What do employers in the UK need to know about the new General Data Protection Regulation (GDPR) from an employment perspective?

Introduction

In an employment context “data protection” is usually seen as confusing and low risk and, much to the annoyance of the busy manager or HR Professional, data protection issues are often most encountered when an employee is threatening litigation and makes a subject data access request (“SAR”). The GDPR, which will apply in EU Member States from 25 May 2018, is one of the most significant developments in EU data protection law in the last few decades. Although there are few dramatic changes in the GDPR from an employment law perspective, there are some changes with which employers should familiarise themselves, not least because a breach of the GDPR will lead to much more severe penalties than the current data protection regime, including fines of up to 20,000,000 euros or 4% of its annual worldwide turnover, whichever is greater.

In the UK, the GDPR will apply between 25 May 2018 and Brexit and most likely post Brexit (see our briefing Brexit and Data Protection: business as usual). The obligations on employers will have immediate impact when the new rules apply in May 2018 so now is the time to start thinking about how to implement the changes. We set out below the key changes from an employment law perspective.

Changes to SARs under the GDPR

The word “subject access request” will often fill an employer with dread; they can be time consuming, costly, confusing and too often a mechanism to add nuisance to litigation or to undertake a fishing expedition prior to litigation or before legal disclosure. SARs are unlikely to become easier to deal with under the GDPR and the process itself will remain the same. The current fee of £10 will no longer be chargeable although when a request is “manifestly unfounded or excessive, in particular because of its repetitive character”, employers under the GDPR will be able to charge “a reasonable fee” taking into account the administrative costs of providing the information. The potential to charge a reasonable fee in these circumstances may discourage employees from making excessively wide SARs or from making SARs which employers consider to be ‘fishing expeditions’. However, unless guidance is provided on what “manifestly unfounded” or “excessive” means in practice, employers may be reluctant to use this power.

The current statutory timeframe of 40 days to comply with a request will be abolished and replaced with an obligation on employers to comply “without undue delay” and at the latest within one month of the request. The removal of the 40 day period is likely to make an employer’s duty to comply more onerous and employers will need to ensure that policies and procedures are updated, staffing requirements are reviewed and staff are adequately trained to ensure compliance with the new timeframes. However, if the request is particularly complex or if there are numerous requests, then the timescale can be extended by up to two further months. An employer wishing to benefit from such an extension will be required to notify the individual of the extension within one month of the receipt of the SAR, including the reasons for the delay. This additional period of time may provide some welcome breathing space for employers.
Consent

Under the Data Protection Act 1998 (“DPA”)

Consent is one of the conditions allowing the processing of personal data. In an employment relationship where the balance of power could be unequal, there is often a question as to whether an employee can truly consent. The Information Commissioner’s Office (ICO) has stated that “the extent to which consent can be relied upon in the context of employment is limited”. The DPA does not define “consent”, but the European Data Protection Directive (the “Directive”) to which the DPA gives effect, states that consent must be “unambiguous” (Article 7), “specific and informed” (Article 2), and “freely given” (Article 2).

If an employer wishes to process sensitive personal data, such as medical records, the employee’s consent to the processing of this data is required to be “explicit”.

Under the GDPR

Freely given consent

The GDPR has adopted the wording in the Directive and consent must be “freely given, specific, informed and unambiguous”.

The extent to which consent can be relied upon in the employment context to justify the processing of personal data is already doubtful under the DPA regime, as reflected in both the ICO’s and the Article 29 Working Party’s guidance. Unsurprisingly, this position will remain the same under the GDPR: consent will be invalid where there is a “clear imbalance between the data subject and the controller”.

Whether there is such an “imbalance” will depend on the circumstances. For instance, it is clear that if there is any threat of disciplinary action or other detriment for refusing to consent then the consent will not be valid. However, a senior employee may be less likely to feel “forced” to consent to the processing of personal data compared to a junior employee, who may feel he has no choice but to consent, and so it may be that in this circumstance the consent is valid.

Blanket consents

Although Part 4 of the ICO’s Employment Practices Code of Practice (the Code) discourages the use of blanket consents (“blanket consent obtained at the outset of employment, cannot always be relied upon”), it has been common practice to include blanket consents in employment contracts and policies. The wording of the Code itself entertains the possibility that in some circumstances a blanket consent may be acceptable.

The GDPR states that “if a data subject’s consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language”. This means that if consent is written as part of an employment contract, it may not be “clearly distinguishable from other matters” and a blanket consent is unlikely to comply.

The recitals to the GDPR further clarify that consent will be presumed not to be freely given if it does not allow for separate consent to be given to different processing operations or if the performance of a contract is dependent on the consent (despite the consent not being necessary for such performance). For example, if an employer attempts to obtain consent in an employment contract to use employee’s personal data to operate a world-wide centralised employee

---

1 ICO Employment Practices Code.
2 The Article 29 Working Party is composed of representatives of the national data protection authorities, the European Data Protection Supervisor and the European Commission. It will become the European Data Protection Board under the GDPR.
database, there is an argument that this consent is unlikely to be freely given because an employee may well feel obliged to sign that employment contract and feel that the offer of employment is dependent on him signing that contract even though the performance of the contract is not dependent on the consent. It is therefore doubtful that consent obtained by standard data protection clauses in contracts of employment and policies will meet the new definition under the GDPR because it is unlikely to be specific enough or freely given.

Withdrawal of consent

The GDPR also states that consent may be withdrawn at any time and it must be as easy for an individual to withdraw consent as it is to give it. Employers are likely to need to review how employees can withdraw consent and consider how they will inform employees of this right.

Approach going forward

The Code is simply a recommendation for dealing with employee data which reflects the ICO’s opinion as to how the DPA may be complied with. It has no legal effect and compliance with its recommendations is not mandatory. We expect that the Code will be amended in due course to reflect the more positive action required under the GDPR.

Consents obtained prior to 25 May 2018 will not be valid from that date if they do not meet the GDPR requirements, so employers may need to update their contracts of employment and other policies, for example to ensure that they do not contain blanket or “conditional” consents.

In any event, given the difficulties of consent in an employment context, processing by employers may, in general, be better carried out under a different ground rather than by consent. For example, relying on one of the grounds for where the processing of personal data is necessary for the performance of the employment contract, to comply with a legal obligation to which the employer is subject or for the purposes of the employer’s legitimate interests.

For further details on the GDPR requirements for consent, please see our briefing Processing of personal data: consent and legitimate interests.
Information to be provided by the employer to the employee or prospective employee when data is collected

The processing of an employee’s personal data should be preceded by a robust notice of data processing which employers must distribute to each individual when personal data is first collected. This will continue to be a requirement in many cases under the GDPR, for instance, the GDPR will continue to require employers to give notice at a very early stage to job applicants, and not just new hires, if personal data is to be collected. The basic notification requirements will remain the same under the GDPR but the notice itself will need to include significantly more information than under the DPA.

All information provided must be concise, transparent, easily accessible and given in plain language. In an employment context employers often rely on the “legitimate interest” condition to allow them to process data i.e. that processing is necessary for the purposes of the legitimate interest of the employer or a third party. If employers rely on “legitimate interest” then they will need to explain what that legitimate interest is and, if the processing is based on consent, the right to withdraw that consent.

In addition, the information must include (i) the identity and contact details of the employer; (ii) the categories of recipients of disclosure of personal data; (iii) that the employer intends to transfer personal data to a third country and the legal basis for the transfer; (iv) the period for which the personal data will be stored or the criteria for determining the period; (v) how employees can exercise the rights of access, correction, erasure and objection; (vi) the right to file a complaint with the data protection authority; (vii) whether the employee is obliged to provide the data by statute, contract, or for another reason, and the possible consequences of failing to provide the data; and (viii) whether the personal data will be subject to any automated processing and, if so, the logic and consequences of the processing for the employee. Regard should also be had to the ICO’s recently published updated guidance on privacy notices under both the DPA and the GDPR.

Privacy notices should be kept under review as an employer’s need to process data may change over time. This will enable the employer to maintain some flexibility as to proposed data uses, whilst continuing to comply with the GDPR.

The right to be forgotten

The GDPR has introduced an enhanced right to “erasure”, giving employees, as with all other individuals, the right to require an employer to delete their personal data when: (i) the data is no longer necessary for the purposes for which it was collected; (ii) they withdraw consent to processing and the employer has no other ground for processing data; or (iii) they object to processing and there is no compelling ground that overrides their interests. There will also be an obligation for employers to take reasonable steps to inform third parties that the individual has requested the erasure of any links to, or copies of, personal data. Employers are not required to erase employee data that they are required to retain under EU or Member State Law that is necessary to establish, pursue, or defend legal claims.

The right to data portability

The GDPR also gives individuals the right to receive personal data concerning them in a structured, commonly-used and machine readable form and have the right to transmit those data to another controller without hindrance. This right will apply when the processing is based on consent, explicit consent or performance of a contract or where the processing is carried out by automated means. This may be relevant to employers, in particular when employees leave the company.
The Article 29 Working Party has already considered the concept of data portability in discussions and has promised guidance on this topic before the end of the year. However, there is as yet no guidance about how to erase employee data and how far employers have to go to search for data over and above that contained in the employee’s personal file, nor is there guidance on how far an employer has to go to inform third parties. As this is likely to be difficult both technically and administratively, it is hoped that the Article 29 Working Party will produce guidance during the course of 2017, if not before. The ICO has already produced some guidance on both topics, which is available on its website.

**Demonstrating compliance**

Although there is a duty under the DPA for an employer to comply with data protection principles, under the GDPR an employer will have to be able to demonstrate this compliance. In practice, this is likely to mean that, at a minimum, an employer will need to have one or more data protection policies in place that demonstrate that the processing of personal data is performed in compliance with the GDPR. The employer should be able to show that it has implemented the policy, for example through staff training, audits and other similar checks.

**Breach notification**

There is no requirement under the DPA for an organisation to report a data breach to the regulators unless it is a telecoms provider or internet service provider under the Privacy and Electronic Communications Regulations 2003. However, the ICO’s guidance recommends that serious breaches of the DPA be reported to it regardless of the sector in which the relevant entity operates.

Under the GDPR employers who are aware of a personal data breach must notify the regulator without undue delay and, where feasible, within 72 hours of becoming aware of the breach. There is no notification requirement if the breach is unlikely to result in a risk to employees. If notification is required, the employer must explain to the regulator what happened and set out the potential number of individuals affected, the likely consequences and the measures taken or proposed. If the breach is likely to pose a ‘high risk’ to an employee’s rights and freedoms then they must also be notified.

The Netherlands brought in equivalent breach notification rules at the start of 2016 and so are effectively front running these new GDPR requirements. From the experience of companies subject to those rules, it appears that this will be a large administrative burden with the Dutch regulator setting a low threshold as to what needs to be notified.

Employers will need to put policies and processes in place to ensure that data breaches are responded to and that the GDPR timescales are met. Records also need to be kept of all breaches including those where there was no obligation to notify the regulator. It is easy for employees to lose memory sticks, phones and laptops and emails are frequently sent to the wrong recipient so this record is likely to be lengthy. An employer will need clear policies in place and individuals with clear roles and training to ensure that any breach is assessed and reported to the regulator, if needed, within the 72 hours timeframe.
Summary of practical steps for employers to prepare for the GDPR

- Review your policies and privacy notices to ensure they are clear and in plain English;
- Review policies and practices to ensure that they demonstrate the processing of employees’ data is compliant with the GDPR;
- Ensure that you are able to deal with the new timeframes for dealing with subject data access requests and ensure that policies and procedures are updated;
- If you rely on consent to process personal data, review whether your documents are adequate and that you can prove that consent is freely given, specific and informed;
- Ensure that there is a process in place for employees to withdraw their consent easily;
- Consider what additional information will need to be given to employees and prospective employees when personal data is collected;
- Prepare for data protection breaches by putting in place clear policies and well-rehearsed procedures so that you can react quickly to any potential breach and notify the regulators within 72 hour if needed;
- Consider how you will deal with a request from an employee to delete their data (the right to be forgotten) and how you will demonstrate that your legitimate rights override the interests of the employee if you do not want to do so.

This briefing is part of a series of publications on the GDPR. To access any of these publications, please go to the ‘Publications’ page on our website. If you have any queries on this briefing or if you would like to discuss any aspect of the GDPR or any data protection or privacy issue, please do not hesitate to contact Rebecca Cousin, Rob Sumroy, Richard Jeens or, if in an employment context, Charles Cameron, or your usual Slaughter and May advisor.

Charles Cameron  
T +44 (0)20 7090 5086  
E charles.cameron@slaughterandmay.com

Rebecca Cousin  
T +44 (0)20 7090 3049  
E rebecca.cousins@slaughterandmay.com

© Slaughter and May 2016
This material is for general information only and is not intended to provide legal advice. For further information, please speak to your usual Slaughter and May contact.

October 2016