Navigating an Ever-Changing Maze: A Guide to Data Protection Law

Article by Sharon Sheehan, BA (Hons) ES Laws, GD Business on behalf of the CPA Ireland Examinations Team for Professional Level Corporate Law, February 2023.

The following article provides comprehensive coverage of the area of Data Protection Regulation as it applies to the CPA Ireland - Corporate Law syllabus. The information is current at the date of publication. This article is intended to complement the core text as specified on the subject syllabus document.

Introduction:

The General Data Protection Regulation (GDPR)[1] became operative on the 25th May 2018, in all of the then 28 European Union (EU) member states[2]. The impetus behind the enactment of the Regulation was to standardise and harmonise the relevant law in all of the member states. The historical enactment of EU Directives on data protection meant that although the crux of the law was similar in the member states, individual transpositions meant that there were some divergent rules. Given the growth in the online market and the globalisation and digitisation of trade, having a uniform law in all of the EU's member states became a key objective. This was achieved upon the implementation of this Regulation. Furthermore, Ireland also took the opportunity to update its own data protection laws to ensure proper structures for the regulation and enforcement of GDPR. These laws are now referred to as the Data Protection Act 1988-2018.

Key Definitions:

The Regulation encompasses key definitions, including the following:

A. Data Controller: A data controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data[3]. Therefore, social media hosts such as Meta, Twitter and Tiktok are all data controllers, as are online marketplaces such as Amazon, Ebay and Etsy. Employers, financial institutions, educational institutions, and government bodies such as Revenue and Social Protection are also data controllers, who are often involved in the processing of large volumes of data.

However, it is important to appreciate that an employee working for a legal entity, whose main duties revolve around data protection compliance, will not be classed as a data controller. The legal entity, in this situation, always remains the data controller.

B. Data Processor: A data processor is a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the data controller[4]. For example, a financial institution may process an employer's payroll data, for the purpose of paying employee salaries. Similarly, an insurance company may process an employer's employee data for the purpose of providing medical insurance, critical illness cover or providing a death gratuity.

---

[1] (EU) 2016/679.

[2] There are now 27 EU Member States, since the United Kingdom withdrew from the Union on 1 January 2020.

[3] Article 4(7).

[4] Article 4(8).

C. **Personal Data and a Data Subject:** This includes any information relating to an identified or identifiable natural person[5] (known as the data subject). To be afforded protection under GDPR, the data must relate to a living person, a deceased person is not afforded protection. In this regard, an identifiable natural living person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[6]. This could include personal information such as an address[7] or date of birth, as well as a person's bank account number or credit card number, licence or passport number, or their CCTV image. The definition of personal data also extends to a student's exam script[8].

   Both manual and electronic data can be classed as personal data. For example, where an accountant is doing a tax return on behalf of a client, who operates a sole trading business, manual data could include physical receipts for business expenses (such as transport or restaurant receipts), whereas electronic data could include electronic purchase and sales invoices.

Obligations Imposed upon the Data Controller:
In addition, to the specific obligations imposed upon a data controller to ensure compliance with the key principles of data protection, a data controller is also required to adhere with the following obligations:

A. To disclose their identify to the data subject;
B. To disclose to the data subject the specific reason why their data is being gathered;
C. To disclose all reasonable information regarding the processing of the data subject's data[9];
D. To enter into a contract containing prescribed terms[10] when they engage a data processor to process personal data on their behalf, as well as ensuring that the data processor has undertaken reasonable steps to ensure the security of the data being processed;
E. To retain appropriate records of all processing activities[11]; and
F. To make a privacy notice available to all data subjects[12].

---

[5] A legal entity does not fall within the remit of this definition.
[6] Article 4(1).
[7] This includes a home address, email address, IP address and a cookie's identification address.
[8] According to the CJEU in *Peter Nowak v Data Protection Commissioner* (2017) C-434/16 at para 49: *"… if information relating to a candidate, contained in his or her answers submitted at a professional examination and in the comments made by the examiner with respect to those answers, were not to be classified as 'personal data', that would have the effect of entirely excluding that information from the obligation to comply not only with the principles and safeguards that must be observed in the area of personal data protection, and, in particular, the principles relating to the quality of such data and the criteria for making data processing legitimate, established in Articles 6 and 7 of Directive 95/46, but also with the rights of access, rectification and objection of the data subject, provided for in Articles 12 and 14 of that directive, and with the supervision exercised by the supervisory authority under Article 28 of that directive."*
[9] Article 13.
[10] Article 28.
[11] Article 30.
[12] As per Articles 12-14, this privacy notice should include the following: (1) the rationale for the collection of the data, and the nature of the intended processing, (2) details of any parties who will receive the data, (3) a statement as to whether a legitimate interest exists in the collection and/or processing of the data, (4) details of the data retention period, and the criteria employed to determine such periods, (5) details of the rights of the data subject, and how these can be exercised, and (6) details of whether and how the controller uses automated decision-making.

In addition, where certain conditions are met the data controller is required to appoint a data protection officer, and in some circumstances, they may also be required to undertake a data protection impact assessment.

Data Protection Officer (DPO)
A DPO must be appointed where[13]:

A. The processing is carried out by a public authority or body[14]. For example, the processing of patient data by the Health Service Executive (HSE), or employee data by the Revenue Commissioners etc…;

B. The core activities of the controller or the processor consist of processing operations, which require regular and systematic monitoring of data subjects on a large scale. This may include data controllers who provide telecommunications services, location tracking or profiling and scoring for purposes of risk assessment. For example, a *Netflix's* customer, whose viewing is monitored by the service so they can provide recommendations to that customer. Similarly, *Amazon* would also monitor customer use of its Prime services, as well as its Kindle readers; and

C. The core activities of the controller or the processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences. In this regard, large scale processing is likely to include the processing of travel data of customer using *Travel for Ireland (TFI)* services, via the use of Leap Cards. Similarly, the processing of patient data by primary care facilities (such as nursing homes) and pharmacies (such as *Boots*) would be likely to be classified as large scale processing.

A DPO may be employed by the data controller as an employee (employed under a contract of service), or an independent contractor (employed under a contract for services). The controller is required to publish details of their DPO to the Data Protection Commission[15].

According to the European Data Protection Supervisor the primary duty of a DPO is to:

> *"… ensure that … [an] organisation processes the personal data of its staff, customers, providers or any other individuals … in compliance with the applicable data protection rules."*[16]

The key tasks required to be undertaken by a DPO include the following[17]:

A. To inform and advise the controller, processor and employees who carry out processing, of their data protection obligations;
B. To monitor compliance with GDPR and data protection laws and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
C. To provide advice where requested as regards a data protection impact assessment;
D. To cooperate with the Data Protection Commission (this could be in relation to audits, enforcement actions or compliance with the rights of the data subject);

---

[13] Article 37(1).
[14] This excludes the Courts acting in a judicial capacity.
[15] Article 37(6)-(7).
[16] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en
[17] Article 39.

E. To act as the contact point with the Data Protection Commission on issues relating to processing, and to consult, where appropriate, with regard to any relevant matters.

Data Protection Impact Assessments (DPIA)

A DPIA should be undertaken where data processing is likely to result in a high risk[18] to the rights and freedoms of individuals. For example, a data controller should use a DPIA to identify and mitigate against any data protection related risks arising from a new project or the implementation of new technologies[19]. According to the Data Protection Commission:

> *"[t]hese risks range from personal data being stolen or inadvertently released and used by criminals to impersonate the individual, to worry being caused to individuals that their data will be used by … [organisations] for unknown purposes."*[20]

In assessing whether to undertake a DPIA, the controller should assess whether it is mandated by the Data Protection Commission[21], who are required to publicise a list of the kind of processing operations that necessitate a DPIA. For example, a DPIA is required where a data controller performs automated decision-making based on personal data profiling. Automated decision-making is often employed by financial institutions, where customers can input personal data online to verify if they are eligible for a loan and to obtain automatic loan approval. Similarly, the Central Applications Office (CAO), the organisation responsible for overseeing undergraduate applications to colleges and universities in the Republic of Ireland, uses automated decision making to offer college places to applicants, based on their Leaving Certificate examination results. Companies can also use this for recruitment purposes, to shortlist candidates.

Where a DPIA is not compulsory, the data controller should still consider whether it is necessary, taking into consideration the nature, scope, context and purposes of the processing, and whether it is likely to result in a high risk to the rights and freedoms of natural persons. Any such assessment should be undertaken in consultation with the DPO, where relevant.

In accordance with Article 35(3) of the GDPR a DPIA should be conducted where the processing involves:

A. The systematic and extensive evaluation of personal aspects relating to natural persons, based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
B. The processing on a large scale of special categories of data[22], or of personal data relating to criminal convictions and offences; or

---

[18] A high risk can be defined as arising where the probability of the data processing resulting in a data breach or privacy violation is high, and where damage is likely to result from such a breach or violation.

[19] These include artificial intelligence and machine learning, self-driving cars and smart technology.

[20] https://www.dataprotection.ie/en/organisations/know-your-obligations/data-protection-impact-assessments

[21] Article 35(4). See: https://www.dataprotection.ie/sites/default/files/uploads/2018-11/Data-Protection-Impact-Assessment.pdf

[22] As per Article 9(1), this includes the processing of data revealing a data subject's (1) racial or ethnic origin, (2) political opinions, religious or philosophical beliefs, or (3) trade union membership, as well as (4) the processing of genetic data or biometric data (for the purpose of uniquely identifying a natural person), (5) data concerning health, or (6) data concerning a natural person's sex life or sexual orientation. For example, where a data subjects genetic data is processing by a genealogy company, for the purpose of creating their family tree. Similarly, where a company uses employee fingerprints scans, face or iris recognition to permit access to systems, hardware or buildings, this involves the processing of biometric data.

C. The systematic monitoring of a publicly accessible area on a large scale[23].

A DPIA should include[24]:

A. A systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
B. An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
C. An assessment of the risks to the rights and freedoms of data subjects arising from the processing; and
D. The measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

Principles of Data Protection:
The main principles of data protection that a data controller must comply with are as follows:

A. ***To obtain and process information lawfully, fairly, and in a transparent manner***[25]: All data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

   In this regard, the processing is deemed lawful[26] where: (1) it is based on the consent of the data subject[27], (2) it is necessary for the performance of a contract[28], (3) it is required for compliance with a legal obligation[29], (4) it is necessary to protect the vital interests of a person[30], (5) it is necessary for the performance of a task carried out in the public interest[31]; or (6) it is in the

[23] This would involve the use of CCTV in public areas such as streets, parks etc… as well as in publically accessible buildings such as museums and libraries.
[24] Article 35(7).
[25] Article 5(1)(a).
[26] Article 6(1).
[27] Article 4(11) requires that this consent must be freely given, and be a specific, informed and unambiguous indication of the data subject's wishes, obtained by a statement or by a clear affirmative action. Consequently, consent obtained as a result of pre-ticked boxes, or refusing consent by un-ticking a box, is not permissible under GDPR. Similarly, where consent is required for multiple processing purposes, such consent should be obtained by individual and not collective affirmation.
[28] For example, the processing of employee data by an employer for payroll purposes, processing of data by a telecommunications company to deal with recurring payments, the processing of personal data by an IT hardware company to comply with an agreed product warranty, the processing of personal data where a person requests an insurance quotation or where a person is entering into a residential lease agreement.
[29] For example, third level educational institutions are required to process international student attendance data by the Garda National Immigration Bureau (GNIB) to ensure that the students are compliant with the terms of their student visa.
[30] Processing on this ground must be essential to protect someone's life, or to mitigate against a serious threat to a person. This may arise in a situation of public health, public safety or even public interest. For example, during the Covid-19 pandemic the government had a vital interest in processing personal data to facilitate contact tracing, in order to notify people to quarantine to curb the spread of the virus. Similarly, a vital interest may arise where a school shares health information or details of the child's parents to a hospital or paramedics, where the child is involved in an accident while at school.
[31] For example, political parties may compile personal data on people's political opinions for reasons of public interest. Similarly, the processing of personal data is likely to be permissible on humanitarian grounds in the event of a natural and man-made disaster. An Garda Síochána are also permitted to process personal data law to investigate criminal activity.

legitimate interests of the data controller or third party[32], except where those interests are overridden by the interests or rights and freedoms of the data subject. In addition, processing is regarded as lawful where it is carried out for archiving purposes in the public interest, scientific or historical research purposes or for statistical purposes[33].

Under this principle, fairness and transparency requires that the data controller makes it known to the data subject, the purposes for which their personal data will be collected, used, consulted, or otherwise processed. In *Case Study No. 4/2021* the Data Protection Commission considered whether the use of employee data from the dispatch system[34], in order to verify overtime and subsistence claims was in line with the fair processing requirements of data protection law. The Commission concluded that the fairness of the processing was to be assessed by reference to the knowledge of the complainant and his fellow employees of the employer's use of the data for that purpose. In the circumstances, the Commission concluded that no breach had arisen as the inclusion of relevant dispatch system reference numbers in overtime and subsistence claims indicated that employees were aware that the data was used not just for logistical processing, but also to verify their claims.

In 2021, the Data Protection Commission fined *WhatsApp* €225m for a range of compliance failures relating to issues of transparency. In addition, they also made an order directing remediation of the information provided to the public through *WhatsApp's* privacy policy. This decision is currently under appeal.

B. ***To keep information only for one or more specified, explicit and lawful purposes[35]:*** The data controller must ensure that the data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[36]. This principle also requires that personal data must not be processed or disclosed for any purpose that is incompatible with the original purpose or purposes for which it was obtained. For example, a third level education provider would be prohibited from disclosing details of any accountancy graduates to CPA Ireland, for the purpose of CPA Ireland marketing their professional accountancy qualification to them. In *Case Study No. 3/2018* a complaint was upheld by the Commission relating to a data subject whose web-chat with a Ryanair employee was accidentally

[32] For example, a credit card provider may have a legitimate interest in processing personal data, where it is strictly necessary for the purposes of preventing fraud. A legitimate interest may also exist where the processing is necessary to ensure network and information security, to indicate possible criminal acts or threats to public security. In *Case Study No. 2/2018* the provision of CCTV footage by a pub owner to the HR officer of a company, relating to an alleged assault between employees during a work related event, was deemed to be a legitimate interest for the purpose of processing. According to the Commission the employer might have been liable for any injuries to any employee that could have occurred during the incident, therefore the CCTV was processed in furtherance of the employer organisation's obligation to protect the health and safety of its employees. Furthermore, the processing related to the legitimate interests pursued by the employer organisation so that it could investigate and validate allegations of wrongdoing against the complainant.

[33] For example, the Central Statistics Office (CSO) processes personal data generated by the Census in order to inform government spending in relation to the provision of public services at a community, local and national level, including areas such as transport, education, housing and health services.

[34] The intended purpose of this dispatch system was to ensure the most efficient use of drivers and vehicles.

[35] Article 5(1)(b).

[36] Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will not, in accordance with Article 89(1), be considered to be incompatible with the initial purpose for which it was obtained.

disclosed by Ryanair in an email to another individual who had also used the Ryanair web-chat service[37].

In *Case Study No.5/2021* the issue concerned the inadvertent storage by the employer of a Workplace Relations Commission submission on a folder accessible by all employees, rather than on one that was accessible only by authorised HR staff. The submission related to a claim of unfair dismissal by a former employee, which included their personal details, as well as an internal investigation report. As this data was only accessible for two days before the employer became aware of their error and rectified it, the Commission determined that there was insufficient evidence to support the claim by the former employee that the internal investigation report had been disclosed, or that their personal data had been accessible by non-employees as well as unauthorised employees.

Similarly, in *Case Study No.22/2021* a statutory body that regulated prescribed professional conduct, training and competence inadvertently sent a letter concerning a complaint against a specialist attached to an email to an incorrect address. The attachment contained personal data of several persons, including health data, and was encrypted. However, the password for the encrypted letter was issued in a separate email to the same incorrect address. The Data Protection Commission determined that this was a breach of their disclosure obligations.

C. ***To ensure that the data is adequate, relevant and not excessive[38]:*** This requires that the data controller ensures that the data is sufficient for the purpose required and is not more than is needed. In effect, the data must be limited to what is necessary in relation to the purposes for which it is processed – this is known as *data minimisation*. This principle also requires the data controller to to establish an appropriate time limit for the erasure of the data, and to undertake periodic reviews of the necessity for the retention of the data.

In *Case Study No. 5/2014* a prospective tenant raised a complaint in relation to the collection of their bank details, PPS numbers and copies of utility bills in their names by a letting agency at the application stage, to review prospective rental properties. The Data Protection Commission determined that the gathering of this information at the application stage was excessive, and that it should only be requested from the prospective tenant once they have indicated their intention to rent a specific property.

In *Case Study No. 17/2022* a request by Vodafone that customers provide them with their employment details and a work phone number, in order to obtain Vodafone services was investigated by the Data Protection Commission. Following the investigation, the Commission required Vodafone to immediately remediate the problem (which was caused by a legacy IT system) and to publish on its website details of what had occurred, so that customers would be aware of the issue.

D. ***To ensure that the data is accurate and up-to-date[39]:*** This principle requires that a data controller takes reasonable steps to ensure the accuracy of the data, as well as its currency.

[37] In this situation, the Commission cautioned against the use of auto-fill functions in software, as it has inherent risks when used to populate recipient details for the purposes of transmitting personal data. They advised that where controllers decide to integrate such a function into their software for data-processing purposes, at a minimum other safeguards should be deployed, such as dummy addresses at the start of the address book, or on-screen prompts to double-check recipient details.

[38] Article 5(1)(c).

[39] Article 5(1)(d).

Accuracy and currency both require that the data is neither false nor misleading[40]. This can be achieved by ensuring that the data is obtained from a legitimate source and by undertaking a systematic review on a regular basis. In addition, where data is inaccurate, the data controller must ensure that it is erased or rectified without delay.

In *Case Study No. 12/2016* a third party address (which the complainant had historically provided to Permanent TSB (PTSB) as a correspondence address, when applying for the previous loan, which she held with her ex-husband), was incorrectly linked by PTSB to the entirely separate subsequent mortgage loan in the data subject's sole name. This was deemed to be in breach of PTSB's obligation to ensure that the customer's personal data was accurate and up to date. According to the Commission:

> *"Failure to adhere to this principle, particularly in the context of contact information perpetuates the risk that further data protection failures (such as unauthorised disclosure to third parties) will flow from such non-compliance."*[41]

E. ***To retain data for no longer than is necessary for the purpose or purposes for which it was obtained[42]:*** This principle requires that a data controller has a data retention policy. Under the terms of this policy, there should be a stated period for the retention of data[43], but also a simultaneous obligation to review the period of retention and determine whether such retention is still necessary in the circumstances. For example, an accountancy practice may have a stated data retention period in respect of client income tax returns to the Revenue Commissioner, but where they provide investment advice to a client, in relation to a one-off transaction, the same period of retention of their personal data may not necessarily apply. Where it is no longer appropriate to retain data or where the data becomes obsolete, the data controller should ensure that it is securely deleted.

Data controllers should also review whether it is necessary to retain data in its totality, or whether it can be minimised to what is appropriate. For example, following completion of a professional accountancy qualification, it would not be necessary for CPA Ireland to retain all of the personal data of their students, only that information that is necessary to verify their qualifications. Similarly, CPA Ireland will retain student exam scripts for the time-period necessary for a student member to request a review or recheck of an exam grade, but thereafter the retention of these scripts is not necessary, and they should be securely deleted.

In *Case Study No. 3 /2020* the complainants involved had previously requested that an Irish state agency erase a file pertaining to an incident at school involving their young child, which had originally been notified to the agency. However while the agency had decided that the incident did not warrant further investigation, it had refused to erase the minor's personal data — indicating that it was their practice to retain such files until the minor in question reached the age of 25 years. Following intervention by the Data Protection Commission, both parties

---

[40] For example, if an employee has worked for the same employer for the past ten years, and is now classed as an exemplary worker, retaining a verbal warning on their employment record, imposed for underperformance in their first year of employment, is likely to be classed as misleading. Similarly, the retention by CPA Ireland of a complaint of alleged cheating by a student in their professional examination, after a full-investigation and impropriety hearing determined that no such cheating took place, would be regarded as misleading.

[41] https://www.dataprotection.ie/en/dpc-guidance/case-studies-annual-report#201612

[42] Article 5(1)(e).

[43] Personal data may be stored for longer periods, where the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the Regulation. This extended retention is subject to an obligation on the data controller to implement appropriate technical and organisational measures to safeguard the rights and freedoms of the data subject.

engaged in amicable resolution and the state agency confirmed to the complainants that the file containing their child's personal data would be deleted.

F. ***All data must be retained in a manner that is both safe and secure***[44]: This principle requires that all data is processed in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. To comply with this principle, data controllers must ensure that they are employing appropriate technical and/or organisational measures. These may include[45]:

(1) The pseudonymisation and encryption of personal data;
(2) The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
(3) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(4) A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing[46].

The nature of the technical and organisational security employed by a data controller will depend on the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

Technical Security

Technical cybersecurity could encompass data encryption and pseudonymisation[47], as well as implementing a web application firewall (WAF)[48], an identity and access management system[49], a data loss prevention system, an incident response plan, third-party risk management protocols (where processing is being undertaken by a third party), a secure access service edge (SASE) system[50], as well as the implementation of a vulnerability management system[51]. According to Joshi[52], a vulnerability management system should revolve around the following:

[44] Article 5(1)(f).
[45] Article 32(1).
[46] This will require staff training and on-going risk assessments.
[47] GDPREU.org defines this as: *"the processing of personal data in such a way that the data can no longer be attributed to a specific data subject, without the use of additional information"*.
[48] This is a system for filtering, monitoring, and blocking any malicious HTTP/S traffic traveling to the web application, and prevents any unauthorised data from leaving the app. For example, Cloudflare.
[49] Such a system is likely to limit access to personal data for authorised parties. This could encompass a dual authentication system for remote access. For example, the banking sector in Ireland employs an authentication system via mobile phones, to reduce instances of credit/debit card fraud.
[50] These systems use cloud services to deploy security protocols to remote locations, and are particularly important for data controllers where employees are working from remote locations.
[51] This is a system designed to identify, evaluate, treat, and report on security vulnerabilities in systems and the software that runs on them. For example, QUALYS, Bitsight, Security Score Card etc…
[52] Joshi, Sagar, *What Is Vulnerability Management? Get the Answers You Need,* see: https://www.g2.com/articles/vulnerability-management

Data controller should also establish an information security policy, which encompasses a password management policy[53]. In *Case Study No. 25/2021* basic security settings, such as strong passwords were not properly enforced by the data controller and multi-factor authentication was not implemented. This left a medium-sized law firm open to a social engineering attack, which arose when a staff member opened an email from a malicious third party that secretly installed malware on their computer. This malware enabled monitoring email communications and permitted the hacker to defraud a client of the firm of a sum of money.

Technical security would also necessitate that all portable IT devices used outside the organisation are encrypted and that biometric access control systems are employed, where appropriate. Furthermore, the data controller should also adopt a remote work policy, with particular requirements in relation to the disposal of personal data. In *Case Study No. 23/2021* an employee of a health science focused university, who was working remotely during the pandemic, disposed of printed copies of a number of job applications and accompanying CVs into a domestic recycling bin. Unfortunately, high winds caused the contents of the bin, including the recruitment documents, to be dispersed. In determining that a breach had arisen, the Commission highlighted that it is the responsibility of the data controller to ensure that employees who work remotely have the means to adhere to the principles of data protection, including, where appropriate, the provision by the controller of devices, such as shredders, to employees to ensure the safe deletion of data.

In addition, technical security would necessitate that systems are designed with access controls, to ensure that only necessary parties can access the data and greater access limitations or controls should apply to highly sensitive data. This is known as data protection by design[54]. In *Case Study No. 6/2021* a breach arose as highly sensitive categories of personal data (including details of an employee's attendance with the company doctor, as well as information about their physical health, mental health and personal circumstances), as well as data pertaining to the employee's personal injury claim against the employer, and details of a disciplinary procedure taken against them, were stored on a shared drive (which could be viewed by anyone in the company), and a copy of this data was also left on a CD-ROM on the employee's desk.

---

[53] All users of a system should have a unique identifier (such as a password, passphrase, smart card or other token) to allow access to personal data. This should necessitate users adopting strong passwords (minimum 12-characters) or passphrases, not re-using old passwords/phrases and requiring passwords/ phrases to be up-dated on a regular basis. According to www.mcafee.com cybersecurity experts recommend changing passwords/phrases every three months.

[54] For example, CPA Ireland could design a student data management system that ensures that only employees of the Exams Department, as well as other authorised personnel, could access this data – and that such data is not accessible from their staff network portal.

Organisational Security

Organisational security would necessitate the data controller building a culture of security awareness amongst staff, ensuring that data protection officers have the appropriate resources and authority to do their job effectively, ensuring all manual data is secure and disposed of appropriately[55] and that obsolete IT hardware is wiped of any data prior to its disposal, as well as limiting access of non-employees to buildings and equipment[56]. Physical organisational security would include the data controller reviewing the quality of doors and locks, and protecting the business premises by means as alarms, security lighting or CCTV, and access logs.

Reporting of Data Breaches

All data breaches must be reported to the Data Protection Commission[57] within 72 hours of knowledge[58] of the breach[59]. However, such a report is unnecessary where the breach is unlikely to result in a risk to the rights and freedoms of natural persons[60]. Where a data controller fails to adhere to this requirement, they will be required to explain this failure to the Commission. This notification should include[61]:

(1) A description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(2) The name and contact details of the data protection officer or other contact point where more information can be obtained;
(3) A description of the likely consequences of the personal data breach; and
(4) A description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where the breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the nature of the breach to the data subject in clear and plain language, without undue delay[62]. Where the breach arises from a hacking incident, this should be reported to An Garda Síochána.

---

[55] This could include a clean desk policy, locked desks and filing cabinets, locked offices etc …

[56] This could include ensuring that non-employees sign in at reception, are given a visitor access pass and accompanied by an employee during their time on the premises.

[57] All breach notifications must be notified to the Commission using the *Breach Notification Form*. All cross-border personal data breaches must be indicated as being cross-border on the relevant section of the form. In 2021 the Commission received 6,616 personal data breach notifications under Article 33 of the GDPR, a 2% decline on 2020. The highest category of data breaches notified in 2021 (71% of reported breaches) related to unauthorised disclosures. In terms of sectoral breaches, 3,677 related to the private sector, 2,707 to the public sector and the remaining 232 came from the voluntary and charitable sector.

[58] Knowledge in this regard is interpreted as when the data controller has a reasonable degree of certainty that a security incident has occurred and compromised personal data – see: Article 29 Working Party Guidelines, at p.10.

[59] Article 33(1).

[60] However, the Data Protection Commission guidance on reporting breaches states: *"… for all breaches – even those that are not notified to the DPC on the basis that they have been assessed as being unlikely to result in a risk – controllers must record at least the basic details of the breach, the assessment thereof, its effects, and the steps taken in response …"* See the DPC's Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR, at p. 5 - https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

[61] Article 33(3).

[62] Article 34(1).

Following receipt of a data breach report the Commission may determine that a more detailed report and/or subsequent investigation are necessary.

Rights of the Data Subject:
Under the terms of the Regulation, a data subject possesses a number of rights. These include the following:

A. **Right to Communication**[63]: A data subject has the right to communication from the data controller relating to the processing of their data in a concise, transparent, intelligible and easily accessible format, using clear and plain language. The information must be provided in writing, or by other means, including, where appropriate, by electronic means, unless otherwise agreed with the data subject. In *Case Study No. 2/2018* a complaint regarding the provision of CCTV data to a third party, also encompassed a lack of communication regarding the use of CCTV by the data controller. However, the Commission determined that a breach had not arisen in the latter case as the data controller (the owner of a bar) had adequate signage alerting patrons to the use of CCTV for the purpose of protecting staff and customers and preventing crime, and that in the absence of any evidence to the contrary offered by the complainant, the complainant had been on notice of the use of CCTV at the time in question.

B. **Rights to Prescribed Information**[64]: Specified data must be provided to the data subject at the time when their personal data is obtained, including: (1) the identify and contact details of the data controller, (2) contact details of their DPO (where appropriate), (3) the purpose and basis for the processing, (4) any legitimate interest in the processing, (5) the recipients of the data, (6) any intention to transfer it to a third country or international organisation, (7) the period and criteria for retention, (8) details of the right to request a restriction on processing, or rectification or erasure of the data, (9) the right to withdraw consent to processing, (10) the right to lodge a complaint to the Data Protection Commission, (11) any statutory or contractual requirements for the processing of the data, and (12) whether the data is being used for automated decision-making (including profiling).

C. **Right to Make a Data Subject Access Request (SAR)**[65]: A data subject is entitled to information regarding the processing of their data and to obtain a copy of their personal data undergoing processing, without charge. There are no specific formalities that a data subject must comply with when making this request. Such a request can be made either verbally[66] or in writing, and should generally contain enough detail in order to allow the data controller to source the data[67]. For example, a client of an accountancy practice may request the practice to provide them with details of all invoices sent to them, in respect of the preparation of their self-assessment revenue returns, from 2010-2023. A data controller should comply with such a request[68]

[63] Article 12. All such communications should be provided free of charge to the data subject, except where they are manifestly excessive or unfounded.
[64] Article 13. In accordance with Article 14, similar prescribed information should be provided to the data subject, where their personal data has not been obtained directly from them.
[65] Article 15.
[66] In this situation, the Data Protection Commission recommends that data controllers record the time and details of the request, in order that they can comply with their statutory obligations.
[67] This is particularly relevant, where the controller processes a large quantity of the subject's personal data.
[68] When complying with such a request, the data controller is entitled to request verification from the applicant that they are the person named in the request. This can be achieved by the applicant providing official documentation, confirming their identity. In this situation, the prescribed timeframe for compliance does not start to run until they have received confirmation of identity. In *Case Study No.2/2021* the data controller (a hotel) asked the data subject (a former guest) to verify their identity by providing a copy of a

without undue delay, and at the latest within one month of receiving the request[69]. Non-compliance with a request is a breach of the legislation[70].

The data subject can require that a portable copy of their personal data be sent to them or sent directly to another entity[71]. Otherwise, such data should be provided in the same method as the request was made, and where the request is made electronically the data can be provided in a commonly used electronic format, unless the individual requests otherwise.

A data controller may consider it justifiable to withhold certain information in response to SAR. In this situation, the controller must identify the exemption under the GDPR or the Data Protection Act 2018 that they are exerting, provide an explanation as to applicability of this exemption and demonstrate that reliance on the exemption is both necessary and proportionate. In *Case Study No. 9/2021* a parent applied to An Garda Síochána for copies of the personal data of his young children. However, An Garda Síochána refused to supply the data. Following a review by the Data Protection Commission the parent was informed that the Commission agreed with the restriction imposed. The rationale for this restriction arose from the fact that the controller had particular knowledge of all of the circumstances pertaining to a shared guardianship arrangement in place (between the parents of the child) and considered that consent of all legal guardians would be required in order to release the data.

Where a SAR involves third party data, the data controller can redact the third party data, seek the consent of the third party to the disclosure, or where redaction is impossible and consent is refused (or cannot be obtained), the data controller can advise the data subject that they are unable to comply with the request. In *Case Study No. 10/2021*, in response to a SAR restrictions were imposed by An Garda Síochána, based on exemption prescribed by the Data Protection Act 2018. The matter related to an individual seeking copies of allegations of abuse made against him with regard to the welfare of his parents. Having examined this matter, the Data Protection Commission determined that releasing the information would entail the release of third-party data and would reveal the identity of the person who made the allegations against him. As the information provided by the third party was supplied in the strictest of confidence, the Commission considered that a statutory exemption applied[72], and the Gardaí were correct in terms of their non-compliance with the request.

---

utility bill and a copy of photo ID verified by An Garda Síochána. The Commission questioned the necessity for this given that the postal address and email address being used by the requester were the same as those provided by them during the booking and check-in process at the hotel. According to the Commission: *"controllers should only request the minimum amount of further information necessary and proportionate in order to prove the requester's identity. Seeking proof of identity would be less likely to be appropriate where there was no real doubt about identity; but where there are doubts, or the information sought is of a particularly sensitive nature, then it may be appropriate to request proof."*

[69] This period may be extended by a further term of two months where the request is complex, or where a data controller has received a number of requests from the same individual. In this situation, the controller must inform the data subject within one month of receiving their request and explain the rationale for the application of the extension.

[70] In *Case Study No. 2/2020*, the failure by an auction house to respond to an SAR was deemed to be a breach, despite the fact that the controller had deleted historical manual data (from 2016) relating to the applicant (data subject), and that all electronic data had been deleted when a new IT system was installed in 2018. The essence of the breach was the failure by the data controller to provide information on actions they had taken in relation to a subject access request, even in circumstances where this is to inform the individual applicant that it does not hold any data.

[71] This is known as the right of data portability.

[72] Section 91(9)(a), the Data Protection Act 2018.

Similarly, in exceptional circumstances, where a SAR is deemed to be manifestly excessive or unfounded, a data controller may refuse to comply with the request, but the burden on proof rests on them in this regard.

D. **Right to Rectification[73] and Erasure[74]:** The data subject has the right to the rectification of inaccurate personal data held by the data controller. This rectification should take place without delay. Taking into account the purposes of the processing, the data subject also has the right to have incomplete personal data completed, including by means of providing a supplementary statement. In *Case Study No. 1/2007* the Data Protection Commissioner (now the Commission) noted that the right to rectification is not absolute and may not always be appropriate[75].

The data subject also has the right to request the erasure of their data (known as the right to be forgotten) where its retention is no longer necessary for the purpose for which it was retained[76], where they have withdrawn consent to processing, where they object to processing[77], where the data has been unlawfully processed, where the information is inaccurate, and where the deletion is in compliance with EU law. Similar to the right of rectification, the right to erasure is not absolute[78]. However, the Court of Justice of the European Union has stated that the right to freedom of expression and information could not be taken into account where a part of the information found in the referenced content proved to be inaccurate[79]. In a request for erasure or rectification on the grounds of inaccuracy, the burden is on the data subject to establish the manifest inaccuracy of the data. In reviewing the obligation on internet search engines to delete personal data from search results based on allegations of inaccuracy, the Court stated:

> *"… where the person who has made a request for de-referencing submits relevant and sufficient evidence capable of substantiating his or her request and of establishing the manifest inaccuracy of the information found in the referenced content or, at the very least, of a part – which is not minor in relation to the content as a whole – of that information, the operator of the search engine is required to accede to that request for de-referencing. The same applies where the data subject submits a judicial decision made against the publisher of the website, which is based on the finding that information found in the referenced*

[73] Article 16.
[74] Article 17.
[75] In this case, the applicant sought the rectification of data in a medical report completed by an independent consultant psychiatrist, on the request of the applicant's employer. In the circumstances, the Commissioner noted that as the issues were medical in nature and therefore involve sensitive/special categories of data, that the applicant data subject's comments in respect of the accuracy of the data should be given careful consideration. As a result of the applicant providing various annotations to the Commissioner to be included in the medical report, they concluded that as the annotations were well founded the data should be rectified.
[76] For example, where a person applies for a job and is unsuccessful, they can request that the data controller subsequently delete their personal data. Similarly, the closure of a bank account or an online social media account, could result in a request by the data subject to be forgotten.
[77] In this situation, the data controller must be unable to demonstrate legitimate grounds for the processing.
[78] However, the data subject's rights to protection of private life and protection of personal data override, as a general rule, the legitimate interest of internet users who may be interested in accessing the information in question.
[79] *TU and RE v Google LLC.* (2022) Case C-460/20. This case concerned two managers of a group of investment companies. These managers requested that Google de-reference (erase) results of a search made on the basis of their names, which provided links to certain articles criticising that group's investment model. They asserted that the articles contain inaccurate claims. They also requested Google to remove photos of them, displayed in the form of 'thumbnails', from the list of results of an image search made on the basis of their names. Google refused to comply with this request.

content – which is not minor in relation to that content as a whole – is, at least prima facie, inaccurate.

By contrast, where the inaccuracy of such information found in the referenced content is not obvious, in the light of the evidence provided by the data subject, the operator of the search engine is not required, where there is no such judicial decision, to accede to such a request for de-referencing. Where the information in question is likely to contribute to a debate of public interest, it is appropriate, in the light of all the circumstances of the case, to place particular importance on the right to freedom of expression and of information."[80]

In *Case Study No. 7/2021* a delisting/erasure request in relation to three URLs, which appeared as results to searches of the individual's name on the search engine were refused. Although the complainant alleged that the statements were inaccurate and defamatory, the Commission noted that the statements were user-generated content and represented third party opinions rather than appearing as verified facts. According to the Commission:

"The role of the search engine in listing is not to challenge or censor the opinions of third parties unless to list results gives rise to personal data processing on the part of the search engine that is irrelevant, inadequate or excessive."[81]

In the circumstances, the Commission concluded that given the individual's business role and role in public life arising from their professional life, there was a public interest in accessing information regarding their professional life within the EU.

E. **Right to Restriction on Processing[82]:** Where the data subject alleges that the data being processed is inaccurate, unlawful, excessive or without legitimate grounds for processing, they can request a restriction on processing. In effect, this means that the data is marked, with the aim of limiting its processing in the future[83]. Where a restriction is imposed such data cannot be processed without the data subject's consent, unless it is for the establishment, exercise or defence of legal claims, for the protection of the rights of another person or for reasons of important public interest of the EU or its member states.

F. **Right to Data Portability[84]**: The data subject has the right to receive their data, as well as the right to request that all of their data is transferred to another third party[85] (where such a transfer is technically feasible). For example, a client of an accountancy practice, who operates a business as a sole trader, may decide to change accountants, and has the right to request that all of their personal data is transferred to their new accountant.

G. **Right to Object:** A data subject has the right to object to their data being used for direct marketing purposes[86] (including profiling)[87]. In 2021 *Three Ireland (Hutchison) Limited*[88] and

[80] Ibid at para. 72-73.
[81] https://www.dataprotection.ie/en/dpc-guidance/case-studies-annual-report#202107
[82] Article 18.
[83] Article 4(3).
[84] Article 20.
[85] This right applies where processing is based on consent, necessary for the completion of a contract or involves automated decision making.
[86] Article 21(2).
[87] This includes sending unsolicited communications to the data subject.
[88] They were also prosecuted for the same offences in 2020 and 2012.

Vodafone Ireland Limited[89] were both found guilty of offences related to the use of personal data for marketing purposes without consent, and were fined and subject to the application of the Probation of Offenders Act 1907. Similarly, in 2019, *Vodafone Ireland Limited, Just-Eat Ireland Limited, Cari's Closet Limited* and *Shop Direct Ireland Limited t/a Littlewoods Ireland* were all prosecuted for the same offences and were subject to the same sanctions.

A data subject also has the right to object to being subjected to a decision based solely on automated processing, including profiling, which produces legal effects or a significant impact[90].

All of the aforementioned rights may be restricted, where deemed necessary and proportionate, in order to: (1) safeguard national security, defence and public security, (2) prevent, investigate, detect and/or prosecute criminal offences or execute criminal penalties, (3) achieve the objectives of general public interest of the EU, (4) protect judicial independence and judicial proceedings, (5) prevent, investigate, detect and/or prosecute breaches of ethics for regulated professions, (6) monitor, inspect or regulate functions connected to the exercise of official authority, (7) protect the data subject or the rights and freedoms of others, and (8) enforce civil law claims[91].

Enforcement and Sanctions:
The Data Protection Commission is the national independent supervisory authority responsible overseeing compliance with the GDPR and Data Protection Acts 1988-2018[92]. It is responsible for upholding the fundamental right of individuals in the EU to have their personal data protected. Its stated mission statement is:

> *"… [to] safeguard data protection rights by driving compliance through guidance, supervision and enforcement."*

As part of its statutory powers, the Data Protection Commission has the authority[93]:

A. To examine complaints from individuals in relation to alleged infringements of data protection law[94].
B. To conduct inquiries and investigations regarding infringements of data protection legislation and to take enforcement action where necessary[95].
C. To promote awareness amongst members of the public of their rights to have their personal information protected under data protection law[96].

---

[89] They were also prosecuted for the same offences in 2019, 2018, 2013 and 2011.
[90] Article 22. This excludes where the automated processing does not relate to special categories of data and is based on explicit consent, is necessary for the performance of a contract, or is authorised by EU law.
[91] Article 23.
[92] As well as the Irish ePrivacy Regulations (2011) and the EU Directive known as the Law Enforcement Directive.
[93] https://www.dataprotection.ie/en/who-we-are/what-we-do
[94] The DPC received 3,419 complaints in 2021 and concluded 3,564 complaints, including 1,884 complaints received prior to 2021. In 2021, the most frequent GDPR topics for queries and complaints continued to be: (1) access requests (37%), (2) fair-processing (37%), (3) disclosures (20%), (4) direct marketing, and (5) the right to be forgotten (delisting and/or removal requests).
[95] The DPC concluded 7,081 queries in 2021, including 826 received prior to 2021. The largest fines imposed in 2021, following inquiries into breaches included: (1) a €90,000 fine to the Irish Credit Bureau (completed in March 2021), (2) a €110,000 fine to MOVE Ireland (August 2021), (3) a €110,000 fine to Limerick City and County Council (December 2021), (4) a €225m fine to WhatsApp (August 2021), and (5) a €60,000 fine to The Teaching Council (December 2021).

D. To drive improved awareness and compliance with data protection legislation by data controllers and processors through the publication of high-quality guidance, as well as proactive engagement with public and private sector organisations.[97]
E. Through consultations with organisations, to assist in identifying risks to personal data protection and offer guidance of best practice methods to mitigate against those risks[98].
F. To cooperate with (including sharing information) other data protection authorities, and act as Lead Supervisory Authority at EU level for organisations that have their main EU establishment in Ireland.

The main enforcement powers of the Data Protection Commission include:

(1) The Commission and its authorised officers are empowered to serve an enforcement notice or an information notice on a data controller or processor. An enforcement notice is served where the Commission is of the opinion that a controller or processor has contravened their data protection obligations, and requires rectification of this breach[99]. An information notice requires a data controller to provide the Commission with information in relation to matters specified in the notice[100]. Non-compliance with either of these notices can result in the imposition on summary conviction of a class A fine and/or imprisonment for a term not exceeding 12 months, whereas a conviction on indictment can result in the imposition of a fine not exceeding €250,000 or imprisonment for a term not exceeding 5 years or both.

(2) The Commission is also empowered to enter the premises of a data controller or processor, and search and inspect that place for any documents, records, statements or other relevant information, as well as remove documents (where required)[101]. The Commission can also obtain a search warrant from the District Court, where it is necessary for the performance of their functions[102]. They can also require the data controller or processor to prepare a written report for them in relation to their data processing[103], and possess the authority to undertake a data protection audit[104].

In accordance with Article 58(2) of the GDPR the Data Protection Commission also has the following corrective powers:

A. To issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of the Regulation.

---

[96] In 2021, DPC Staff presented at over 90 speaking events. As Covid-19 restrictions came into effect, the majority of staff participation was conducted online, except where public health guidance permitted.
[97] In 2021, the DPC published its finalised *Fundamentals for a Child-Oriented Approach to Data Processing*, which is intended to provide direction to organisations involved in the processing of children's data.
[98] In 2021, the legislative measures that the DPC engaged in consultation on included, the Birth Information and Tracing Bill, the Garda Síochána (Powers) Bill and the Garda Síochána (Digital Recording) Bill, the Judicial Appointments Commission Bill, the Policing and Community Safety Bill, the Protected Disclosures (Amendment) Bill, the Sex Offenders (Amendment) Bill, the Teaching Council (Information to be furnished by employer in case of dismissal or resignation) Regulations 2021, the Workplace Relations (Miscellaneous Provisions) Bill and the Inspection of Places of Detention Bill. It also consulted with the healthcare sector, regarding anti-money laundering regimes, smart metering and insurance.
[99] Section 133, Data Protection Act 2018.
[100] Ibid at Section 132.
[101] Ibid at Section 130.
[102] Ibid at Section 131.
[103] Ibid at Section 135.
[104] Ibid at Section 136.

B. To issue reprimands to a controller or a processor where processing operations have infringed provisions of the Regulation.
C. To order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to this Regulation.
D. To order the controller or processor to bring processing operations into compliance with the provisions of the Regulation, where appropriate, in a specified manner and within a specified period
E. To order the controller to communicate a personal data breach to the data subject.
F. To impose a temporary or definitive limitation including a ban on processing.
G. To order the rectification or erasure of personal data or restriction of processing .
H. To withdraw a certification or to order the certification body to withdraw a certification, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met.
I. To order the suspension of data flows to a recipient in a third country or to an international organisation.
J. To impose an administrative fine pursuant to Article 83, in addition to, or instead of the aforementioned corrective measures.

Administrative Fines

Breaches of data protection obligations may also result in the imposition of administrative fines. For especially severe violations (as set down in Article 83(5) GDPR), the fine framework can be up to €20 million, or in the case of an undertaking, up to 4% of their total global turnover of the preceding fiscal year, whichever is higher. For less severe violations, (Article 83(4) GDPR) fines of up to €10 million can be imposed, or, in the case of an undertaking, a fine of up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher.

The following factors are taken into consideration, when determining the quantum of the fine to be imposed:

A. The nature, gravity and duration of the infringement
B. The number of data subjects affected, the type of personal data affected and the level of damage suffered by the data subject
C. Whether the infringement was intentional or negligent
D. The measures taken by the Data Controller to mitigate the damage suffered by the data subject
E. The degree of responsibility and co-operation by the data controller/processor
F. The controller/processors history of past breaches
G. Any of relevant or mitigating factors.

The Data Protection Commission issued more than €1.64 billion in fines from January 2022 to January 2023, according to a report by law firm DLA Piper (this compared to €1.1 billion in 2021)[105]. In total, since the implementation of the General Data Protection Regulation European regulators have issued a combined €2.92 billion in fines. The report noted that Ireland ranked highest for fines imposed, with five of the top ten fines issued by the Irish Data Protection Commission. The highest GDPR fine of 2022 was levied against Meta-owned social networking platform Instagram, by the Irish Data Protection Commission[106]. The €405 million sum is also the second-highest fine under GDPR, after Amazon's €746 million penalty in 2021.

[105] See: https://www.dlapiper.com/en-ae/insights/publications/2023/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2023
[106] This is currently subject to appeal.

Compensation for Data Protection Breaches

There are no provisions in either the Data Protection Acts 1988-2018 or the General Data Protection Regulation for the automatic payment of statutory compensation for data breaches. Any such action is limited to an action under the law of tort, in respect of the negligence of a data controller or processor. To succeed in such a claim the data subject must prove that (1) there was a breach of data protection law, (2) they suffered damage[107], and (3) the damage was caused by the breach. According to Justine Feeney in *Collins v FBD Insurance* (2013)[108]:

> *"It is consistent with the general principles of the Irish law of torts that a person seeking compensation arising from a breach of statutory duty must establish that the loss or damage which they have sustained flowed from that breach."*[109]
>
> *"The tort of negligence … requires proof of damage."*[110]

In *UI v Österreichische Post* (2021)[111] the Advocate General rejected the argument that there is an irrebuttable presumption of damage once a GDPR violation has occurred, particularly that an infringement results in a "*loss of control*" over data[112]. He stated that compensation should not be available for "*mere annoyance or upset*". Therefore, the data subject must demonstrate some distress or damage over a *de minimis* threshold of triviality to succeed in a claim for compensation[113]. The mere infringement of provisions of the GDPR is insufficient for the purposes of awarding compensation.

Conclusion:

Given the range of sanctions and the severity of fines that can be imposed for non-compliance by a data controller or processor with their data protection obligations, they should undertake a voluntary audit to assess levels of compliance, regularly review their systems and procedures, and seek professional guidance and advice, where appropriate.

---

[107] This can be either financial or non-financial damage, such as damage to reputation.

[108] [2013] IEHC 137.

[109] Ibid at para 21/3.6.

[110] Ibid at para 27/4.4.

[111] Case C-300/21.

[112] This was also reiterated in *Lloyd v Google LLC* [2021] UKSC 50 wherein the UK Supreme Court stated that their Data Protection Act 1998 (UK DPA) could not *"reasonably be interpreted as giving an individual a right to compensation without proof of material damage or distress…".*

[113] As per *Rolfe & Ors v Veale Wasbrough Vizards LLP* [2021] EWHC 2809 (QB). Furthermore, Justice O'Donohue in the Irish Circuit threw out claims for compensation in respect of data protection breaches by SIPTU stating that proof of *"more than minimal loss"* was necessary before such cases could succeed.