people & business

KeystoneHR

GDPR – When it comes to information about your employees, are you ready?

With just over 3 months to go until the changes to current Data Protection law (GDPR or General Data Protection Regulations) come in to force this practical summary will help you prepare and ensure that you are compliant when it comes to processing and retaining your HR related data.

What is GDPR?

In case you need a recap the GDPR is part of the EU Data Protection Regulation and it will replace the existing Data Protection Directive. The aim of the new regulation is to standardise and strengthen the rights of European citizens to data privacy. This means that any organisation that deals with people's private data must meet new standards of transparency, security and accountability.

The onus is on data controllers (employers) and processors (HR) to identify potential compliance issues within their Company, to analyse the private data that is currently being held, and to review the consent procedures by which employees agree to the processing and retention of their personal data.

Whilst the following steps focus on the data you hold in relation to your employees (past, present and future), don't forget GDPR also applies to data you may hold about your customers, suppliers, contractors etc. so you will also need to ensure you follow appropriate processes for these groups.

As an Employer, what does this mean for you?

Consent

At the moment, when we process HR related data, we usually rely on a clause in a Contract of Employment that provides consent to do so. Under GDPR we can no longer rely on this as consent must be 'freely given, informed, specific and explicit'. Whilst consent will still be required for certain data such as for Occupational Health referrals, going forward you will need to clearly set out the lawful grounds for processing personal data, such as a legal obligation, the performance of a contract or other legitimate interests.

Subject Access Data Requests

Whilst there is no change in the right employees have to request to see the data their employer is holding about them, under GDPR the data now has to be provided within one month – and you will no longer be able to make a charge for providing it. All the media and information around GDPR may well lead to increased employee awareness of the right to request the data held about them so it is important to be prepared for such requests. Additionally, if the accuracy of the personal data is contested by the employee, it can only be processed with the employee's consent, which could potentially hold up performance management or change management processes.

people & business

KeystoneHR

Information at the point of data collection

Under GDPR, you will need to provide more information to people about how their data will be processed at the time you collect it, and if data is then processed for a new purpose the employee must be notified again.

Data Impact Assessments

Where a type of processing, in particular using new technologies, is likely to result in high risk to the rights and freedoms of employees, it will be necessary to carry out an assessment of its impact on the protection of personal data e.g. mobile monitoring

Data Breaches

If your employee data is subject to a data breach, IT related or otherwise, you must now pro-actively report this to the ICO (Information Commissioner's Office). You will also need to have a process in place to ensure that this happens.

Claims

GDPR will make it easier for individuals to bring claims against employers in the event of a data breach – and receive financial compensation for loss or hurt feelings. At the same time, fines against companies for non-compliance will be much higher than under current data protection legislation.

GDPR will make it easier for individuals to bring claims against employers in the event of a data breach – and receive financial compensation for loss or hurt feelings.

Next steps

Whilst compliance with the GDPR may seem like a daunting prospect, it is important that you start planning for this as soon as possible. So, here are our key steps to help get you started:

Step 1
Conduct an audit

- What information do you hold e.g. name, address of employees?
- Where did it come from e.g. employee application form/new starter form?
- Why you hold it e.g. you need employee's information for payroll
- Who do you share it with e.g. the employee's manager?
- Is it shared with any third party data processors e.g. payroll provider?
- How long to you currently retain the data?

Step 2
Issue 'Privacy Notices'

Employees need to be told:

- why their personal data is being held
- the legal basis for doing so
- the company's retention policy
- their right to make a complaint to the ICO
- their right to make a subject access request.

This information needs to be detailed in a straightforward and simple 'privacy notice' and given to all employees.

people & business

KeystoneHR

Step 3
Updated Contracts of Employment and other HR polices

Employers will need to have a revised data protection clause in their contracts. This will serve as a notification to employees that they must comply with the company's policies in relation to data protection and will notify them that full details about the data that the company is processing about them, is contained in the Privacy Notice (see step 2).

Other policies they will need updating or drafting include:

- Recruitment policy
- Data retention and disposal policy
- Access Requests policy
- Personal Data Breach Notification and Response Plan
- Disciplinary policy
- IT security policy

Step 4
Training for employees

Ensure employees understand their obligations in relation to data projection including

- Changes to any existing policies and procedures
- What GDPR is and how it impacts on their day to day work
- What they need to do to comply with the requirements of GDPR
- How to report a breach

There has been a lot of talk about GDPR and the huge potential fines that can be imposed for GDPR breaches and whilst there is no expectation that businesses will achieve perfection from day 1 it is important that you do take appropriate steps to ensure compliance and understand what data you hold on your employees (past, current and future candidates) and what legitimate reason you have for dealing with/ retaining that item of data.

KeystoneHR and people & business have teamed up to create a GDPR HR Toolkit for Employers which will include:

- A template audit pro forma with clear guidance notes
- Guidance on Privacy notice and data protection policy
- Guidance on what other HR policies/documents need to be updated e.g. Contracts of employment, recruitment policy, use of CCTV etc
- A PowerPoint presentation to support the training of employees
- One hour of telephone/email support to answer queries

If required, we can support you to carry out the audit of your current HR data and advise on what actions you need to take in order to become compliant.

If you would like further details, please do not hesitate to contact us

- Debbie at people & business: **07801 443880** | **dtaylor@peopleandbusiness.co.uk**
- Jo at KeystoneHR: **07866 487673** | **jo@keystonehr.co.uk**