GDPR Factsheet – Employer's Overview

New Data Protection Laws – Employer's Overview

Major changes to the UK's data protection laws will come into effect on 25 May 2018. Better known as the GDPR, the General Data Protection Regulations (EU 2016) will bring significant changes and substantial fines for non-compliance, so it is vital that businesses prepare themselves well in advance of the implementation date.

In this brief Q&A guide we consider the key legislative changes relevant to data protection in the context of the employer/employee relationship.

- What is the GDPR?
- Why is the law changing?
- The UK is leaving the EU, will GDPR still apply after Brexit?
- Current employment contracts vs GDPR requirements
- Will we have to draft new employment contracts for everyone?
- Do I have to conduct an audit?
- I own a small business; does this really apply to me?
- I've never conducted a data audit – how do I go about it for GDPR?
- How will I need to present or report my audit results?
- Does GDPR only affect internal data?
- What happens if I decide to do nothing?

Q. What is the GDPR?

A. The General Data Protection Regulation (GDPR (EU 2016) is a new data protection and privacy law replacing legislation in all EU member states; in the UK it will replace the Data Protection Act 1998 (DPA).

Q. Why is the law changing?

A. The idea behind the GDPR is to replace 28 separate sets of EU privacy and data protection legislation with one overarching set of regulations, to create some consistency across the EU and bring the law up to date to reflect the changes in technology which have taken place over recent years. It will incorporate the current DPA, but significantly adds to it with increased rights and responsibilities. The three main aims are:

- to increase the privacy rights and protections for individuals;
- to strengthen the obligations of businesses towards individuals; and
- to greatly increase sanctions for non-compliance.

Q. The UK is leaving the EU, will GDPR still apply after Brexit?

A. Yes, at least for the immediate future. Since the UK is not expected to leave the EU before March 2019, there will be nearly a year after the GDPR comes into effect when we'll still be a member of the EU, and therefore subject to the new requirements.

GDPR Factsheet – Employer's Overview

The Information Commissioner's Office (ICO, the body which oversees data protection laws in the UK) has indicated that the UK will continue to follow the GDPR, or legislation which is broadly equivalent to it, once we leave the EU.

> "I acknowledge that there may still be questions about how the GDPR would work on the UK leaving the EU but this should not distract us from the important task of compliance with the GDPR by 2018"
>
> Elizabeth Denham, UK Information

Q. Current employment contracts vs GDPR requirements

A. Most businesses currently issue employment contracts that include general 'catch-all' clauses, in which employees and workers give consent for their employers to process personal and sensitive data as they deem necessary. Under the GDPR these consent clauses will no longer be valid, so employers will no longer be able to rely on contractual consent clauses for collecting and processing personal and sensitive information.

Instead employers will need to review exactly what data they collect about employees, and justify which classes of data are fundamentally necessary to the employer-employee relationship, and the running of their business. The best way to do this is by data mapping and an audit.

Q. Will we have to draft completely new employment contracts for everyone?

A. Not necessarily. Understandably, the prospect of re-drafting every employee contract in the UK is something that would fill most business managers (and HR) with dismay, so no, this is not a necessary step. The regulations can be met by due diligence exercises and an audit (although putting in place a GDPR-compliant employment contract for new hires moving forward is a good idea).

> Consent for data processing must be "actively and freely given, specifically and on an informed basis" (meaning transparency as to its use), and refusal to give, or withdrawal of, consent must not be "detrimental" to the individual (referred to as the "data subject").

Q. Do I have to conduct a data audit?

A. Ideally **all** businesses should be conducting data-mapping exercises and an audit of their current data in preparation for GDPR, as the regulations apply to **all** data held on EU citizens: suppliers, customers, marketing prospects and third parties, and of course your employees. Some businesses are exempt from full-scale data auditing, but any employer will have to do this. You may find that renewal of any business insurance in the coming months will require your GDPR compliance statement.

GDPR Factsheet – Employer's Overview

Data mapping is a process that shows how data from one information system transfers to another; this can be manual as well as digital. An audit should highlight where and how you hold and manage data that is personal or sensitive, this will cover IT, finance and other business departments – from an HR perspective this includes everything from applicant CVs, background checks, referee details, addresses, contact details, through to banking information for payroll, bonuses, pension, tax codes and NI numbers and any historical information about sickness absences, occupational health, and performance tracking.

Q. I own a small business; does this really apply to me?

A. The short answer is yes – the new regulations apply to all EU citizens and to all businesses who work with, employ, trade with or otherwise process EU citizen's data, even sole traders and micro businesses. The GDPR will have global reach and effect, so the implications and responsibilities cannot be avoided.

The General Data Protection Regulations are the single most important update to EU privacy laws in the last 20 years

Q. I've never conducted a data audit - how do I go about it for GDPR?

A. Relax, it isn't as hard as it sounds, and we can help you get started or assist with the audit and reporting. We have a range of factsheets to help you get to grips with what needs to be done, and we can support you every step of the way.

Once you start considering what data you use on a regular basis (ideally through a data-mapping exercise) you can then look at the specific and necessary grounds you have for processing this data – there are several laid out under the GDPR:

- for the performance of the employee's employment contract;
- for compliance with a legal obligation that the employer is subject to;
- to protect the wellbeing and interests of the employee, or another individual;
- for a task carried out in the public interest or in the exercise of official authority held by the employer; and
- for the legitimate interests of the employer or a third party (except where the interests or rights of the employee override them).

After auditing, you can then issue a statement to employees and workers outlining the business justifications for processing their personal and sensitive data, in line with GDPR requirements. Follow on audits on a regular basis will be much easier once the initial work is done.

Q. How will I need to present or report my audit results?

A. As mentioned above, there are several scenarios where employers can state legitimate interest in processing

employee's personal data. You will need to spell out the rights of individuals, such as the right to withdraw consent to data processing and lodge a complaint with the ICO; clarifying their rights and how the business is meeting its obligations is a key foundation of the GDPR.

The notice you issue needs to specify the purpose and legal basis for processing each category of personal data, including how personal and sensitive data is managed and stored, the security of that storage, who has access and why, for how long the data will be held, how it will be destroyed upon expiry of usefulness, and whether data is also shared and processed through third parties (such as through payroll providers, and pension schemes) to name a few.

GDPR extends to other business practices you may take for granted (with the legitimate aim of protecting company systems and information), including recruitment advertising, CV screening and background checks, monitoring company email systems, and use of company IT tools for personal use

Your data-mapping and audit will highlight the impact other policies and practices, which may need reviewing, redrafting to comply with the regulations, and recommunicating to employees (such as communicating to applicants how long you'll keep their CVs on file, any BYOD practices, use of company laptops and phones, remote and homeworking etc.).

Q. Does GDPR affect only internal data?

A. No – as mentioned, the GDPR covers all data held on EU citizens, which likely includes all of your suppliers, customers, marketing prospects and third parties, not just your employees. Your audit will need to consider the data protection and privacy responsibilities you place on employees and workers when handling sensitive and confidential information in their roles.

Standard privacy and confidentiality clauses aimed at protecting the business will therefore also need to be reviewed and updated, as will your statements about how you will manage data for external parties, especially if you list these policies or clauses in supplier and third party contracts or on your corporate website. You may have noticed some of your suppliers are already taking similar preparatory steps.

Third party data processing and liability also comes under scrutiny of the GDPR, so your audit should capture all suppliers and third parties.
See our factsheet on data-mapping and audit and checklists for more information.

Q. What happens if I do nothing?

A. After 25 May 2018, non-compliant businesses could face severe fines of up to €20 million or 4% of turnover, whichever is higher (as opposed to the maximum fine available under the current Data Protection

Act of £500,000). Fines to businesses for breaching DPA regulations usually only came after complaints were raised to the ICO, or following employment tribunal cases. Moving forward under GDPR, the increased rights for individuals to hold businesses and employers to account directly (rather than through complaints to bodies like the ICO), mean the regulations will be **actively** monitored for breaches. It is highly likely that we will see these increased employee rights being used in the context of employment disputes.

The actual level of fines will vary according to the severity of the breach, but given the potential for high penalties it is important that all employers should be focusing on data protection preparation now rather than after the legislation comes into effect.

In Summary

The GDPR has been in the pipeline for a long time, and arguably impacts micro, small and medium businesses more than larger companies with staff and departments to share the administrative burden. Sphere HR are uniquely placed to help you review your business data sources and prepare for the GDPR in a timely fashion – contact us for a free initial discussion: www.spherehr.co.uk/get-in-touch

Visit www.spherehr.co.uk/free-stuff to download more factsheets and checklists.

More Information

The Information Commissioner's Office overview of the GDPR:
https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

The EU's GDPR portal: http://www.eugdpr.org/

BBC News article on the Queen's Speech, July 2017:
http://www.bbc.co.uk/news/technology-40353424

The Guardian Small Business Network news article, February 2016:
https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses

Small Business news article, June 2017:
http://smallbusiness.co.uk/risk-huge-fines-gdpr-2539289/