EU General Data Protection Regulation: implications for employers

by ***Steven Lorber***, Lewis Silkin LLP

Practice notes | **Maintained** | European Union, UK, United Kingdom

A note on the General Data Protection Regulation, which will apply from 25 May 2018, and how it is likely to affect employers in the UK.

Note: UK data protection law will change on 25 May 2018, when the new EU General Data Protection Regulation takes effect. We are updating all our maintained resources between now and 25 May 2018. See *Provisional publishing schedule: Employment* for more information.

Scope of this note

This note provides an overview of the implications for employers of the *General Data Protection Regulation* (GDPR). It briefly explains the background to the changes, the likely timing of the implementation and those aspects likely to have most impact. The note also addresses the rights of data subjects and the duties of data controllers, and considers appropriate next steps for employers.

Unless the context indicates otherwise, references to an employer or to an employee are to the employer as data controller and to the employee as data subject.

Revised EU data protection regime: introduction

After a four-year gestation period, the text of the *GDPR* was formally adopted in April 2016 (see *Legal update, EU Parliament approves data protection reform package*). The text has been translated into the EU's official languages and published in the Official Journal of the European Union. It will apply in all member states from 25 May 2018, two years from its entry into force on 24 May 2016 (see *Legal update, EU Parliament approves data protection reform package*). The UK government has confirmed that the UK will be implementing the General Data Protection Regulation in May 2018 (see *Legal update, Government confirms UK will opt in to GDPR in May 2018*). It has announced that the Data Protection Act 1998 will be replaced by a new Data Protection Bill, yet to be published (see *Legal update, Queen's Speech 2017: data protection implications*).

One-stop shop

The European Commission's strategy was to establish a "one-stop shop" for data protection, with a common set of rules applying across the EU. It sought to achieve this using the tool of an *EU regulation*. Unlike an EU directive, a regulation has *direct effect* and becomes part of the law of each member state without the need for implementing legislation. Although the GDPR will have direct effect and apply throughout the EU, member states are given power to legislate domestically in a few areas, one of which is employment. Member states may establish "more specific rules to ensure the protection of ... rights and freedoms in respect of the processing of employees' personal data".

It is not clear to what extent states will take advantage of the power to make domestic rules on employment. However, exercise of the power in an area that is likely to affect every business has the potential to undermine the one-stop shop strategy. This is because employers will need to check the legal position in each member state in which they operate. The European Commission has claimed that these changes will save businesses EUR2.3 billion a year. Some commentators have challenged that figure and expect compliance to increase the burden on business rather than yield savings (see *EurActiv: EU's General Data Regulation could be costly for businesses*). Whatever the correct analysis, the combination of expanded privacy notices and increased policy documentation coupled with the potential for variation between member states mean that significant savings are unlikely in the context of employment.

Tougher enforcement

The rules in the GDPR are underpinned by a tougher penalty regime. The maximum penalty for non-compliance is EUR20 million or, if it would be higher, 4% of an undertaking's worldwide turnover, compared to the current maximum penalty in the UK of £500,000. Although this does not necessarily mean higher penalties in practice, this change is likely to lead to a greater focus on compliance. In the UK, the *Information Commissioner* has a reputation for a more pragmatic and proportionate approach to enforcement than regulators in some other member states. As the GDPR puts great emphasis on collaboration between regulators and consistency, it is not clear whether the UK's distinctive approach will be maintained. In addition, where a business operates in more than one member state, its lead regulator will be in the state in which its main establishment is based. Although an issue may arise in the UK, the relevant regulator may be based in a different state, particularly if the issue has a cross-border aspect.

Employment data

Data protection legislation bites on all areas in which a business processes personal data, including data relating to customers, suppliers and website users. However, the implications for data relating to employees are particularly significant, for the following reasons:

- Businesses are likely to process significantly more data in relation to employees than in other contexts. Data processed on office workers might include:
    - CCTV film on their arrival at work;
    - lift or floor access information;
    - data on computer log on; and
    - data on websites visited, phone calls made and emails sent or received.

  Personal data relating to customers or suppliers is likely to be much less extensive.
- Much employment data is likely to be unstructured. This creates particular challenges for an employer seeking to comply with principles relating to data minimisation and storage limitation or in handling a data subject access request. The text of an email may contain personal data about the sender, the recipient or a third party. Some of that data may be sensitive personal data, or even sensitive personal data about a child (for example "Sorry, can't make the meeting, my daughter has chickenpox"). Although the employer is a data controller, it exercises little or no control over unstructured data such as this. By way of contrast, although a credit card company, internet service provider or search engine provider will collect significant personal data, most of this will be held in a pre-defined structured format.

- Although a dispute can arise with a customer or supplier, a dispute with an employee is more likely to be personalised, intense and engage personal data.

General Data Protection Regulation: overview

The approach of the GDPR is similar to that of the *Data Protection Directive* (*95/46/EC*). Using core concepts (*Article 4*) (for example "personal data", "processing", "controller" and "processor"), the GDPR requires data controllers to comply with a set of principles for processing personal data. A data controller must ensure that it can meet at least one of a number of gateway conditions providing the legal basis for processing. In doing so, it must give data subjects information on its purposes. Data subjects have a range of rights, including in particular a subject access right.

Although its general approach will be familiar to those advising on data protection, the GDPR will lead to a greater focus on data protection in practice. Compliance will require:

- More granularity.
- Greater focus on the legal basis for processing.
- More extensive information and policies.
- Extended rights for data subjects.

All this is backed up by greater potential penalties.

Transparency

Under the Data Protection Directive, data must be processed fairly and lawfully. Article 5.1 of the GDPR adds the concept of "transparency" which, in an employment context, this translates to openness and explanation. For example, when responding to a subject access request, employers will, if asked, need to explain how they have approached it.

Consent

The giving of consent by a data subject is one of the gateways through which a controller can establish a legal basis for processing personal data. In the early days of data protection, many employers used consent as a legal basis for processing through the vehicle of the employment contract. However, regulators disapprove of the use of consent in most contexts (see *Europa: Article 29 Data Protection Working Party: Opinion 15/2011 on the definition of consent (13 July 2011)*).

The GDPR sets out stricter and more detailed conditions for the use of consent:

- Consent must be freely given, specific, informed and unambiguous. It will not be considered freely given if there is no genuine free choice. At present, many employers obtain consent for processing personal data by the use of standard provisions in their employment contracts. In general, employment contracts are offered on a "take it or leave it" basis, under which an employee has no real choice. This means the consent obtained in the contract is unlikely to be effective.

- The onus is on the employer to show that the employee gave consent.
- If consent is given by means of a written declaration, the request must be made in a manner that is clearly distinguishable from other aspects of the document. If consent is incorporated in an employment contract, the employer must use a separate signature box.
- An employee has the right to withdraw consent at any time and must be told of this right by the employer. It must be as easy to withdraw consent as it is to give it.

(*Article 7.*)

Although the use of consent may have its place in a one-off context, such as consent to an employer sending health information to a specialist, in general its use in an employment context will be impracticable and risks being ineffective.

Employers should consider other grounds on which to justify processing (relying, for example, on their "legitimate interests" (*Article 6.1(f)*) or that processing is necessary for the performance of a contract to which the data subject is party (*Article 6.1(b)*)).

In light of the GDPR, the ICO has issued draft *guidance on consent* which is expected to be published in final form in late summer 2017 following a consultation.

Information on data

Under the existing law, employers are required to provide job applicants and employees with a privacy notice (sometimes called "fair processing information") setting out the purposes for which data is processed, together with any further information needed to ensure processing is fair.

Under the GDPR, all information provided must be concise, transparent, easily accessible and given in plain language (*Article 12*). In addition to the information provided under the current rules, employers must provide information on the legal basis for processing. This will involve a careful analysis of the data processed and the available legal bases. Some of the data may be sensitive (for example health, union or diversity data). If data is sensitive, an employer will need to specify which of the conditions for processing sensitive data it is relying on, in addition to providing details of the general basis for processing that data.

In an employment context, the processing basis relied on most commonly is the "legitimate interest" condition, that processing is necessary for the purposes of the legitimate interests of the employer or a third party except where those interests are overridden by the interests, rights and freedoms of the employee. If this is relied on, the employee must be told what the employer's or third party's "legitimate interests" are.

In addition, employers will need to explain:

- The source of the data (unless it originates from the data subject).
- Who will receive personal data (or the categories of recipients).
- The period for which data will be stored, or if that is not possible the criteria used to determine the period.
- The existence of data subject rights including subject access, rectification and erasure.

- The right to object to processing on grounds related to an employee's "particular situation" (*Article 21.1*), which applies if an employer relies on the "legitimate interest" condition.
- The right to withdraw consent, if the employer is relying on consent as a legal basis.
- The right to complain to the regulator.
- The legal basis for the transfer of the data to a non-EU third country (where this is to take place) and, if the employer relies on standard contractual clauses, on the safe harbor or on binding corporate rules, information on the safeguards applied and on how the employee can obtain a copy.

Employers will need to provide significantly more information than at present. There is a tension between the level of detail required and the obligation to provide information concisely, accessibly and in plain language.

Data subjects rights

The GDPR extends data subjects' existing rights and makes them more explicit. In addition to the data subject access right, there is a package of rights that may be summarised as "delete it, freeze it, correct it" (*Articles 12 and 15-21*). This package includes the following:

- The right to erasure or to be forgotten.
- The right to rectification.
- The right to restriction of processing.
- The right to object to processing.

With the exception of data subject access rights, these rights are rarely asserted in an employment context. However, there is increased focus on the right to be forgotten following *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12) [2014] QB 1022* (see *Legal update, ECJ confirms right to have search engine results removed where they affect privacy rights*). When this is combined with the revised penalty regime and stricter enforcement within the one-stop shop, it may well lead to employee data subject rights having greater significance, if only as leverage in an employment dispute.

Data subject access rights

The data subject access right (DSAR) in Article 15 of the GDPR is broadly similar to the right under the existing rules. However, the employer will be required to provide the following information in addition to the information that it currently needs to provide:

- The envisaged period of storage.
- Details of the "delete it, freeze it, correct it" rights.
- The safeguards applied on a third country transfer of data.

The current default period for compliance of 40 days will be replaced with an obligation to comply without undue delay and within one month, with an extension of two additional months if necessary, taking into account the complexity of the request. Given the complexity of most DSARs in an employment context, it seems likely that the normal period for compliance will be up to three months.

The £10 fee applicable to requests under the Data Protection Act 1998 will be abolished. However, where a request is "manifestly unfounded or excessive" the employer may either charge a "reasonable" fee, taking into account administrative costs, or may refuse to act on the request altogether. This is a significant change. What is "manifestly excessive" will depend on the specific circumstances, but it is likely to discourage onerous requests. In many contexts, a person making a DSAR may not appreciate the scale of the work involved in responding to a request. Where requests are substantial, the revised rules should lead to a dialogue between employer and employee. This should lead to an agreement on what the employee wants and how to handle the request, with the fallback of the regulator if either side is being unreasonable. If nothing else, the rule should inhibit requests encompassing thousands of emails requiring days of work from a team of people.

"Delete it, freeze it, correct it!"

As well as DSAR, an employee has a package of rights including:

- The right to erasure (to be forgotten) (*Article 17*).
- The right to rectification (*Article 16*).
- The right to restriction of processing (*Article 18*).
- The right to object to processing (*Article 21*).

The circumstances in which these rights can be exercised vary, but as a generality they are triggered if there is non-compliance with data protection principles.

The right of erasure may be exercised where any of the following apply:

- The processing of data is no longer necessary in relation to the purposes for which it was collected or processed.
- Data has been unlawfully processed.
- The data subject objects and the employer cannot show "overriding legitimate grounds" for continuing in circumstances where the processing is based on the "legitimate interest" condition.

The right to rectification arises where data is inaccurate or incomplete.

The right to restriction of processing (freezing) arises where:

- Processing is unlawful.
- Data accuracy is contested by a data subject.
- A data subject has objected to processing based on the "legitimate interest" condition pending a decision as to whether or not the employer has compelling legitimate grounds which override the rights of the employee.

(*Articles 18 and 21.1.*)

These rights may be used in employment disputes in various ways:

- Many, perhaps most, emails are no longer necessary for the purposes for which they were processed. An email inviting an employee to a meeting or the response declining the invitation is ephemeral, but may still be

personal data. Although there is no reason to keep the email, few will spend the time necessary to review it and decide on deletion.

- If privacy notices are defective or reliance has been placed on ineffective consent, processing may be unlawful.
- An employee faced with a disciplinary allegation based on a covert investigation may seek to freeze processing of data on the basis that his or her right to privacy trumps the employer's "legitimate interests".

The "manifestly unfounded or excessive" rules referred to in relation to DSARs also apply in relation to these rights. If "delete it, freeze it, correct it" requests are clearly excessive, the employer may refuse to act on the request or charge a fee.

Controllers' duties

Demonstrating compliance
As data controller, the employer has a duty to comply with data protection principles. But the GDPR also requires it to be able to demonstrate compliance (*Article 24.1*). In principle, a regulator (and perhaps even an employee) may require the employer to implement technical and organisational measures and to show that it complies. It will not be sufficient to say "but we are not in breach"; compliance must be demonstrated.

Where proportionate, the GDPR requires implementation of data protection policies, which is an organisational or technical measure. This is likely to be lead to a proliferation of policies. If challenged, an employer will say that it has a policy with which it complies.

Data protection by design and by default
Employers will be expected to take steps to build data protection into system design (*Article 25*). Subject to what is technically practicable and cost, they will need to build in safeguards to comply with the rules. Measures must be taken to minimise data collected, ensuring it is necessary for the specific purpose for which it was obtained. Where an employer is contemplating a new HR system, it would be advisable to consider to what extent data protection can be built into the design.

Data processors

Employers typically use data processors in a number of contexts, including banking, payroll and as a provider of cloud services. The GDPR tightens the rules on the use of data processors, extending the formal contractual requirements needed between data controllers and processors (*Article 28*). The processor may only process personal data if it has documented instructions from the data controller. It must ensure data security. It will have an obligation to demonstrate compliance to the controller and to permit inspection and audit.

Currently, only data controllers have liability to data subjects for compliance. Under the revised rules, data processors will have a duty to comply and potential liability if they fail.

Processors will seek to limit their risks by wanting greater clarity on their responsibilities. In light of this, engaging a processor for anything more than a simple task is likely to become more complex. Many processors will need to appoint a data protection officer, which will itself lead to greater focus on compliance.

Data protection officers

The main roles of a data protection officer (DPO) are to:

- Advise data controllers or (as the case may be) data processors of their legal obligations.
- Monitor compliance with the GDPR and with data policies and related training.
- Be a point of contact for the regulator

(*Articles 37* - 39.)

A DPO will be independent, with a position in some ways analogous to an auditor. DPOs may be employees, contractors or consultants.

Although some employers will appoint DPOs voluntarily, there is only a requirement for a controller to have a DPO if its core activities involve systematic monitoring or large-scale processing of sensitive data (for example, health data or criminal records) or if it is a public body. Although employers hold sensitive data, particularly in relation to health, it is unlikely that processing will be sufficiently large-scale for appointment of a DPO to be mandatory.

Public authorities (such as local authorities, health trusts and government departments) and public bodies (such as non-departmental public bodies and many social landlords) will be required to appoint a DPO. Processors will also be required to appoint a DPO if processing is carried out by them on behalf of a public authority or body. Many processors including outsourced service providers, payroll agents and providers of cloud services will be operating in a market that includes public authorities and bodies. They will need to appoint a DPO.

At its December 2016 plenary meeting, the Article 29 Working Party adopted guidelines on DPOs (see *Guidelines (WP243)* and *FAQs*). Following the receipt of comments, the Working Party plans to adopt amended versions of these guidelines in April 2017 at the latest (see *Legal update, Article 29 Working Party provides update on GDPR implementation guidance, Privacy Shield and enforcement matters*).

Personal data breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of personal data (*Article 33*). Employees make mistakes; they leave laptops on trains, send emails to the wrong person and are careless with passwords. These are all personal data breaches.

Under the revised rules, employers discovering a personal data breach must notify the regulator promptly and within 72 hours, if feasible. If the notification is not made within this time, the employer must provide a "reasoned justification" explaining the delay. The notification requirement does not apply if the breach is unlikely to result in a risk to data subjects (for example, because all data on a laptop was encrypted).

In notifying a breach, an employer must describe what happened and set out the approximate numbers of individuals affected, the likely consequences and the measures taken or proposed. If there is a high risk to a data subject, he or she must be told.

Records must be kept of all data breaches and action taken, including those in respect of which there was no obligation to notify the regulator.

Data breaches can occur at any time and are not uncommon. For example, most businesses lose laptops and memory sticks from time to time. Some emails go to the wrong recipient. Although not all such breaches are serious in their impact or need to be notified, the three-day time frame means that employers will need to have clear policies on how they handle a breach, with defined roles fulfilled by individuals who understand what they are doing.

What should employers do now?

The revised rules will not apply until the summer of 2018 and the outcome of the referendum in June 2016 means that there will be a number of changes before then. In a speech, the Data Protection Minister, Baroness Neville-Rolfe DBE CMG, explained that if the UK remains within the Single Market, EU rules on personal data might continue to apply fully in the UK, but in other scenarios, all EU rules might be replaced with national ones. However, if any country wishes to share data with EU Member States, or handle EU citizens' data, it will need to provide an adequate level of data protection. See *Legal update, DCMS view on Brexit, the GDPR and EU-US Privacy Shield.*

The ICO states, in its *Overview of the EU's General Data Protection Regulation*

"The result of the 23 June 2016 referendum on membership of the EU now means that the Government needs to consider the impact on the GDPR.

However, we still think it will be useful to publish this overview. This is because once implemented in the EU, the GDPR will be relevant for many organisations in the UK – most obviously those operating internationally. The other main reason is that the GDPR has several new features – for example breach notification and data portability. Therefore we thought it would still be useful to familiarise information rights professionals with the GDPR's main principles and concepts.

With so many businesses and services operating across borders, international consistency around data protection laws and rights is crucial both to businesses and organisations, and to consumers and citizens. The ICO's role has always involved working closely with regulators in other countries, and that will continue to be the case. Having clear laws with safeguards in place is more important than ever given the growing digital economy, and we will be speaking to government to explain our view that reform of UK data protection law remains necessary."

Therefore, although there is no specific or pressing need to take action now, employers may still want to take steps to in light of the GDPR.

At a high level, organisations seeking to be compliant need to embrace a culture of taking data protection responsibilities seriously. The possibility of penalties of EUR20 million or more if the UK does have to comply with the GDPR may well focus minds at board level.

Steps required may include:

- Identifying all existing data systems and the personal data processed. Consider setting up an information asset register. Understand the legal basis for processing the data and identify what will need to change to comply with the revised regime.

- Ensuring the resources to prepare for change have been allocated. Identify who takes overall responsibility and ensure that they have the time and support to plan for the reforms.
- Considering appointing a DPO, and whether appointment would be mandatory.
- Reviewing privacy notices and other fair-processing information given to employees (and job applicants). Consider what additional information will need to be included. For example, what "legitimate interests" underpin processing? How long will data be stored?
- Assessing whether the business uses consent to justify processing. Consider relying on other routes such as the "legitimate interests" ground or that processing is necessary for performance of the employment contract.
- Reviewing contracts of employment, handbooks and policies to see whether and how they deal with data protection (and in particular, whether contractual "consent" is sought).
- Establishing a policy (with a timeline) for handling data breaches. Obtain a full picture of exposure to potential data breaches by ensuring that breaches and loss are reported to whoever is responsible.
- Training staff on data protection responsibilities and how they are affected in their job.
- Developing and implementing a policy on retention and storage of data, including emails.

Employers should watch the *ICO website* for any guidance on how to prepare for the changes. The ICO has published details of what guidance on the GDPR it will be producing, and when (see *Legal update, ICO publishes priorities on GDPR*). It has also published its *Overview of the EU's General Data Protection Regulation*.

This note provides a brief summary of a complex piece of legislation. There are many further aspects which will apply in certain contexts. These include rules on transfers outside the EU and a duty to carry out data protection impact assessments.

END OF DOCUMENT

