Keeping HR on track
Our experienced GDPR advisers
The direction of travel

Whilst they were many years in the pipeline, the most significant reforms to EU data protection law since the Data Protection Directive of 1995 are now here. The General Data Protection Regulation took effect in the UK from 25 May 2018, accompanied by the Data Protection Act 2018 to facilitate implementation and exercise some of the permissible derogations.

The implications of the GDPR and the task facing organisations in applying it should not be underestimated. The impact is all the more significant for businesses with a global reach because the wider territorial scope of the GDPR means many companies outside the European Economic Area (EEA), who provide or assist in providing services to employers within that area, are subject to new obligations. Furthermore, it not just data controllers who fall within the provisions of the GDPR but those data processors who undertake data processing activity. This significant change means payroll providers, recruitment consultants, etc., to whom institutions outsource functions are now directly subject to the GDPR.

At the heart of compliance with the GDPR is accountability, the regulation applying a much more prescriptive approach to data protection compliance. Employers and human resources practitioners are invariably at the forefront of these changes to data protection practice and, just as crucially, how such matters are communicated to the workforce and beyond. Considerably larger penalties also provide strong incentives for institutions to comply with the GDPR. For the first time, penalties can be linked to an institution’s turnover, with potential fines of up to 4% of global annual turnover or a maximum of €20,000,000, whichever is higher.

HR practitioners and institutions have had a great deal to think about to prepare for the changes. Those who failed to appreciate the full impact in advance are now doing so. However, even those who produced a carefully considered and planned strategy in anticipation are having to adapt as full understanding and practical effect of the GDPR emerges.

This presents a significant challenge for institutions and, for many, has required a major change in mind set. Those who fail to embrace this essential concept within their policies and approach will not only find compliance with the GDPR difficult but will also struggle to defend themselves against the considerable financial penalties which could be imposed.

The GDPR requires a hard line, pragmatic approach to employee information to identify why information is needed, what it will be used for, who can see it and what the employee is told. Contractual changes and use of impact assessments (whether as formally required by GDPR or conducted voluntarily) are also important tools for institutions to help identify areas of risk, appropriate response and employee awareness. Externally, the terms of engagement of payroll or employee-benefits providers, recruitment agents, etc., also need to have been reviewed to clearly delineate the more stringent, shared data protection responsibilities.

A further essential aspect of demonstrating accountability under the GDPR, is the need for many institutions to keep records of their data processing activity. How this is done, how much detail is recorded and where it is stored are important questions.

We have the necessary experience to assist you in developing your data strategy for the future within the GDPR framework and in the task of reviewing your employment contracts and terms with service providers from time to time and recording such steps appropriately.

Enhancing or updating your data protection policy and procedures
Drafted appropriately for your organisation’s needs in accordance with the GDPR, your policies and procedures must at all times demonstrate compliance and act as a vital guide for employees and relevant third parties, as well as a means of managing expectations in terms of data handling. Accessibility of policy documents plays an equally important part, not just in terms of where they can be found but in how they are worded and the language in which they are provided, to limit misunderstanding.

Whilst having an appropriate policy is now fundamental to data protection compliance, how it is applied in practice and by whom are just as important to meet GDPR obligations. All policies across the institution should also be consistent in message and approach. For example, a disciplinary policy should reflect employee-responsibilities and the gravity of default.
Lawful data processing

In an HR context, one of the most important illustrations of how the GDPR is more onerous for employers is where an individual had given consent to the processing of their data, such as via their employment contract, and the employer relied on that employee consent for processing. Reflecting an acceptance that such provision is not consent which is truly "freely given", employers should be conducting their data processing according to one of the legitimate reasons identified by the GDPR and that reason should be identified in offer letters and contracts of employment. Examples include that processing is necessary for the performance of the employment contract; for employer compliance with a legal obligation or for the pursuit of the legitimate interests of the employer (or a third party). If the legitimate interests condition is being relied upon, employees need to be informed what the alleged interests are. Making appropriate assessments of the rationale for processing is key and HR professionals play a pivotal role in identifying these reasons, recording how they are being applied but also ensuring appropriate proportionality.

If you do continue to use consent as a lawful condition for processing, you should bear in mind that such consent can be withdrawn at any time, potentially suspending HR functions. You also need to inform your employees of their right to withdraw their consent.

Transparency and pro-actively communicating data policy

For there to be accountability, one must have transparency. As a result, the GDPR places considerable emphasis upon the responsibility of institutions to keep their data subjects informed about personal data processing and of their rights. The regulation is also more prescriptive in terms of the information employees must be given. Having an appropriate communications strategy and mechanism is vital to ensure employees are made aware of which personal data you are processing, why and their rights with regards to those data.

HR practitioners bear much of the responsibility in most workplaces for the preparation and communication of privacy notices to current employees, new employees and job applicants, (more accurately described as "fair processing notices"). We regularly provide bespoke training for organisations and their staff regarding their increased rights and obligations under the GDPR, and ongoing changes that might be needed, tailored to existing practices.

Responding to requests for data access

How institutions approach subject access requests or "DSARs" is an aspect of data handling which often causes them concern. Having a clear and accessible policy is essential but institutions also need to respond quickly if they are to meet the strict one month turnaround time stipulated by the GDPR. Institutions should note that the GDPR has also removed the right to charge for responding to DSARs unless the request is "manifestly excessive" but this is likely to be a high threshold to meet, so reliance upon it is likely to be limited.

However, DSARs are only one of various data subject rights. To comply with GDPR requirements, therefore, managers and other staff likely to receive data enquiries from employees, need to be able to recognise data requests in the various forms they may take and whether they are a DSAR, objection, request for deletion, correction, or portability. They will then need to action the request appropriately in an efficient and timely manner. Clear guidance and training in these aspects should be provided.

Our team of experts frequently advises upon appropriate responses to such requests, as well as to alleged failures to comply. Communications with the Information Commissioner’s Office can prove particularly daunting, as well as critical to the organisation’s defence of its actions. We can provide advice and assistance with all such matters.

Reporting breaches

Institutions are now subject to a mandatory reporting of data breaches "without undue delay" but not later than 72 hours after becoming aware. You need to move quickly to assess whether mandatory reporting applies in the particular circumstances, whilst meeting the 72 hour deadline, where required. Additionally, employees and affected individuals themselves may need to be notified where the breach is likely to result in high risk to them, unless the institution can establish that encryption or the extent of circulation allows containment. In all cases, the institution must nonetheless retain its own record of what occurred, action taken, etc.

This reporting obligation not only requires fast action on the part of the institution but attracts much higher penalties if it is not observed. Institutions must therefore ensure that their procedures and practices for dealing with security are appropriate, both in terms of preventative measures but also steps if breaches occur, including their reporting. HR personnel need to be alert to the risks and equipped to deal with them promptly.

We have a team of specialist data protection advisers with significant experience in dealing with such matters and who can assist you, should you require help or advice.

Key

DSAR - Data Subject Access Request
GDPR - General Data Protection Regulations
HR - Human Resources