ReedSmith

Driving progress
through partnership

The GDPR is coming: what are the key issues for HR professionals?

November 2017

Executive summary

The General Data Protection Regulation (referred to below as the Regulation or as the GDPR) comes into effect on 25 May 2018. The new Regulation is a major challenge for employers and, in particular, for HR teams, who will need to grapple with fresh requirements around how employee data is processed (including how such data is gathered, stored, handled and erased). As the risks of non-compliance with the new Regulation are significant (with fines running up to the higher of 4 per cent of annual worldwide turnover or €20 million), preparation for the GDPR is crucial.

In this briefing we highlight six key areas of the GDPR that HR professionals should be aware of, along with recommended practical steps to aid compliance with the Regulation.

For more information, please contact one of the authors, listed below.

Philip Thomas
Counsel, IP, Tech & Data
London
+44 (0)20 3116 3526
pthomas@reedsmith.com

Bethany Parker
Associate, Employment
London
+44 (0)20 3116 2979
bparker@reedsmith.com

Consent

What is the issue?

Where employers wish to rely on employee consent as a lawful basis for processing personal data, the criteria for a valid consent are set to become stricter.

Under current EU and UK legislation, it has been doubtful whether an employer can always rely on an employee's consent to process their personal data, given the imbalance of power between employer and employee. The challenge is that even if an employee (or job applicant) indicates their consent, such consent may not be 'freely given' if, in practice, they felt they had no option but to give consent (for example, because of a fear that a job offer could be withdrawn or that their prospects could be harmed if they did not consent). This remains the case under the GDPR, albeit it also remains the case that employee consent will be obligatory in certain circumstances (for example, where the employer wishes to process 'sensitive personal data' and no other legal basis for processing applies).

The key change under the GDPR is that there are even more stringent requirements as to what qualifies as consent. **Clear, affirmative action** is required, demonstrating a **freely given, specific, informed and unambiguous** indication of the individual's agreement. Consent must be given to each stage of processing, and it must be as easy for the individual to withdraw consent as it was for them to give consent in the first place. Implied consent is no longer likely to suffice. Additionally, any consent must be "clearly distinguishable from other matters", meaning that 'bundled consent' (where consent for a number of distinct processing purposes are bundled together) is unlikely to meet the new requirements.

Practical steps:

- Review all processing of employee personal data. Identify and record the legal basis for the processing in each case.
- Before relying on consent as the legal basis, consider whether another legal basis may be more appropriate – for example, where the processing is necessary for the performance of a contract with the employee (or a data subject), or where the processing is necessary for compliance with a legal obligation. One of the main drawbacks of relying on consent is that consent can always be withdrawn, which can give rise to practical difficulties where some employees consent to a processing activity and others do not.
- Where consent is relied upon as a lawful basis for processing, review existing consents to ensure that they comply with the GDPR. Any such consent will not be valid from 25 May 2018, unless it already conforms to the enhanced requirements of the GDPR.
- Clauses giving consent to data processing activities can still be included in contracts of employment, but they are unlikely to amount to valid consent under the GDPR because the consent may not be freely given. This is on the basis that any such contract of employment is implicitly conditional on the employee giving consent to the data processing activities.
- Where employee consent is required, provide for it to be given in writing in a document that is separate from the employment contract. Ensure the employee is fully informed of the processing activities that the consent would cover, and be clear that the employee is free to refuse their consent without repercussions. Also avoid bundled consents.

Mandatory data breach notification

What is the issue?

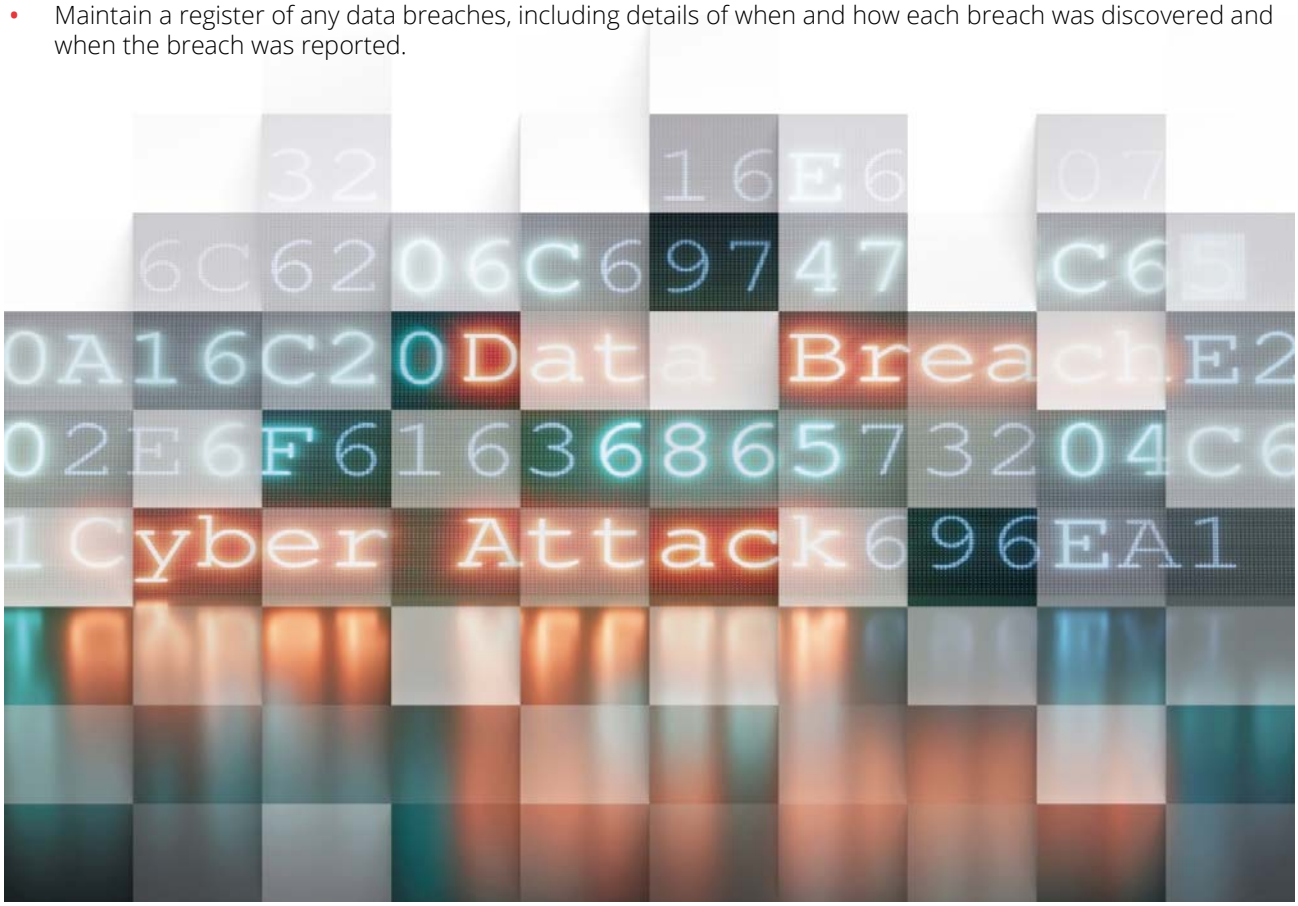
Data controllers will need to notify the relevant data protection authority (in the UK, the Information Commissioner's Office (ICO)) of any data breaches.

It is first worth noting the difference between a data controller and a data processor. A data controller is the person (or business) who determines the purposes for which, and the way in which, personal data is processed. A data processor is anyone who processes personal data on behalf of a data controller (other than the data controller's own employees).

The GDPR requires data controllers to notify data breaches to the ICO "without undue delay" and, in any event, within 72 hours if possible. In turn, data processors must notify the relevant data controller of any data breaches "without undue delay". Certain minimum information (including a description of the nature of the breach, its likely consequences, the measures proposed or taken to address the breach, and the data controller's contact details) must be included in the breach notification. Employee assistance will be crucial in identifying and reporting data breaches.

Practical steps:

- Put a data breach response plan in place, train employees to identify and report data breaches in accordance with the plan.
- Allocate responsibility for notifying the data protection authority, and encourage a culture of compliance and transparency among employees.
- Consider whether any deliberate or negligent failure to report data breaches should amount to misconduct or poor performance.
- Maintain a register of any data breaches, including details of when and how each breach was discovered and when the breach was reported.



Data Subject Access Requests

What is the issue?

For the most part, the Data Subject Access Request (DSAR) process and requirements will remain similar to how they are at present. However, there are a few important practical changes of which employers need to be aware.

First, a fee can only be charged where a request is manifestly unfounded or excessive, or if further copies of the same information are requested. In such cases the fee cannot be more than a "reasonable" one. Outside of these circumstances, information must be provided free of charge.

Second, the time limit for compliance is reduced. Information must be provided without delay and, in any event, within one month of receipt of the request. An extension of a further two months is possible where the request is complex or where numerous requests are made. The individual must be informed of the extension within one month and an explanation for the extension must be provided.

Practical steps:

- Preparation and organisation are key to compliance within a reduced timeframe. Put in place a written policy/procedure for dealing with DSARs and allocate responsibility for the processing of requests.
- Organise personal data so that it is easy to locate and maintain a written list of all locations in which such data is stored.
- Communicate with the requestor so that the scope of the request can be clearly understood, and, if necessary, request additional details to assist your search for relevant data.
- Inform the employee of the estimated timescale for delivery of the information and record the steps taken to locate and deliver the data.

Right to data portability

What is the issue?

The right to data portability will allow individuals to request their personal data in a structured, commonly used, machine-readable and interoperable (i.e., capable of working across different IT systems) format.

This right only applies to personal data (i) which the individual has provided to the controller, and (ii) where the legal basis for processing is either consent or the performance of a contract. In addition, the processing must be carried out by automated means. Provided these conditions are met, the individual is entitled to obtain such personal data, or to request that it is transferred directly to another organisation (provided this is technically feasible). In common with the other rights of the data subject (such as subject access rights, the right to object to processing on certain grounds and the right of erasure), organisations must provide information about the action they have taken on data portability within one month of each request (although a two-month extension is possible where the request is complex or there are a number of requests).

Practical steps:

- Keep records of the source of personal data (i.e., whether it has been provided by the data subject), the basis for processing (i.e., whether it is consent or contract) and the means of carrying out the processing (i.e., whether it is automated).
- Establish a policy and timeframes for receiving, considering and responding to requests for data portability.
- Allocate responsibility for responding to requests.

Right of erasure

What is the issue?

Individuals have enhanced rights to request the deletion or removal of their personal data.

Under the Data Protection Act 1998, the individual's right to erasure is implicit, since the data controller is prohibited from retaining data for longer than necessary to fulfil the processing purpose. Under the GDPR, however, there is an express right of erasure whereby individuals can request the erasure of their personal data in a number of specific circumstances. This includes where the individual has withdrawn their consent to the processing, where the processing of the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed, where the individual objects to the processing and there is no overriding legitimate interest for continuing the processing, and/or where the personal data was unlawfully processed. Valid requests for erasure can only be refused in limited circumstances, such as where the data is processed for the exercise or defence of legal claims.

Practical steps:

- Keep clear records of processing activities, the purposes of these processing activities and the legal basis on which such processing activities are undertaken.
- Where consent is relied on as the sole legal basis, keep a clear record of when and how this consent was obtained.
- Establish a data retention policy with appropriate retention periods for the HR data categories that are kept. Allocate responsibility for receiving, considering and responding to requests for erasure.

Accountability

What is the issue?

The new principle of accountability means that it will no longer be sufficient to comply with data protection laws – in addition, organisations will need to be able to **demonstrate** compliance.

As part of meeting this new accountability requirement, employers will need to have appropriate policies and procedures in place to document how the organisation is capable of complying with GDPR requirements. For example, failing to have a policy in place that tells employees how to report a data security breach may itself breach the accountability principle, even if no security breach has yet occurred. Existing HR policies and procedures may not already comply fully with the GDPR and new policies may also need to be put in place.

Other aspects of accountability are the principles of 'privacy by design' and 'privacy by default'. Privacy by design means that privacy needs to be factored in from the outset of any process, initiative or policy involving the processing of personal data. The notion is that privacy should not be an afterthought. Privacy by default means that the default position should be that any personal data processing activities should be conducted in the least privacy-invasive way. The use of data protection impact assessments can be a useful tool in assessing (and documenting an employer's assessment of) the privacy impact of any process, initiative or policy that involves the processing of personal data.

Practical steps:

- Review existing HR policies for compliance with the GDPR. Consider what changes, if any, may be required.
- Consider whether any new policies may be needed to supplement existing policies.
- Establish a data protection impact assessment process which includes a procedure for employees to identify and report any new initiatives having a privacy impact.

GDPR and Brexit

Because it is a regulation and not a directive, the GDPR has direct effect in the UK. This means that it will come into effect on 25 May 2018 without the UK government having to implement any independent legislation transposing the Regulation into UK law. However, as we all know, Brexit is looming. Does this mean that organisations can ignore the GDPR?

In short, no, for three main reasons:

1. The Regulation will come into effect prior to the UK's date of exit from the EU. Given the significant sanctions for non-compliance, organisations should aim to be compliant from day one.
2. Immediately following the UK's exit from the EU, the European Union (Withdrawal) Bill anticipates copying all existing EU legislation into domestic UK law. In addition, the UK government has published a draft Data Protection Bill which (once in force) will transpose the GDPR into UK domestic law and will set out how the UK has implemented those aspects of the GDPR which have been delegated to individual EU member states to implement as they deem appropriate. This means that although EU regulations may no longer be directly effective in the UK following Brexit, the requirements of the GDPR will nonetheless remain in force in the UK notwithstanding Brexit.
3. The UK Information Commissioner has confirmed that there is no appetite to dilute data protection laws in the UK. This is because the UK is keen to avoid being considered 'a third country', like the United States, whose data protection laws do not provide equivalent protection to those of the EU. The consequence of having weaker data protection laws would be that it may inhibit EU countries from viewing the UK as a 'safe' data protection location.

Organisations should therefore proceed on the basis that the Regulation will apply for the foreseeable future.

Looking ahead

With less than seven months left before the GDPR is fully effective, the pressure is now on for HR teams to review their structures, processes and records to make sure they are compliant with the new Regulation. There's much to learn about the GDPR but the guidance above can serve as a starting point to reduce the risk of expensive non-compliance issues in future.

Reed Smith can provide guidance and assistance on all aspects of the GDPR. For more information on developments in this area, please get in touch with Philip Thomas for data protection aspects, Bethany Parker for employment aspects, or your usual contact at the firm.

Philip Thomas
Counsel, IP, Tech & Data
London
+44 (0)20 3116 3526
pthomas@reedsmith.com

Bethany Parker
Associate, Employment
London
+44 (0)20 3116 2979
bparker@reedsmith.com

Reed Smith is a global relationship law firm with more than 1,700 lawyers in 27 offices throughout the United States, Europe, Asia and the Middle East.

Founded in 1877, the firm represents leading international businesses, from Fortune 100 corporations to mid-market and emerging enterprises. Its lawyers provide litigation and other dispute-resolution services in multi-jurisdictional and high-stakes matters, deliver regulatory counsel, and execute the full range of strategic domestic and cross-border transactions. Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, advertising, entertainment and media, shipping and transport, energy and natural resources, real estate, manufacturing and technology, and education.

ABU DHABI
ATHENS
BEIJING
CENTURY CITY
CHICAGO
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com