CLYDE&CO

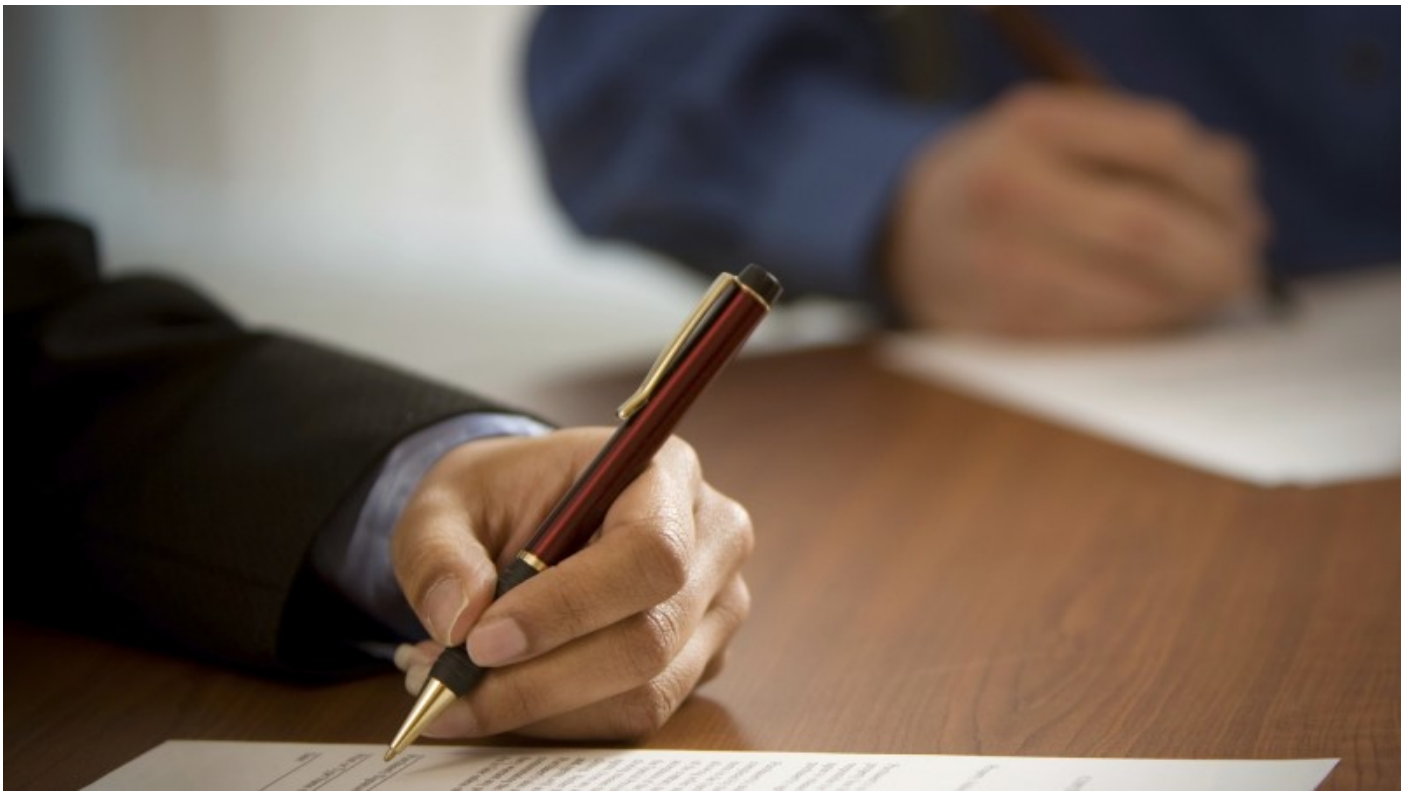
THE EMPLOYMENT HIVE

AUGUST 21, 2017

GDPR - 10 key questions for employers

Written by Chris Holme & Dan Sulkowski

Data protection laws will be changing from 25 May next year. This is the date when the European General Data Protection Regulation (GDPR) comes into force across the EU, including the UK.



Earlier this month, a government press release confirmed that the Data Protection Bill, setting out how the new law will apply in the UK, will be published in September. This will replace the UK's current Data Protection Act and implement the GDPR, subject to some permitted changes, from 25 May 2018. Please see our recent bulletin for further details of what the statement of intent revealed.

We will be broadcasting a briefing shortly after the Bill has been published and you can register your interest in that briefing here.

Businesses need to review and prepare for the change in data protection laws in every area where they gather

and process personal data. This note is focused on the particular issues that businesses have as employers in relation to the new law, and is aimed at HR departments, employment in-house counsel, and anyone else who is reviewing how the changes will impact the gathering and processing of personal data from an employment perspective.

We have set out below the 10 key questions which employers should be asking themselves to help prepare for the introduction of GDPR.

1. What personal data are you processing in relation to your people (past, present and future), and why?

All employers will process personal data in relation to their staff - personal data includes any information relating to an employee who can be identified from that data and any expression of opinion or intention in relation to an employee.

Some employers may also process sensitive personal data such as information relating to racial or ethnic origin, trade union membership or physical / mental health.

Both categories of data (meaning both personal data and sensitive personal data) are changing under the GDPR.

Personal data will be wider, for example expressly including online identifiers such as IP addresses. Sensitive personal data is given a catchy new name - 'special category personal data' – and will now include genetic data and biometric data. Data relating to criminal convictions will no longer come within the general definition of "sensitive personal data", but will instead be dealt with separately and subject to even more rigorous processing restrictions.

The GDPR will require employers to ensure that only the minimum amount of personal data necessary for each specific purpose is processed and retained for no longer than necessary.

We therefore recommend that, as a preliminary step, employers start carrying out a data mapping exercise now, in order to determine:

- what personal data, special category sensitive data, and criminal records data, is being processed in relation to staff (past, present, and future);
- why it is being processed; and
- how long it is retained.

This data mapping / due diligence will assist employers answer the key question of whether it is necessary for them to process the data (necessity is a common theme in the GDPR) and justify the processing if challenged. It is a necessary first step when determining how you are going to comply with the GDPR.

2. Will you rely on 'necessity' or 'consent' or both to process personal data?

Historically, employers have relied on wide ranging general consent provisions in contracts to enable them to lawfully process a wide range of information in relation to their staff.

This approach needs to be reviewed in light of how the GDPR defines and approaches the issue of consent. Consent will have to be explicit, in relation to each processing activity, and freely given. As a result, employers will not be able to rely on a generic reference to consent within an employment contract or data protection policy, which an employee is required to agree as part of wider terms and conditions.

Note that even a more specific and detailed approach to obtaining consent (where you list out each and every aspect of processing of personal data to which an individual is consenting) is unlikely to be either pragmatic or satisfactory. Even if this was administratively possible, consent can be withdrawn by an employee at any time on immediate notice. Employers will therefore not want to rely on it when they need to process data as part of the relationship.

This leads naturally to an examination of whether or not the (currently little used) exemption of "necessity" to enable employers to process data should be used more often.

The GDPR provides that the processing of personal data and special category personal data will be lawful if it is necessary by reference to certain justifications set out within the GDPR. Properly documenting the justification for necessity by way of a data processing map is recommended, particularly as this could be used to demonstrate the lawful basis of processing to the ICO should it ever be needed.

We believe this will become the default position adopted by employers for the majority of their processing of staff data.

Indeed the draft guidance from the ICO which indicates that employers should rely on 'necessity', wherever possible, to process personal data unless they need consent (because, ultimately, necessity does not apply).

Whilst some employers may consider riding two horses by relying on both consent and necessity, one horse may trip up the other. The reliance on consent may undermine an employer's ability to rely on necessity on the basis that consent would not be required if processing was genuinely necessary.

Accordingly, if an employer concludes through its data mapping that it is "necessary" to process certain data, consent should no longer be asked for (nor relied upon). Instead an employer should be clear that it is using necessity as the rationale (and exemption) for processing that data.

However, specific consent may be appropriate in limited circumstances – for example, as a pre-requisite before an employee accesses an instant messaging platform provided by an employer, or before an employee is given their company car with telematics technology within.

3. How do you keep data secure and what will you do in the event of a security breach?

Employers must keep personal data secure and although the GDPR expresses this in general terms, appropriate safeguards will be even more important under GDPR in view of the potential serious sanctions for non-compliance (see question 8).

Personal data breaches must also be reported to the Regulator within 72 hours and, in some cases, the Regulator will require employers to report breaches to affected individuals unless an exemption applies. One such exemption is having appropriate safeguards in place to protect data such as encryption.

Therefore, employers should consider reviewing and updating security measures and setting up processes for reviewing, documenting and notifying breaches.

This will bring a renewed focus on policies around taking data out of the office space, working from home (and how data can be accessed remotely), who can access data (and limiting access to systems to those who need it for their work), use of employees' own devices, and any other policy which governs (or interacts with) the use of an employer's data, and how it is shared and processed.

4. How long will you need to retain data?

The "Principles" in relation to retention periods for personal data remain unchanged under the GDPR. Personal data should be kept no longer than necessary for the purposes for which it was processed.

Historically data retention policies have perhaps not been taken as seriously (and implemented as seriously) as they will need to be going forwards. The increased, and serious sanctions for non-compliance should encourage employers to be stricter about managing data retention properly.

In addition, employers should be mindful that poorly managed data retention may significantly increase the burden created by data subject access requests ("DSARs") – a tool increasingly used by employees who want to find information processed about them. The GDPR is introducing changes to DSARs with employers allowed less time to comply and, potentially, a wider pool of data being captured by such requests. Therefore, an increased focus on retention should ensure that:

- the costs and time incurred in relation to DSARs is no greater than necessary; and
- DSARs do not flag wider non-compliance in relation to unnecessary processing of documents.

The data mapping exercise to be carried out in preparation for GDPR will also help identify where data is and what is held. As a result, employers should be far more ready to deal with a DSAR than they may have been historically.

5. Do you have to worry about the historic personnel files in the filing cabinet which nobody opens anymore?

Yes. The data in historic files will still be deemed to be 'processed' and:

- employers will not be able to rely on existing consent. All personal data, including data collected before implementation of the GDPR, will have to be processed by consent or necessity in accordance with the GDPR;
- the focus on not retaining data longer than necessary means that the risk of sanctions increases if historic files are ignored.

Hence a data mapping exercise to determine the totality of data held by employers should be considered.

6. How easily are you able to remove data from your systems?

Employees will have the right to erasure (deletion of data in relation to them) and to restrict/object to processing, which will be triggered as a result of non-compliance with the data protection principles. Non-compliance can include an employer retaining data longer than necessary.

Therefore employers should consider what it will mean for their business if employees exercise these new rights, and set up processes to record and act on erasure requests.

7. Do you carry out cross border processing?

Employers will be subject primarily to the regulator in the jurisdiction in which they have their main establishment.

Therefore, employers should consider where their main establishment is in order to obtain advice as to any specific derogations from the GDPR which will apply within that territory.

In addition, the GDPR prohibits the transfer of personal data outside the EU unless certain conditions (broadly the same as those under the existing rules) are met. Therefore, if you transfer data outside the EU, consider reviewing your current data transfer processes and consider if they are justified now in order to determine whether they will also be justified under the GDPR.

8. How will you demonstrate compliance with data protection principles if challenged by the Regulator?

Employers must be able to demonstrate compliance. Throughout the design stage of any policy, process, product or service, employers must take data protection risks into account. This involves:

- Assessing and implementing appropriate and proportionate technical and organisational measures and procedures from the outset;
- Putting mechanisms in place to ensure that only personal data necessary for each specific purpose is processed;
- Completing a detailed Privacy Impact Assessment if carrying out "high risk" processing, such as CCTV monitoring or the processing of special category sensitive data (this may require consultation with the Regulator about whether risk mitigation is adequate); and
- Creating and maintaining a record of the processing which they are carrying out to ensure that the processing remains necessary.

A failure to comply with the GDPR has, potentially, far more serious consequences than a breach of the Data Protection Act - the regulator will be able to issue fines of up to 4% of annual worldwide turnover, or €20 million. Individuals can also claim compensation to recover both material and non-material damage (e.g. distress).

9. Will you need to appoint a data protection officer(s)?

Where an employer's core activities involve regular and systematic monitoring of data subjects on a large scale or large-scale processing of sensitive personal data, a DPO will need to be appointed.

DPOs must be involved in all data protection issues and must report directly to the highest level of management within the organisation. Employers not required to appoint a DPO should still consider whether to appoint one on a voluntary basis – or at least an individual responsible for reporting non-compliance to the Regulator.

10. What documents will you need to create/update?

Employers will need to update employment contracts and policies to reflect the new data protection regime.

New contractual provisions will also need to be considered for contracts with data processers (such as HR services providers) as some aspects of the GDPR are directly applicable to data processors.

In addition, privacy notices, which tell employees what you will do with their personal data, will need to be updated. These must be in place at the point that employees provide personal data. Under the GDPR, the privacy notices must be "concise, transparent, intelligible and easily accessible", yet the GDPR prescribes additional information to be included, not previously required.

Employers will also need to consider how they will inform employees of changes brought about by the GDPR, how they will document consent (if consent is sought), and/or how the explanation for necessity will be conveyed or made available to employees.

If you would like any further details in relation to this please contact Chris Holme or your usual contact at Clyde & Co.

Authors

Chris Holme
Partner

Daniel Sulkowski
Senior Associate

More by the authors

‘Good Work’ Report – 10 key points for employers from the…

Mind the Gap: Our latest analysis of the gender pay gap reports published so far

Mind the Gap: Our analysis of the gender pay gap data reported so far

Employment Tribunal fees decision - update No.2

The Data Protection Bill is coming but are you ready?

Categories

Market insight