SQUIRE PATTON BOGGS

GDPR Compliance
How Employers Can Meet the 25 May 2018 Deadline

Have You Set Your Compliance Clock?

The new EU General Data Protection Regulation (GDPR) will have direct effect throughout the EU from 25 May 2018 and it is likely to apply in the UK even post-Brexit. The scale of the changes imposed by the GDPR is significant, and organisations caught by the new rules need to take steps now to ensure compliance by May 2018 and to avoid fines of up to €20 million, or 4% of global turnover, whichever is the higher.

The GDPR will govern employers' use of the personal data of applicants, employees, former employees, workers, contractors, etc. It will also apply to any other data they use about individuals, such as customers and suppliers.

This document highlights the main steps that employers should take to comply and provides average time estimates for each step of the process. A number of the steps can, however, be undertaken in parallel.

Our global Data Privacy & Cybersecurity team can help you develop and implement a compliance plan and timetable to suit your needs.

Step 1: Data Mapping

3-6 Months +

Action

Create detailed records of all data processing activities, including the categories of personal data, data subjects and recipients, the purposes of processing, any transfers of personal data outside the European Economic Area (EEA), the time limits for storage of the data and the security measures in place to protect it.

The business as a whole will be required to produce a data map in respect of all personal data held/used by it, but HR will be best placed to provide this information in relation to workers. Undertaking this mapping exercise early on will also help the HR team and the wider business to identify possible gaps in their compliance.

Why?

It will be mandatory for employers to maintain these records under the GDPR and they may be required to produce them to the Information Commissioner's Office (ICO).

Step 2: Privacy Governance/ Data Protection Officer

1-3 Months

Action

The business must assess whether it is required to appoint a Data Protection Officer (DPO) (usually where it engages in large-scale use or monitoring of individual customer data, e.g. utilities, loyalty card operators, etc.) and, if so, appoint someone who meets the GDPR criteria. Whether or not it is strictly obliged to appoint a DPO, the business will need to review and, if necessary, improve its corporate governance policies and structure, including those relating to HR, to ensure that they are sufficient to achieve GDPR compliance, and it makes sense to have someone nominated with that responsibility.

Why?

Robust data governance is key to fulfilling the accountability obligations placed on all organisations under the GDPR. The most extensive and sensitive information held by a business is likely to be about its employees, making compliance in the HR field critical.

Step 3: Data Sharing and Service Providers

6 Months +

Action

Identify all circumstances where personal data is shared with third parties, either for that party's own purposes (e.g. a parent company), or to a service provider in the course of its providing the service (e.g. payroll processors, providers of domestic or global HR databases, external intranet hosts, external trainers/training platforms, etc.). Review all contracts with processors and draft and negotiate necessary amendments to comply with the GDPR.

Why?

The GDPR requires new provisions to be included in agreements with processors (including as to sub-contracting, audit assistance, acting on documented instructions only, breach reporting, etc.) and expands the employer's due diligence obligations before engaging them. It also makes it more advisable to have written data sharing agreements with other data controllers.

Step 4: International Data Transfers

In parallel with Step 3

Action

Identify whether any of your data sharing or service contracts involve the transfer of personal data to, or access to it from outside, the EEA. These could include where data is held in the cloud or on servers outside the EEA. It may also apply if support, for example, IT services, are provided 24/7, even if the contract is with a European entity. Ensure that a transfer mechanism approved by the European Commission is in place, remembering for the US that Safe Harbor has now been replaced by the EU/US Privacy Shield.

Why?

The GDPR retains the current requirement to have adequate measures in place when transferring personal data outside the EEA.

Step 5: Justification for Processing

2-3 Months

Action

Carefully consider what data is collected and whether it is needed. Consider what justifications for processing employee data the employer has, avoiding, where possible, reliance on consent or "legitimate business interests". This is about establishing a specific business **need**, as opposed to a nice-to-have.

Why?

The GDPR makes it much more difficult to rely on consent as a justification because it considers that there will always be inequality of bargaining power between employer and employee or job candidate and, therefore, that such consent may not be truly freely given. The ICO, in draft guidance, has said that it will almost never be appropriate to rely on consent as a justification for processing employee data, and could even be misleading. Those employers that seek to obtain consent for processing personal data by including standard wording in their contracts of employment should consider what other grounds are available to justify processing, such as being necessary for the performance of the employment contract, or to comply with a legal obligation.

Step 6: Privacy Notices

1-2 Months

Action

Review and revise all privacy notices given to applicants, employees and other workers, to comply with the GDPR. This information is frequently included in data protection policies or contracts of employment and these will, therefore, need to be updated.

Why?

The GDPR introduces additional provisions that must be included in privacy notices. These include detailed statements of what data is being processed and why and of the individual's rights to removal, rectification, objection, portability, etc., of the data, plus the right to refer issues to the ICO. With consent largely falling away as a justification for processing, privacy notices become all the more important.

Step 7: Review Consents and Automated Processing/Profiling

1-2 Months

Action

Consider all circumstances where you currently rely on consent as the justification for processing, e.g. consent to an employer sending health information to a medical specialist. If consent is still appropriate (which will primarily be for optional extra benefits or where the employee is seeking disclosure, e.g. of salary to a mortgage lender, not data needed for the operation of the employment contract), ensure that the manner of obtaining and evidencing consent complies with new GDPR requirements.

Consider whether any wholly automated decision-making or profiling is undertaken in relation to applicants or employees, e.g. computer marking of multiple choice entry tests.

Why?

In the very limited circumstances where consent can be a valid justification for processing personal data about workers, there are strict new rules as to how consent must be obtained and evidenced. Any consents should be opt-in, not opt-out. Workers must always be informed about profiling and automated decision-making, and there are strict limitations around its use.

Step 8: Data Security and Breach Management Process

3-6 Months

Action

Review the data security measures in place to ensure they are sufficient to protect personal data from unauthorised access or disclosure, and to assess whether the specific additional measures referred to in the GDPR, especially encryption, are (or should be) in place.

Put in place a data breach response plan, as the GDPR requires data breaches involving any risk to individuals to be reported to the ICO without delay and within 72 hours, and affected individuals to be notified if the breach is high risk.

Why?

Suffering a security breach is one of the most common ways for employers to come to the attention of the ICO. Having a data breach response plan helps avoid the "rabbit in headlights" effect if a breach occurs.

Step 9: Privacy by Design and Default

6 Months

Action

Review or establish procedures to ensure GDPR compliance is embedded in all applications and processes. Employers implementing a new HR system should be seen to consider to what extent data protection can be built into the design.

Why?

To comply with the new Privacy by Design and Default obligations, which require GDPR compliance to be integrated into all data processing, including data minimisation, the process of reducing the processing of personal data to a minimum in terms of least possible data, shortest storage periods, minimum distribution and access, etc.

Step 10: Individuals' Rights

3 Months

Action

Identify which of the new individual rights provided under the GDPR are likely to be exercised against employers (rectification, erasure, restriction, objection, portability, etc.) and establish procedures for dealing with them in accordance with the GDPR. Review the procedures in place in order to comply with existing (but expanded) rights such as subject access requests and amend internal policies and processes, where required.

Why?

The time limit for responding to subject access requests is reduced to 30 days. Where "legitimate interests" is the justification for processing, if an individual objects to the processing, it must be suspended while the request is investigated, unless and until the employer can confirm to the employee that it has compelling grounds for the processing which overrides their objection. This might be to comply with health and safety or other legal obligations, such as disclosure in litigation or operation of PAYE.

Step 11: Data Protection Impact Assessments

3 Months

Action

Assess whether any use or proposed use of personal data could be classed as "high risk" under the GDPR. If so, carry out a Data Protection Impact Assessment (DPIA) and, if necessary, consult with the ICO.

Why?

DPIAs must be carried out in relation to all high risk processing, and consultation with the ICO may be required in certain circumstances. The GDPR contains a non-exhaustive list of high risk processing, which is to be supplemented by guidance from the ICO in due course.

Step 12: Roll-Out of Compliance Tools

6 Months +

Action

Roll out new privacy notices and (if any) consent forms. Publish new and revised policies and procedures. Provide training to all HR staff. Review template contracts of employment and consider whether any data protection wording needs changing to constitute the privacy notice if this is not to be a separate document.

How Can Our Data Privacy & Cybersecurity Team Assist Employers?

We Can:

- Carry out GDPR audits to identify the gaps in employers' compliance and devise a GDPR compliance plan
- Assist with data mapping
- Draft GDPR-compliant Data Sharing Agreements and Data Processor/Service Agreements
- Review the form and process for obtaining consents and any automated use of data and advise how to plug any gaps
- Evaluate whether data uses are high risk and carry out Data Protection Impact Assessments and advise on the consultation requirements
- Review and redraft Privacy Notices
- Develop data subject access response systems
- Draft Data Protection policies and Data Retention Policies
- Provide training for employers, their staff and others who will be affected by the new obligations
- Advise on Data Security requirements
- Draft Data Breach Response Plans

Key Contacts