CIPHR

ALL ABOUT PEOPLE

Introducing the GDPR

Will your HR department be ready?

Contents

4 SECTION 1 - What is the GDPR and how will it affect the HR department?

11 SECTION 2 - What do I need to know?

13 SECTION 3 - What can I do to prepare?

SECTION 1

What is the GDPR and how will it affect the HR department?

Introduction

If you handle personal data you'll need to know about the GDPR and what impact it will have on your organisation.

The General Data Protection Regulation (GDPR) is new EU legislation that reforms laws regarding the handling of personal data and **will come into effect in the UK from 25th May 2018.**

The introduction of the GDPR significantly raises the bar for personal data privacy and most organisations will have to examine and determine how they collect, store, manage and protect personal data in order to comply with the GDPR.

For those that don't comply, the penalties are severe. Fines can be as high as 20 million Euros for serious violations of the GDPR, or 4% of a company's global turnover, whichever is greater.

The severity of these fines is a sign of how seriously the GDPR should be taken. Companies will need to review current practices and make necessary changes to how they handle their employee data. A large proportion of those resulting changes will impact directly on HR departments so it's imperative that you understand what the GDPR means for you.

This guide will help you think about the things your business needs to consider and practical steps you can take to prepare for the introduction of the GDPR next May.

Why is this such a big deal for HR?

The reason GDPR is such a widespread topic of discussion at the moment is that **it will fundamentally change how organisations can handle personal data**, including their employee's personal data. The main changes are around access, rectification, deletion and transfer rights, as well as new requirements around reporting a data breach.

The GDPR is designed to strengthen the rights of individuals in the EU and becomes more prescriptive about the collection and storage of personal data and how it will be used.

For those working in HR, this means a rethink about how personal data is collected, used and retained. Data protection issues have an impact on most HR activities from handling recruitment and employer references, to how employee performance is monitored and how employee records are handled before, during and after employment.

Will the GDPR affect my organisation and HR department?

With few exceptions, yes.

The GDPR applies to the personal data of individuals in the EU, held by an organisation, including personal data of an organisation's employees, leavers and job applicants.

What does it mean by ‘personal data’?

The current definition defines personal data as **‘any information relating to an identified or identifiable natural person’**[1] so this includes ‘direct identification’ (for example, the name of an employee) or ‘indirect identification’ (for example, any other information that could identify them such as their job description or title).

Be aware, though, the GDPR makes changes to the concept of what constitutes personal data in several ways, for instance it now includes online identifiers and location data which now means IP addresses, mobile device ID's and such like are all officially classed as personal data, even if it has been encrypted.

[1] http://www.privacy-regulation.eu/en/4.htm

What happens if we don't comply or if there's a breach?

GDPR is serious about strengthening the rights of individuals in the EU and the level of financial penalties demonstrates just how seriously governments are taking this.

At the moment, the ICO (Information Commissioner's Office) can apply fines of up to £500,000 for contraventions of the Data Protection Act.

Under the new GDPR, this will rise to 10 million euros or 2% of global turnover (whichever is greater) for lesser incidents and 20 million euros or 4% of global turnover for serious violations.

The GDPR also introduces a new accountability principle which makes it your responsibility not just to comply with the principles, but to **demonstrate that you comply** with the principles.

How does the GDPR differ from current regulations?

The GDPR will update many of the broad principles already in place in the Data Protection Act.

Among other changes the GDPR will:

- **Implement more stringent controls of what constitutes unambiguous, informed 'consent'.** Consent cannot be "assumed" and can be freely withdrawn.
- **Provide enhanced rights for data subjects** such as rights of data erasure, correction of inaccurate data, removal from digital marketing, rights to request transfer of personal data to another service provider and the right to be notified of data breaches in certain circumstances.
- **Introduce new accountability measures** including conducting privacy impact assessments, and appointing data privacy officers in certain circumstances.
- **Require organisations to report data breaches to the Information Commissioner's Office** (ICO) within 72 hours if a breach may risk the rights and freedom of individuals.

SECTION 2

What do I need to know?

GDPR privacy principles

The principles of the GDPR are as follows:

Article 5 of the GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals.

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

SECTION 3

What can I do to prepare?

As an HR professional, many of the regulations within the GDPR will apply to your organisation and your work but there are practical steps you can take to prepare for the GDPR coming into force.

Here are 10 suggestions, although by no means definitive, of things you can do to prepare for the GDPR before May 2018.

1 Start the Discussion

Regulations are likely to impact several areas of your business and you need to raise awareness not just of the oncoming implementation but also the seriousness of any breaches or non-compliance.

2 Assess your Current Compliance

Use the opportunity to assess and discuss where you are with compliance currently and identify any new requirements from the GDPR that will impact your own situation. You will need to examine how and where you use the personal data you collect and audit how you store and track that data.

3 Review Privacy Notices and Policies

Take the time between now and next May to **review how easily understood your current privacy notices are** and update them to include the additional information and more stringent regulations of the GDPR.

Review your current data protection policies and practices including existing employment contracts, staff handbooks and employee policies.

4 Educate Yourself on the Requirements

Make sure you study and fully understand the more detailed regulations. As an HR professional, you may need to make sure the relevant people within your organisation have received the training they require to understand the new laws.

5 Consider Consent

The GDPR states that consent from the individual needs to be freely given, specific, informed and unambiguous. It also requires some form of affirmative action, so pre-ticked boxes, silence or inactivity doesn't constitute consent. It also needs to be verifiable so you need to think about how you will keep records of how and when consent was given.

6 Put Processes in Place

The GDPR accountability principle requires you to show how you comply with the principles. You will need to maintain relevant documentation on processing activities and decide who will do this within your team.

7 Be Ready to Respond Swiftly

You will need to be ready to respond quickly and you should update your procedures now to make sure you can handle the requests for access to, correction or deletion of personal data within the shorter one month timescale.

8 Consider Appointing a Data Protection Officer

All public authorities and those private companies involved in regular monitoring or large-scale processing of sensitive data **will need to appoint a Data Protection Officer** to advise on GDPR obligations, monitor compliance and liaise with the data protection authority.

9 Develop a Data Breach Response Programme

Data breaches under the GDPR are treated very seriously. You will need to have a fast-moving internal breach reporting procedure in place.

It's a good idea to develop a Data Breach Response Programme to make sure members of your team notify you promptly and that you, or the person responsible, notifies the relevant authorities within 72 hours.

10 Consider a Self-Service System

The ICO provides a best practice recommendation that organisations should try to give remote access to a secure self-service system to give the individual direct access to their own information. **Self-service functionality provides transparency and enables individuals to ensure data accuracy.**[2]

[2] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-of-access/?q=best+practice

How CIPHR can help

Using CIPHR's SaaS HR system, **employees can access and update their own personal information via a secure self-service portal**. CIPHR also includes tools that will help you to document when consent from employees was granted for processing personal data. Furthermore, CIPHR has strict policies, procedures and security systems in place which are designed to ensure that **our client's data remains secure**.

If you currently use spreadsheets and documents to store employee data, you may find it difficult to comply or demonstrate compliance with the GDPR so you'll need to think about how you may need to do things differently.

The arrival of more stringent regulations may be a wakeup call for many HR professionals to review how they currently store and organise their employee data.

To see how a secure, self-service HR system can help your organisation to comply with the GDPR **call CIPHR** on **01628 814 242** or visit **www.ciphr.com** now.

CIPHR

ALL ABOUT PEOPLE

Abbey House
28 – 30 Chapel St
Marlow
Bucks
SL7 1DD
01628 814 242
info@ciphr.com
www.ciphr.com

To see how CIPHR's secure, self-service HR system can help your organisation to comply with the GDPR **call 01628 814 242 or email info@ciphr.com**