COVINGTON

Are You Ready for the European General Data Protection Regulation? A Practical Checklist for Employers

May 25, 2017

Data Privacy, Cybersecurity and Employment

Overview

One year from today, on May 25, 2018, employers located or with staff in the European Union ("**EU**") will have to comply with a new data protection law—Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data—commonly referred to as the General Data Protection Regulation ("**GDPR**"). This will replace the Data Protection Directive 95/46/EC.

The GDPR was originally intended to introduce a single legal framework applicable across all EU member states. However, the final text of the GDPR has fallen short of this aim, since it contains an express carve out for EU member states to enter into laws or collective agreements that provide for more specific rules relating to processing data in the employment context. In addition to developing an understanding of the GDPR, employers will therefore need to keep abreast of relevant local law developments that 'gold plate' the GDPR provisions.

Failure to comply with the GDPR will result in substantial financial penalties—up to €20,000,000 or 4 percent of worldwide turnover for the most severe infringements, whichever is higher. In addition, there is an increased likelihood of lawsuits from individual data subjects and representative bodies, due to the potential to recover compensation for both material and non-material damage. As a result, GDPR compliance is now a major area of risk for employers.

The GDPR builds on a number of existing data protection laws and introduces significant new concepts. This alert provides a practical checklist of key considerations for employers and human resources professionals preparing for the new regime, ahead of its implementation next year.

1. Determine Whether the GDPR Applies to Your Organisation

This analysis will be straightforward for many organisations; employers located or with staff in the EU will fall within the scope of the GDPR.

Organisations cannot confine themselves to considering solely whether they have EU-based employees. Directors, partners, temporary agency staff, zero-hours workers, consultants, self-employed contractors, apprentices, volunteers, job candidates and former staff are all "data

subjects" for the purposes of the GDPR. Throughout this alert we use the generic terms "employer" and "staff" to capture these various relationships.

Employers with UK operations will not escape the need to comply with the GDPR after Brexit. The UK Government has confirmed its commitment to adopting the GDPR as part of its digital strategy, and will soon begin repealing parts of the UK Data Protection Act 1998—particularly its enforcement provisions—so that inconsistences with the GDPR are avoided.

2. Conduct an Audit and Gap Analysis

Once a legal requirement to comply with the GDPR is established, a sensible starting point for employers will be to examine current data processing practices via an audit, covering:

- the categories of HR information currently processed by the organisation (e.g., payroll data, information relating to job applicants, any special categories of data such as diversity information);
- whom HR information is shared with (e.g., group companies, third party benefit providers);
- how and where the information is stored (e.g., electronically or paper files, on central cloud-based HR systems, in local files);
- whether HR data are subject to automated processing (e.g., during the recruitment process);
- how long information is stored for;
- any cross-border transfers of HR data (outside the European Economic Area ("**EEA**")); and
- variations in practice across different business units and countries.

The results of the audit and gap analysis will help identify key risk areas and what needs to be done to bridge the gap to becoming GDPR compliant. Employers should also consider how to build privacy considerations into HR systems from the outset and on an ongoing basis, to help meet the GDPR standard of "privacy by design and default."

3. Assess Whether a Data Protection Officer Is Required

Employers in the private sector must appoint a Data Protection Officer ("**DPO**") in two circumstances:

- if the core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale;
- if the core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

EU member states may also require that a DPO is appointed in other situations.

Regulators have recently published guidance on these tests and on the various aspects of the DPO's role. The DPO will take responsibility for data protection compliance, including coordinating with the relevant supervisory authority, so it is essential the right person within an organisation is appointed who has a deep understanding and knowledge of the employer's

organisation and data protection law. The DPO has the right under the GDPR to be protected from being penalised or dismissed for performing his or her role.

4. Review Existing Terms with Third-party Processors

The GDPR imposes more detailed and onerous obligations on employers to ensure that appropriate contractual protections are in place with third-party processors, such as external payroll companies, benefits providers and HR software suppliers. Contracts between the employer and any processors that are identified as part of the audit process should be reviewed and, in some cases, renegotiated to ensure compliance with the GDPR.

5. Update Existing Privacy Notices and Policies; Conduct Staff Training

The GDPR sets out detailed requirements for the information that must be provided to employees and other data subjects when processing their personal information. Such privacy notices must be concise, accessible and written in clean and plain language.

Employers must explain, among other things, the legal basis for processing each type of data, how long data are retained for, details of the organisation's Data Protection Officer (if any) and their right to complain to the supervisory authority. Existing privacy notices will need to be updated and reissued to cover the mandatory requirements of the GDPR.

In addition, staff need to be informed about their duties and responsibilities when processing data on behalf of the organisation. Employers will need to put in place policies outlining the steps staff must take to meet the general requirements of the GDPR as well as particular focus areas, such as retention of HR records, how to respond in the event of a data breach and dealing with the new data subject rights (see below).

Implementing policies alone is not sufficient to ensure GDPR compliance. Employers should roll out training programs to staff to raise awareness of policies and ensure they are adhered to in practice.

6. Limit Reliance on Consent

The GDPR makes clear that consent will rarely be an acceptable legal basis for processing employment data, due to the imbalance of power between the employer and data subject. The UK Information Commissioner's Office has recently confirmed this in draft guidance. There are other reasons to avoid reliance on consent in the employment context, including the ability of data subjects to withdraw consent to processing at any time, as well as the associated rights that are linked with consent (including the right to be forgotten and the right to data portability).

Wherever possible, employers should consider an alternative legal basis for the processing of that information, such as compliance with a legal obligation or the pursuit of a legitimate interest of the employer.

7. Be Prepared for Enhanced Data Subject Rights

The rights that data subjects enjoy under the GDPR have been significantly enhanced, and now cover:

- subject access;
- the right to have inaccuracies corrected;

- the right to have information erased (the so-called “right to be forgotten”);
- the right to prevent direct marketing;
- the right to prevent automated decision-making and profiling; and
- data portability.

Organisations must ensure that they are prepared to respond to the exercise of these rights by members of staff. For example, employers should ensure that there are guidelines and training in place where a subject access request is received from a current employee, or where a member of staff asks for certain data to be erased.

8. Review International Data Transfers

Multinational employers will continue to face restrictions when seeking to transfer personal data to countries outside of the EEA that are not deemed to give adequate protection to data under local law. Although the GDPR does not change the current framework significantly, this is an evolving landscape in light of on-going challenges to EU-US transfers, EU model contractual clauses (approved contracts for exporting data outside the EEA), and Brexit. There is also scope under the GDPR for the list of countries that are deemed to have adequate data protection laws to be reviewed and amended in the future.

A welcome change for employers is that the GDPR removes the requirement that transfers based on model contractual clauses be notified or approved by local data protection authorities.

9. Identify Automated Decision-making Processes

The GDPR gives data subjects the right not to be subject to a decision based solely by automated processing where that decision significantly affects him or her. In the employment context, common automated decision-making processes that impact employees include recruitment tools (e.g., auto-shortlisting for roles), performance management software, and employee monitoring. Where the employer’s GDPR audit identifies that such automated decision-making processes are in use within the organisation, the employer should consider whether it has the ability to understand and explain decisions, as well as whether alternatives that involve human decision making are available in the event a data subject objects to the automated processing of his or her data.

10. Prepare to Meet Staff Information and Consultation Requirements

Multinational employers must be mindful of any country-specific information and consultation obligations with employee representatives or works councils that may be a prerequisite before amending terms and conditions, staff notices, company policies etc., in order to become GDPR compliant. Sufficient time must be built into the employer’s GDPR compliance plan to ensure consultation requirements can be met in time for next May.

Failure to do so could lead to staff bringing claims in the relevant labour courts, resulting in financial and other disciplinary penalties, as well as employee relations issues.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our HR Employment/Privacy practice:

Daniel Cooper	+44 20 7067 2020	dcooper@cov.com
Helena Milner-Smith	+44 20 7067 2070	hmilner-smith@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com
Ashley Moss	+44 20 7067 2291	amoss@cov.com