instructed by his employer to destroy documents before disposal and there was a policy in place that required documents to be securely destroyed before being disposed of. The employee had not been provided with a shredder and disposed of the documents in the domestic recycling bin. High winds caused the contents of the bin to be dispersed.

It is important to put in place good policies in terms of dealing with information, but employees must also be provided with the means to implement those policies.If employees are required to securely destroy documents, then they should be provided with a shredder or some other means to destroy the documents securely.

Conclusion

With the recent publication of the Data Protection Commission's regulatory strategy and the contents of the Annual Report, it is clear that the DPC is intending to take a more robust approach on enforcement. This will require investment by employers in ongoing skills training for their staff. The case studies contained in the Annual Report show the importance of getting the basic steps correct and serve as a useful reminder of some things that can go wrong.

If you would like to learn more information about anything in this article, or how these issues may apply to your organisation, please contact Aideen Burke or your usual contact in our Data Privacy team.

About the Authors

Aideen Burke
Partner

Aideen is Head of our Intellectual Property, Technology, Media and Data Privacy team.
T: +353 1 637 1574 **E:** aburke@lkshields.ie

James Green
Associate Solicitor

James is an Associate Solicitor in our Intellectual Property, Technology and Privacy Department.
T: +353 1 637 1567 **E:** jgreen@lkshields.ie