APERTURE
PARTNERS
ADVISORY

The General Data Protection Regulation
A Twelve-Step Plan for Employer Compliance

APERTURE
PARTNERS
ADVISORY

Overview

The implementation of the long-awaited European Union ("EU") General Data Protection Regulation ("GDPR" or the "Regulation") is now clearly on the horizon. The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from 1995, when the Directive was established. Although the key principles of data privacy have been retained in the GDPR, many changes have been proposed to the regulatory policies.

The GDPR takes effect and is enforceable from the 25 May 2018, at which point organisations in non-compliance may be liable to penalties.

In this bulletin, we explore what practical steps employers can take to ensure compliance.

Employee Rights

Employees will have a right under the GDPR to obtain information from employers about whether their personal data is being processed and, if so, where and for what purpose.

Employees will have the right to have their details used in line with data protection regulations, the right to information about their personal information, the right to access their personal details, the right to know if their personal details are being held, the right to change or remove their details, the right to prevent use of their personal details, the right to remove their details from a direct marketing list, the right to object to their details being used, the right to freedom from automated decision making, and the right to refuse direct marketing calls or mail.

Employees have the right to data protection when their details are held on a computer, held on paper or other manual form as part of a filing system, and made up of photographs or video recordings of their image or recordings of their voice.

The aim of these rights is to help the employee ensure that the information stored about them is: factually correct, only available to those who should have it and only used for stated purposes.

Employer Actions

To assist companies with the initial preparation for the changes in the GDPR, the Data Protection Commissioner ("DPC") has prepared an introductory document for companies which lists 12 steps that can be taken now to prepare for the changes expected to come into force in May 2018. It should be noted that the guide is not an exhaustive list and companies should ensure that their preparations take account of all actions required to bring them into compliance with the new law.

1. **<u>Awareness</u>: Employers should review and enhance their company's risk managements processes and try to identify problem areas now. Implementing the GDPR could have significant resource implications, especially for larger and more complex companies.**
2. **<u>Information Employers hold</u>: Employers should make an inventory of all personal data they hold. Why do they hold it, do they still need it, and is it safe? If the company has inaccurate personal data and has shared this with another company, they will have to notify the other organisation so it can correct its records. This can only be done if the company knows what personal data is held, where it came from and who it is shared with. Documenting these details will help to comply with the GDPR's accountability principle requiring organisations to be able to show how they comply with the data protection principles, for example by having effective policies and procedures in place.**

3. **Communicating Privacy Information: Employers should review all their data privacy notices and make sure they keep service users fully informed about how their data is used. The current privacy notice is used when personal data is collected, it details the company's identity and how it intends to use the personal information. Under the GDPR there are some additional items - it will need to explain the legal basis for processing the data, the data retention periods and that individuals' have a right to complain to the DPC if they think there is a problem with the way their data is being handled.**
4. **Individuals' Rights: Employers should ensure their procedures cover all the rights individuals are entitled to, including deletion and data portability. Can the company respond appropriately to a request to have personal data deleted and would current systems and procedures help to locate and delete the data?**
5. **Subject Access Requests: Employers should plan how they will handle all requests within the new timeline of one month. There will be different grounds for refusing to comply with subject access requests – unfounded or excessive requests can be charged for or refused. For refusals, policies and procedures must be in place to demonstrate why the request meets these criteria.**
6. **Legal Basis for Processing Personal Data: Is the employer relying on consent, legitimate interests or a legal enactment to collect and process data? The legal basis for processing personal data must be explained in the privacy notice and when a subject access request is answered.**
7. **Consent: Employers should review how they seek, obtain and record consent. Consent must be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes, "opt out" boxes or inactivity. If an individuals' consent to process their data is relied upon, employers must ensure that it meets the standards required by the GDPR. Employers should note that consent must be verifiable and that individuals generally have stronger rights where a company relies on consent to process their data. The GDPR is clear that controllers must be able to demonstrate that consent was given and must review the systems used for recording consent to ensure there is an effective audit trail.**
8. **Children: Although unlikely to arise in an employment relationship, employers should be aware that adequate systems must be in place to verify individual ages or gather consent from guardians. This aspect is likely to be more of an issue for commercial internet services like social networking sites. If a company collects information about children – generally those under 16 years of age, but Member States are given discretion to lower this to 13 years of age – then a parent or guardian's consent will be needed in order to process their personal data lawfully.**
9. **Data Breaches: Is the company ready for mandatory breach reporting? Employers should ensure that they have procedures in place to detect, report and investigate data breaches. The GDPR will bring in a breach notification duty for all companies. Not all breaches will have to be notified to the DPC – only those where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach. In some cases, the individuals whose data has been subject to the breach directly will need to be notified, for example where the breach might leave them open to financial loss. Larger companies will need to develop policies and procedures for managing data breaches. A failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself**
10. **Data Protection by Design and Data Protection Impact Assessments ("DPIA"): A DPIA is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals. It will allow organisations to identify potential privacy issues before they arise, and come up with**

a way to mitigate them. It has always been good practice to adopt privacy by design as a default approach, privacy by design and the minimisation of data have always been implicit requirements of the data protection principles. However, the GDPR will make this an express legal requirement. It is not always necessary to carry out a DPIA – but one is required in high-risk situations, for example where a new technology is being deployed or where a profiling operation is likely to significantly affect individuals.

11. **Data Protection Officers ("DPO"): Will the company be required to designate a DPO? If so, it is important to ensure that the DPO (whether it is someone appointed from within the organisation, or an external data protection advisor) takes proper responsibility for data protection compliance and has the knowledge, support and authority to do so effectively.**
12. **International – the GDPR includes a 'one stop shop' provision which will assist those data controllers whose companies operate in many Member States. Companies should identify where their Main Establishment is located in the EU in order to identify their Lead Supervisory Authority. Companies may also need to review how transfers of personal data outside the EEA will continue to be permitted.**

Conclusion

Owing to the breadth of the GDPR, companies are advised to conduct a review of their existing data protection procedures, to allow sufficient time and resources to affect the necessary changes required to ensure GDPR compliance.

This document is purely for guidance, and does not constitute legal advice or legal analysis. All organisations that process data need to be aware that the General Data Protection Regulation will apply directly to them. The responsibility to become familiar with the Regulation and comply with its provisions from 25th May 2018 onwards therefore lies with the organisation.

The new and expanded rights under the GDPR hugely increase the potential for data protection to be used as a weapon in the context of employment disputes. In future briefings, Aperture Partners will focus on other practical impacts of the GDPR on the employment relationship and what employers and HR professionals can do to manage these risks, and prepare for implementation.

APERTURE
PARTNERS
ADVISORY

About Us

Aperture Partners is a provider of search and advisory services to a diverse client base. Our goal is to develop lasting partnerships, built upon our core values of integrity, honesty and a commitment to excellence. Aperture Partners Advisory provides a wide range of professional employment law and human resource services based on expert knowledge and practical experience.

Aperture Partners Advisory manages risk along the entire employment spectrum, from employee hiring, through to employee exit, being entrusted to manage our clients' most reputationally sensitive and complex employee relations issues. We can provide this exceptional support thanks to our unique balanced practice model, combining real-world human resource guidance, informed by relevant employment law provisions.

Barry trained as a solicitor with Arthur Cox before working with global law firm, Dechert. He is a solicitor member of the Law Society of Ireland, the Dublin Solicitors Bar Association and the Employment Law Association of Ireland. Barry was educated at the National University of Ireland, Galway, the University of London, Trinity College Dublin, the Law Society of Ireland, the Honourable Society of Kings Inns and University College Dublin.
E: bcrushell@aperturepartners.ie

Carmel is a former Group Head of Human Resources where she advised on best practice procedures concerning human resources and employment law issues. Carmel combines commercial acumen with sound advice to guide clients through the rigours of the employment law and human resources process. Carmel has completed a diploma in human resources management and a degree in law, from Dublin Business School. She is currently undertaking her barrister-at-law degree.
E: cbyrne@aperturepartners.ie

3-4 Pembroke Street Upper
Dublin 2
Ireland
+353 (0)1 9053 503
info@aperturepartners.ie

1 Royal Exchange
London
EC3V 3LT
England
+44 (0)20 30538633
info@aperturepartners.ie