Data Protection Series | Sanctions for non-compliance

Two years have passed since the introduction of the GDPR on 25 May 2018, and data protection compliance remains a significant and complex challenge for employers. Some of the main issues in this respect include:

- responding to data subject access requests by current or past employees;
- identifying the legal basis for processing employee data including special category data;
- managing employee records and data retention; and
- monitoring employees in the workplace.

This first article in our data protection series will discuss the importance of ensuring compliance with GDPR in the workplace and the repercussions for failing to do so.

For some, GDPR compliance is prioritised as part of an organisation's culture and belief in protecting the rights of data subjects. For others, the risk of action from the Data Protection Commission (the "**DPC**") and compensation claims from employees remain key factors motivating compliance. However, these two motives are not always mutually exclusive, and the consequences for non-compliance is an understandable concern for any organisation.

Employment disputes and the role of the DPC

The DPC's 2019 Annual Report[1] explained that disputes between employees and employers or former employers remain a significant theme of the complaints it deals with. Such disputes that require the DPC's involvement have centred on the employer's right to process certain personal data of the employee as part of the main employment dispute.[2] This may result in the DPC making an order that the employer does not have a right to process the employee's data, which can ultimately impact the employer's right to rely on such data as part of the employment dispute.

Where the employee's complaint indicates that the alleged data breach is of an extremely serious nature and/or indicative of a systemic failing by the employer, the DPC may decide to commence an inquiry. This may result in the DPC issuing a formal decision on the matter and/or the organisation being subject to an administrative fine or other corrective power.

Administrative Fines

The DPC can directly impose administrative fines on organisations that fail to comply with GDPR. This includes a fine of either:

- 2% of an employer's annual worldwide turnover, or €10 million (whichever is higher); or
- 4% of an employer's annual worldwide turnover, or €20 million (whichever is higher).

Whether a lower or higher tier fine will apply will depend on the type of breach that has occurred.[3] Article 83 of the GDPR sets out factors that the DPC must consider before imposing a fine, including: the gravity and the nature of the infringement, whether the infringement was intentional or negligent, whether any actions have been taken by the organisation to mitigate damage to data subjects, whether the employer has cooperated with the DPC and if the employer notified the infringement to the DPC.

Corrective Powers

Where, on the basis of an inquiry, the DPC decides that an infringement has occurred, a corrective power may be applied against the organisation. These include powers to:

- issue reprimands to an employer;
- order the employer to comply with an individual's request to exercise their rights;
- order the employer to bring its data processing operations into compliance with the GDPR;
- order the employer to communicate a personal data breach to an individual;

---

[1] The DPC's 2019 Annual Report can be accessed here

[2] For further information, see our article on *Doolin v the Data Protection Commission [2020] IEHC 90* here.

[3] Further information on the lower and higher tier fines can be accessed by clicking here.

- impose a temporary or permanent ban limitation on an organisation, including a ban on processing personal data;
- order the rectification or erasure of personal data or the restriction of the processing of personal data;
- withdraw certification or order a certification body to withdraw (or not issue) certification, where requirements for certification are not or are no longer met;
- impose an administrative fine, in addition to or instead of another corrective power; and
- order the suspension of data flows to a recipient in a third country or an international organisation.

Individual Redress

In addition to making a complaint to the DPC, an individual may pursue a data protection action in either the Circuit or High Court for compensatory or injunctive relief against a controller or processor for a breach of their data rights resulting in both "material" damage (i.e. direct financial loss such as loss of earnings) and "non-material" damage (i.e. non-quantifiable damages such as pain and suffering). Recital 75 of the GDPR provides examples of such damages including discrimination, loss of confidentiality and even reputational damage. Reputational damage is particularly relevant within the employment context considering the impact that this can have on an employee's right to earn a livelihood.

In this regard, under the GDPR, controllers and processors are joint and severally liable for any damage caused to an individual. This means that where both a controller and processor are involved in the same processing and are responsible for the damage caused to the individual, each will be held liable for all of the alleged damages and the individual will only need to make a claim against one of them. The controller or processor can subsequently claim compensation from the other for any damage that they are responsible for.

This provides the individual with the opportunity to elect the organisation to pursue for damages provided, of course, that they were in some way responsible for the alleged damage. As the GDPR does not set a maximum limit for any compensation awarded, it is likely that the resources of the controller/processor will be a primary factor when initiating such litigation and in the majority of cases, the party with the deeper pockets will be the employer.

In addition, a data subject - or group of data subjects - can authorise a not-for-profit body, organisation or association that is committed to the protection of personal data, to bring an action on their behalf for a breach of their data protection rights.[4] This provides data subjects with greater resources in litigating their rights from the outset of any such claim.

Compliance as the best line of defence

In light of the potential liabilities under the GDPR, the best defence for an employer is to ensure it has appropriate procedures in place to demonstrate GDPR compliance. Even where an individual successfully demonstrates there has been a breach of their data protection rights, employers can help mitigate any potential sanctions/damages by pointing to efforts made to achieve compliance.

The second article in our data protection series will discuss the impact of data subject access requests within the context of employment disputes and how such requests can prove to be a powerful litigation weapon in the disgruntled employee's armoury.

Our Employment & Corporate Immigration Department regularly advise employers in respect of data protection issues within the context of employment disputes. If you or your organisation have any queries regarding the issues outlined in this article, please contact Bláthnaid Evans or Sheila Spokes on +353 1 639 3000 or visit www.leman.ie.

[4] Article 80 GDPR and Section 117 of the Data Protection Act 2018