Preparing for the GDPR— advice for employers

Ann Bevitt, Partner, and Chris Stack, Associate, Cooley (UK) LLP, explain where employers should focus their compliance attentions over the coming months

The text of the European Union's new data protection framework was published in the Official Journal of the European Union on 4th May 2016. Regulation (EU) 2016/279, commonly referred to as the General Data Protection Regulation ('GDPR') shall apply from 25th May 2018 and will replace current Data Protection Directive 95/46/EC (the 'Directive').

Generally speaking, the structure and concepts in the GDPR will seem familiar to employers. However, the increased obligations on both employers and their service providers, combined with enhanced privacy rights for employees and significantly increased fines, mean employers will need to ensure they fully comply with both the familiar and new requirements in the GDPR.

Primary considerations — scope for national variations

Unlike its Directive predecessor, the GDPR has direct effect in all EU Member States, meaning that there will be no requirement for domestic legislation for its transposition. A common set of rules across the EU should provide greater clarity for businesses which operate in more than one Member State. However, from an employment perspective, the position is not quite that straightforward, because the GDPR gives Member States the right to legislate domestically with regard to many aspects of the employment relationship.

Recital 155 and Article 88(1) of the GDPR state that Member State law or collective agreements may provide for specific rules on the processing of employees' personal data in the employment context. That includes, among other things, when employees' personal data may be processed on the basis of employees' consent, and what is permissible when processing for purposes of recruitment, the performance of the contract of employment, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, rights and benefits related to employment, and termination.

The net result is that employers, whilst getting to grips with the changes brought in by the GDPR, will still need to grapple with different employee data protection regimes in each Member State.

This article highlights what employers need to know about and what they should be doing now to prepare for the GDPR. It does not consider the position if, on 23rd June 2016, the UK votes to leave the EU, in which case the impact of the GDPR in the UK would depend upon its relationship with the EU post-'Brexit'.

Territorial scope of the GDPR

Although the GDPR is European legislation, it will apply to data controllers and processors that are established outside the EU where they offer goods or services to data subjects in the EU or monitor the behaviour of data subjects in the EU.

In practical terms, this means that the GDPR has an extra-EU territorial scope and all businesses which have or want access to the EU market will need to be aware of its impact, as will any company that monitors EU-based employees (which will cover the vast majority of employers with any EU-based employees).

In combination with this, employers need to be aware that the GDPR will also apply to data processors, meaning any entity which processes data on an employer's behalf. Therefore, employers will need to consider what service providers they use for HR purposes, which could include, for example, payroll or HR cloud service providers, and review their contractual terms to ensure they are GDPR compliant, regardless of where the service provider is located.

Consent

It is common for employers to rely on an employee's consent gathered within the employment contract to legitimise the processing of their personal data. Under the GDPR, where consent is freely given, specific, informed and unambiguous, this will constitute one of the six lawful bases for the processing of personal data.

(Continued on page 12)

(Continued from page 11)

However, the GDPR sets out conditions for consent to be valid which are more onerous than those under the Directive. These include that the consent opt-in must be presented in clear and plain language in a manner which is distinguishable from other matters, and that there must be a right to withdraw consent.

When considering whether consent has been freely given, account will be taken of whether the provision of consent was an unnecessary condition of the performance of a contract.

Employers will still be able to rely on employees' consent in order to process their personal data. However, that consent will need to be distinct from the employment contract and comply with the GDPR conditions for validity; there will need to be a genuine choice from the employee to agree to their data being processed.

Moreover, the processing of 'special categories of personal data', being data which relates, for example, to racial or ethnic origin, religious or philosophical beliefs, health or sexual orientation (in other words, 'sensitive personal data'), requires 'explicit consent'. This means that consent needs to be especially clear and detailed.

It would therefore be prudent for employers to review the method by which they currently obtain their employees' consent and amend it in line with the GDPR requirements to reduce the compliance burden in May 2018. Employers should also be aware that obtaining a generic consent for all processing is unlikely to be effective and they may therefore need to obtain a number of consents from their employees.

"Employers will still be able to rely on employees' consent in order to process their personal data. However, that consent will need to be distinct from the employment contract and comply with the GDPR conditions for validity; there will need to be a genuine choice from the employee to agree to their data being processed."

Processing on the basis of 'legitimate interests'

The GDRP will permit employers to process employees' personal data where processing is necessary for the legitimate interests of the employer. That is a lawful basis for processing which employers should continue to rely on, particularly in circumstances where employees could easily withdraw their consent at any time.

However, it will be necessary for the employer to explain what 'legitimate interests' it is pursuing in processing employee data, which will require some assessment and rationalisation. For example, employers will need to evaluate and explain why employee monitoring is necessary, and employers' interests will not automatically trump those of employees. Consequently, employers may also want to rely on 'necessity' for the performance of the employment contract or compliance with a legal obligation as alternative bases for the lawful processing of employees' personal data.

Transparency and information

The GDPR places greater emphasis on transparency and the provision of information to data subjects.

For employers, this means that they will need to ensure that they provide employees with the following:

- details of the legal bases for processing;
- who will receive their personal data (or the categories of recipients);
- the data retention period (or the criteria used to determine that period);
- their rights as data subjects (which include the right to request their data, and have it rectified or erased);
- their right to withdraw consent at any time; and
- the right to complain to the applicable regulator.

All of this information will need to be provided in clear and plain language, in a concise, transparent, intelligible and easily accessible form. Employers will therefore need to ensure that they have a sufficient, comprehensive and understandable data protection policy in place which provides the requisite information.

Data subject access requests

This subject access right remains in the GDPR, although the 40 day deadline for responding (in the UK) is replaced with an obligation to respond 'without undue delay and in any event within one month' of the request. There is a possibility of a further two month extension where the complexity of the request warrants it.

The data subject access response will need to be provided without any fee charge, save that it will be possible to charge a 'reasonable fee' or to refuse to act where a request is manifestly unfounded or excessive.

Employers can expect little change in the nature, frequency or scope of employees' data subject access requests. However, they should be aware that, in addition to copies of the requested data, employees will also be entitled to additional information including the purpose of the data

processing, the recipients to whom the data have been disclosed and the period for which the data will be stored.

Rectification, erasure and restriction of processing

In addition to data subject access request rights, the GDPR will entitle employees to have inaccurate data rectified, to have personal data concerning them erased without undue delay (commonly referred to as the right to be forgotten), to restrict the processing of their personal data or to object to its processing altogether.

These rights are conditional upon satisfaction of an applicable basis for exerting the right. For example, in order for an employee to have the right for personal data to be erased, it must no longer be necessary for the purpose for which it was collected. In other words, the right to be forgotten is not absolute, so its impact on employers is likely to be limited provided that the latter has the correct policies and procedures in place. Nevertheless, employees will have enhanced rights in their hands and, as with subject access requests, it is likely they will use them in the context of an employment dispute.

The key for employers will be to ensure that they have documented, legitimate and lawful grounds for processing an employee's personal data and that such data are accurate, up-to-date and kept for no longer than necessary. Employers should also be aware that where employees exert their rights in a way which the employer can demonstrate to be manifestly unfounded or excessive, particularly because they are repetitive in nature, then they will be able to charge a reasonable fee or may be able to refuse to act on the request.

Do you need a Data Protection Officer?

It will be necessary to designate a Data Protection Officer where the 'core activities' of the data controller or processor consist of 'processing operations which…require regular and systematic monitoring of data subjects on a large scale' or the processing of sensitive personal data on a large scale. All public authorities or bodies will also need to appoint one.

Broadly speaking, employers who operate in the big data arena or provide certain cloud services are likely to need to appoint a Data Protection Officer. That individual will need to be appointed on the basis of professional credentials and expert knowledge of data protection law.

What happens when there's a personal data breach?

Employers are at risk of personal data breach from a number of different sources ranging from an external cyber-attack which breaches security through to the employee who accidentally leaves a file containing personal data in a coffee shop.

Pursuant to the GDPR, the regulator will have to be notified of a personal data breach without undue delay and, in any event, within 72 hours (unless you can explain the reason for the delay). That notification will need to describe the nature of the personal data breach, the likely consequences of the breach, the measures taken to address the breach and the details of a contact point where more information can be obtained (which will be the Data Protection Officer, if there is one). If the data breach affects employees, then they will also need to be notified without undue delay, which may adversely impact employee relations.

Employers will also need to ensure that they document and record the facts and effects of any personal data breaches together with any remedial action taken. So it will be crucial for employers to have a notification procedure in place together with a system for satisfactorily recording data breaches.

The potential cost of violation

Failure to comply with certain provisions of the GDPR, such as the lawful data processing principles or data subjects' rights, can result in a fine of up to €20 million or 4% of an undertaking's total worldwide annual turnover. There is, therefore, the potential for a significant penalty for a failure to comply with the GDPR, particularly when compared with the current maximum fine in the UK of £500,000.

However, the reality is that the largest fine ever issued by the UK regulator was £350,000 and there is no reason to suggest that it is likely to immediately and materially change its approach when it has the authority to impose higher fines at its disposal.

Nevertheless, the Information Commissioner's Office will not be acting in isolation and may come under pressure from other Member States' data protection authorities to act collaboratively in imposing larger monetary sanctions.

Conclusion

Employers have plenty of time to ensure compliance before the GDPR comes into force on 25th May 2018. However, they should start now to ensure a smooth transition to the new regime. Employers should begin by conducting an audit of their current employee data processing policies, HR processes and HR service providers against the GDPR's requirements. Where inadequacies are identified, they should be rectified and the documentation updated, as that will be fundamental to demonstrating compliance with the GDPR.

Ann Bevitt and Chris Stack
Cooley (UK) LLP
abevitt@cooley.com
cstack@cooley.com