LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

GDPR and Employee Data

by **lk-shields**

GDPR and Employee Data

8th February 2018 | by

Most firms collect and process personal data relating to their employees on an ongoing basis as part of their everyday personnel administration. Personal data processed by your firm could be anything from salary details for administering payroll to sick notes presented by employees regarding absence. As a result, most firms will be affected by the EU General Data Protection Regulation ("GDPR"), which will regulate the processing of personal data, when it becomes directly applicable from the 25 May 2018. With 4 months to go before the GDPR applies to your firm, this article focuses on what the GDPR is and some practical measures you should consider in terms of processing employee data.

What is the GDPR?

Over the past 2 years, we have noticed many organisations struggle to assess where they should start in terms of preparing for the GDPR. It is helpful to remember that we have had data protection legislation in Ireland since 1988 and therefore firms who have taken data protection compliance seriously are already in good shape for meeting the GDPR's increased compliance standards. The GDPR builds upon and enhances many of the existing data protection requirements and principles under current Irish data protection legislation. The GDPR should be viewed as an opportunity to re-visit your firm's level of data protection compliance rather than feared.

From the 25 May 2018, the GDPR will replace the 1995 Data Protection Directive, which is the EU Legislation on which the main Irish data protection legislation, the Data Protection Acts 1988 and 2003 (as amended) (the "DPA"), is based. There will also be Irish implementing national legislation to give further effect to, and provide for exemptions, from the GDPR. In Ireland, the Department of Justice and Equality published the General Scheme of the Data Protection Bill 2017 in May 2017 ("General Scheme"). The General Scheme essentially sets out the heads that are proposed to be included in the Irish implementing legislation when it is enacted. As a general comment, the General Scheme is very much in draft form and is lacking in detail. Therefore, publication of the draft Bill is anxiously awaited. At the time of writing, it is not yet known when a draft Bill will be published, but it may be released before publication of this article.

"Consent" in Employment Contracts

As with the current DPA, in order to process an employee's personal data your firm needs a legal basis to do so. Many of the legal bases that employers currently rely upon to process employee personal data will continue to exist under the GDPR. The most relevant legal bases to employers both under the DPA and the GDPR are the following:

- the employee has given their consent to the processing;
- processing is necessary for the performance of a contract to which the employee is a party to;
- processing is necessary in order to take steps at the request of the employee prior to entering into a contract;
- compliance with a legal obligation;
- processing is necessary to comply with the employee's vital interests; and
- for the purposes of the legitimate interests of the firm.

In practice, we find that many employers tend to rely upon the first legal basis mentioned above for data processing, namely consent, which is usually procured in the Employment Contract. For consent to be valid, it must among other things be "freely given", which raises concerns in an employment context, as it is questionable whether an employee's consent is freely given on the basis of the imbalance of power between an employer and an employee. The Irish Office of the Data Protection Commissioner ("ODPC") has also raised this concern in the context of the existing DPA. The Article 29 Working Party, which is the representative group of EU Data Protection Authorities, recently commented in non-binding guidance that an employee is rarely in a position to give free consent.

Significantly for employers, consent can also be retracted by employees at any time and it must be as easy to withdraw consent as it is to give it. Operationally, firms will need to have the resources in place to facilitate an employee retracting their consent.

Another point to bear in mind when relying upon consent is that certain data subject rights can only be exercised where consent is the legal basis, for example the right to data portability and the so-called "right to be forgotten".

Based on the concerns with relying upon consent, now is the time to consider whether alternative legal bases could be relied upon by your firm for certain processing of personal data. For example, processing an employee's details as part of payroll could instead be based upon the legal basis of performance of a contract with the employee. There may, however, be situations where consent is the only appropriate legal basis to rely upon. Such a situation may arise for example in the context of processing an employee's medical information where such processing is not required by employment law. Where it is necessary to rely upon consent as a legal basis, consent should be procured through a declaration or other document separate to the Employment Contract which is not intrinsically linked to the employee's acceptance of their employment with the firm.

Data Subject Rights

The GDPR introduces new data subject rights and also modifies some of the existing rights under the DPA. A modified right which many firms may be familiar with is the data subject access right ("SAR"), which essentially gives an individual the right to receive a copy of their personal data which a data controller (e.g. an employer) holds about them. In practice, we are finding SAR's are being made more frequently by employees, particularly as an alternative to discovery in litigation or as a fishing exercise prior to making an employment claim against the employer.

SARs as they currently exist can be onerous for an employer to comply with and the GDPR is not making them any easier from an employer's perspective. The current tight timeframe to respond to a SAR of "as soon as may be" but not longer than 40 calendar days will shorten under the GDPR to a response being required "without undue delay" and in any event within one month of receiving a valid access request. Currently under the DPA, employers are entitled to charge an administrative access fee of €6.35 for processing a SAR, which will be abolished by the GDPR unless the employer can demonstrate that the cost will be excessive.

The shorter timeframe for responding to a SAR means that firms will need to ensure that they have the policies and procedures in place to comply with a SAR received and that it has sufficient staff and resources to comply with a SAR. However, if a request is complex or a number of requests are made, then the timeframe can be extended by a further two months where necessary, provided the data subject is informed of the extension and the reasons for it within one month of the employer having received the SAR.

Accountability

Accountability is a core principle of the GDPR. It requires that firms not only comply with the GDPR by implementing appropriate technical and organisational measures and appropriate data protection policies, but they must also be able to demonstrate their compliance. The current Data Protection Commissioner, Helen Dixon, has previously noted that this is not just a pen pushing exercise. Therefore, you need to be able to meaningfully demonstrate compliance. As such, this will involve more than simply having data

protection policies and processing registers in place that comply with the GDPR, but your firm will also need to be able to show that it has implemented such policies which could be through staff training and regular checks and testing for example.

Information to be provided to employees

As with the DPA, under the GDPR certain information must be supplied to employees before their personal data is collected and processed by your firm, otherwise such processing is unlikely to be considered fair and is likely to be contrary to the data protection principle that personal data must have been obtained and processed fairly and lawfully. The information will typically be provided in the form of a notice to job candidates and a further privacy policy will be supplied to successful job applicants as part of their on-boarding induction to the firm. While this information requirement continues under the GDPR, the content of such notices and policies will need to include additional information. Under the GDPR, the following information will need to be provided:

1. the firm's name and contact details and the name and contact details of your data protection office (where one has been appointed);
2. the purpose(s) of the processing as well as the legal bases for processing;
3. where the legal basis for processing is based on the firm's legitimate interests, those legitimate interests should be identified;
4. the recipients or categories of recipients of personal data;
5. that the firm intends to transfer personal data to a third country and the legal basis for the transfer;
6. the retention period for personal data and the criteria used to determine this;
7. how employees (or job candidates) can exercise their right of access, rectification, erasure, restriction to processing, objection to processing and data portability, if such rights apply to the employee (or job candidate);
8. how employees (or job candidates) can retract their consent to processing, where the processing by the firm is based on consent;
9. the right to submit a complaint to the relevant Data Protection Supervisory Authority;
10. whether the employee (or job candidate) is required to provide their personal data pursuant to statute or a contract, and the consequences of failing to provide such data; and
11. the existence of automated decision-making, including profiling, and the logic and consequences of the processing for the employee (or job candidate).

It is important to review your existing notices and policies given to employees and job candidates in order to check that they include the above information.

Data Protection Officer ("DPO")

An important change being introduced by the GDPR is the requirement for certain data controllers and processors to appoint a DPO. The DPO be responsible for overseeing an organisation's compliance with data protection. The DPO is not, however, a new concept. While this will be the first time in Ireland that this role has been codified, many organisations may already have an individual responsible for data protection compliance and DPO's are in fact required in Germany. What is new under the GDPR is the fact that a DPO must under statute be appointed for the following controller and processor organisations:

public authorities or bodies (except for courts acting in a judicial capacity);
data controllers and processors whose core activities consist of processing "which require regular and systematic monitoring of data subjects on a large scale"; and
data controllers and processors engaged in large scale processing of sensitive personal data or personal data relating to criminal convictions and offences.

The Article 29 Working Party in guidance recommends that controllers and processors document their internal analysis conducted to decide whether a DPO is required. An important point that the Article 29 Working Party have also highlighted is that while organisations are free to voluntarily appoint a DPO and the Article 29 Working Party encourages this, if an organisation does so, a voluntarily appointed DPO is under the same obligations as a mandatorily appointed DPO.

With the above in mind, many firms that may already have an individual whose day to day work is largely the same as a DPO, may want to consider the increased responsibility of the role, the fact that the DPO reports to the highest management level and must be adequately resourced and further that a DPO is expected to have an expert knowledge of data protection law. Significantly, it is a form of protected employment as the DPO cannot be dismissed or penalised for fulfilling their tasks within the firm. This role needs to be carefully considered before appointing someone.

This article was first published in the February 2018 edition of Accountancy Ireland.

About the Author