LK SHIELDS
YOUR LEGAL COUNSEL

EMPLOYMENT, PENSIONS AND EMPLOYEE BENEFITS

GDPR: Key Steps for Employers

by **Aoife Bradley, Jennifer O'Neill**

GDPR: Key Steps for Employers

2nd May 2018 | by Aoife Bradley, Jennifer O'Neill

The GDPR substantially increases the obligations and responsibilities on organisations and businesses in relation to how they collect, use and protect personal data. Employers should take some key preparatory steps to ensure they are ready when the GDPR has direct effect in Ireland on 25 May 2018 and the Irish Data Protection Bill 2018 becomes law.

Regulation (EU) 2016/679 is known as the General Data Protection Regulation (GDPR).

Data Assessment

Employers should assess the personal data which they hold on their employees and establish why they are keeping it. For example, employee personnel files may contain application forms, details of next of kin, sickness reports, appraisal forms, etc. Employers should review all of these documents and determine what they are holding, why they are holding it and for how long they can lawfully retain these documents. If there is a significant amount of personal data held which is no longer necessary, a data purging exercise will be required with the aim of minimising the amount of data held.

Many companies are also updating their data retention policies (or creating one where they have not previously had such a policy) as part of their GDPR preparedness programmes.

Basis for Processing Employee Data

In order to process employee personal data employers must have a legal basis to do so. When assessing the personal data held, the legal basis for retaining each category of the data should be identified and recorded.

There are a number of permitted legal bases for processing personal data under GDPR:

- the employee has consented to the processing
- processing is necessary for the performance of a contract to which the employee is party
- processing is necessary for compliance with a legal obligation
- processing is necessary to protect the vital interests of the employee
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the employer
- processing is necessary for the purposes of the legitimate interests of the employer

Consent

In practice many employers have relied on a consent clause in a contract of employment which provides that the employee consents to the retention and processing of their personal data under the contract. Under GDPR, while consent is still a valid basis for processing personal data, to be valid it must be "freely given", which an employee is rarely in a position to give in light of the nature of the employer/employee relationship. Also to be valid, consent must be retractable. As a result of these concerns, consent is often unsuitable as the legal basis for processing employee data. Employers should therefore consider whether any of the other legal bases (outlined above) are suitable as the basis for processing employee personal

data, for example where processing is necessary for the performance of the contract of employment or for the legitimate interests of the employer.

Employers may also hold sensitive personal data relating to employees such as data on medical and health issues. Such data will be regarded as special categories of personal data which can only be processed if specific conditions are met. One such condition particularly relevant for employers which is permitted under the current version of the the Irish Data Protection Bill 2018 is the processing of data concerning health where the processing is necessary and proportionate for the purposes of following a policy of insurance or life insurance, a policy of health or health-related insurance and, an occupational pension. Such processing is also permitted under the 2018 Bill for the assessment of the working capacity of an employee. Employers will need to identify all such data held and establish what legal basis it has to entitle it to process such special category data.

In the event that any HR functions are outsourced, such as occupational health or payroll, which may result in the transfer of employee data to a third party, a detailed agreement will be required between the employer and the third party service provider (this is already the case under current law).

Review Contracts of Employment

Employers should review their contracts of employment and assess any provisions relating to employee data. As consent is no longer a reliable legal basis for processing employee personal data, clauses in contracts of employment whereby employees consent to the processing of their personal data should not necessarily be relied upon as a legal basis for GDPR purposes. Contracts of employment may either be amended to remove references to consent to data processing or employees may be issued with a notice informing them that the employer no longer relies on the consent clause as set out in the contract of employment. Notice of the lawful basis for processing employee personal data will then need to be provided to the employees.

Employees Right to Information

It is a requirement under GDPR that each employee must have specified information provided to him/her regarding the personal data relating to him/her which is collected by the employer. This information must be provided at the time the personal data is obtained, which in the case of most employee data is at the commencement of the employment relationship.

Specific information must be provided, including:

- The identity and contact details of the employer or its representatives.
- The contact details of the data protection officer, where applicable
- The purpose(s) and the legal basis for the processing of the personal data
- The legitimate interest of the employer or third party - where processing is based on this ground
- The recipients of the personal data concerned, if any
- The details of any transfers out of the EEA, the safeguards in place and the means by which they obtain a copy of them
- The period for which the data will be stored or the criteria used to determine that period
- The right to request access to and rectification or erasure of personal data
- Where processing is based on consent, the right to withdraw consent at any time
- The right to lodge a complaint with a supervisory authority
- Whether the provision of personal data is a contractual or statutory requirement and the possible consequences of failure to provide such data

If the employer already has a data protection policy in place, it should be reviewed to ensure that it complies with all of the additional information requirements of the GDPR. This policy should then be brought to the attention of employees.

If no data protection policy is in place which includes the required information, the employer will need to issue a Data Protection / Privacy Notice to employees. This Privacy Notice should contain all of the information required under the GDPR. This should be provided to all new hires on commencement of employment and to existing employees before 25 May 2018. In order to properly comply with the

information requirements, a full data assessment should have been conducted by the employer to identify the data held and the legal basis for processing it.

Data Handling Policy

Employers, as controllers of personal data, are required to implement appropriate technical and organisational measures for the purpose of ensuring that the processing of personal data is carried out in compliance with the GDPR (including the implementation of a data protection policy). Such measures must provide a level of security appropriate to the harm that might result from accidental or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to, the data concerned. In this regard, employers must take all reasonable steps to ensure that their employees and other persons at the place of work are aware of and comply with the relevant measures.

In order to meet this requirement, we recommend that employers prepare a data handling notice/policy specifying how all workers who have access to personal data are expected to handle this data. Employees should be made fully aware of these requirements and receive training on what is required of them. Employees should also fully understand the consequences that will follow in the event of a breach by the employee of the employer's data protection policies, including disciplinary action up to and including dismissal.

Practical Security Measures

Access to HR data should be limited to only those who need the data. Passwords should be standard for HR reports and HR personal data should be encrypted. Increased security measures should be in place to protect any special category of personal data held. It is also advisable that the IT systems used by HR are stress tested regularly.

We recommend that employers should provide employee training on data handling and on the steps to be taken in the event of a data breach. Employers should also identify the personnel responsible for any notification to the data protection commissioner and data subject.

Action Plan

1.	Assess the employee personal data held
2.	Determine the legal basis for holding each category of employee personal data, including sensitive employee data and develop a retention policy
3.	Review contracts of employment and any data protection policy in place
4.	Issue updated data protection policy or privacy notice and data handling notice compliant with GDPR to employees
5.	Ensure appropriate security measures are in place to protect employee personal data

---

For more information, please contact Aoife Bradley or Jennifer O'Neill of our Employment, Pensions & Employee Benefits Group.

About the Authors

Aoife Bradley
Partner

Aoife is Head of Employment, Pensions and Employee Benefits.
T: + 353 1 637 1583 **E:** abradley@lkshields.ie

Jennifer O'Neill
Consultant

Jennifer is an experienced employment law practitioner with considerable expertise advising clients on general employment law compliance issues.
T: + 353 1 637 1527 **E:** joneill@lkshields.ie