HR & GDPR

People

KEYSTONE LAW

HR Checklist for GDPR compliance

This checklist will cover the main areas you need to address to prepare for the GDPR (General Data Protection Regulation) which comes into force on May 25th, 2018.

People

People is a web-based human resources management system that helps progressive HR professionals make better decisions, engage their workforce, and deliver high-impact results that influence your organisation's success. Thousands of companies rely on People to handle essential HR tasks such as recruitment, performance and holiday management. But beyond helping you work more efficiently than you can with spreadsheets, paper files and email, People also helps make your work more meaningful. Built-in advice based on HR best practice shows you a clear path for your HR processes, while heat maps, alerts and reminders support good judgement calls in areas such as absence and attendance.

Visual, clutter-free and easy to pick up, People automates the tasks you hate, and draws your attention to the areas of HR that will make the biggest difference, helping you boost business growth and master your career. Your journey with People begins with a proven implementation process that safely moves your data into its new home, and continues with expert support, every step of the way, from a friendly team of experts.

Modern and mobile, everybody in your workforce will find it easy to manage their own routine tasks from anywhere in the world, and you'll make a big impression at every level of business – from giving front-line employees a holiday booking system that makes sense, to showing your board-level directors the impact HR has on their bottom line.

KEYSTONE LAW

Born from a passion for innovation and a desire to create something better, Keystone was established with one mission, to provide clients with dedicated legal advice delivered by experienced lawyers at competitive rates. The business proposition was twofold. Invest in technology, to form a business that could operate seamlessly, minus the added overheads often found in the traditional law firm and without the need for a high volume of support staff - all of which usually result in added expense for the client. Appoint lawyers who combine in-depth legal knowledge, client empathy and an entrepreneurial spirit.

Our original business model makes us an ideal choice for companies both large and small, and our commitment to building strong relationships has resulted in many household names investing in us as their trusted adviser. Meanwhile, the flexible and agile offering that we maintain enables us to cater for a wealth of private clients.

We are proud to offer clients a 250-strong lawyer offering across nine key locations. Our team is a carefully curated group of individuals who average 23 years' post-qualification experience. Some have built their careers at some of the UK's most established firms; others have cut their professional teeth in-house at major multinationals. Whatever the background, our advisers are always loyal to the Keystone culture. And at the heart of the culture is the priority that we place on each client and their individual needs.

FOR FURTHER INFORMATION

RACHEL TOZER

Consultant Solicitor

Rachel is an employment lawyer who advises UK and international clients on all aspects of UK employment law from tribunal claims, business reorganisations and transactions to day-to-day HR advice. Rachel has co-authored a book explaining the current data protection laws and best practice to employers and is busy helping several employers prepare for GDPR.

T: 020 3319 3700
E: rachel.tozer@keystonelaw.co.uk

Checklist

1. Raise awareness

A recent survey has found that a quarter of businesses in London are entirely unaware of the new law and only 16% are prepared for it. GDPR is not an HR issue alone. Your business' Board of Directors should be fully engaged with preparing the whole business for this change.

2. Nominate a data protection officer/privacy manager

Not all employers have to appoint an official data protection officer, but all businesses will need to assign responsibility for data protection compliance to an individual/team of appropriate people.

If the person responsible for protecting HR data in your company isn't you, make sure your data protection officer/privacy manager sees a copy of this checklist.

SME's (Small – Medium Enterprises) might find they don't have the resources to allocate one person sufficient time to cover all of the businesses' data protection needs. You might find it easier to delegate data protection responsibility by department or get specialist advice on how to manage GDPR in your businesses, but there will need to be an overall plan.

3. Create a data log

Consider what data you process, and create a log demonstrating the following. This will help you to show GDPR compliance and that you proactively protect data in an easily audited manner.

- The type of data (e.g. personal, or special personal (which used to be called sensitive))
- The categories of data (e.g. recruitment information, bank details, performance information, absence details)
- Who the data concerns (e.g. employees, next of kin, applicants, etc.)
- Who has provided the data to you (e.g. the applicant/employee themselves, credit reference agencies, other employees)
- What legal basis you have to process (e.g. to perform the employment contract, complying with a legal requirement or legitimate interests (you need to identify which interest you are relying on and balance it against the

individual's rights and freedoms)? Also remember that consent will rarely be valid in an employment context under the GDPR. What additional legal right do you have to process special data (e.g. complying with employment law or assessing the working capacity of an employee)?)

- The purpose of processing (e.g. to pay the employee, to report salary information to HMRC, to manage performance)
- Where the data will be stored and who has access to the data (e.g. digitally in HR software which only HR can access)
- Data transfers: (if this is a regular occurrence, you may need a separate log). You should also include any events of data being transferred, including:
    - *who data was transferred to*,
    - *when it was transferred*,
    - *where they are storing it*,
    - *and how you transferred the data*.
    - *whether you are transferring any personal data outside of the EU and if so what protections are in place*
- When data will be deleted (e.g. a period of time after an unsuccessful application/after the employee leaves)
- Whether you carry out any automatic decision making or profiling (e.g. electronic recruitment sifting based on academic achievements, psychometric testing)
- Whether you need to carry out a data protection impact assessment and when you are likely to need to do so in the future (e.g. due to the fact that you carry out or will carry out high risk processing or will be introducing new technology)
- How you respond to data breaches

4. Check your IT infrastructure allows you to be compliant

Your IT infrastructure will be highly relevant to two main themes in terms of GDPR compliance – security and employees' rights.

Security issues:

- Is the IT system secure? - GDPR states data protection should be by design and default i.e. it should be part of project planning from the outset not an afterthought.
- You should consider using a password policy for employees, and/or two-factor-authentication.
- A single sign on policy for your employees may be useful.
- The relevant level of encryption should be deployed on all company devices.
- Is all your HR data really only stored in HR? Do managers keep their own records? How are such records secured?
- Don't forget about hard copy documents – think about data which is taken out of the office whether to external meetings, to employees' homes or customers' sites. Is that necessary and if so how will you ensure it is kept secure?

Employee rights:

- Do your automated decision-making processes allow you to deal with objections and involve a human decision maker if requested?
- Can you easily search for all data relating to a particular individual? This will make responding to subject access requests much easier.
- Can you restrict data so that it is merely held but not otherwise processed? This will be necessary in some situations.
- What processes do you have for an employee to exercise their right of objection?
- How do you ensure that the data you are holding is up to date and accurate?
- How will you achieve the deletion of personal data, across the business, at an employee's request in relevant situations?
- Can you export data from your system? .csv, .pdf, or .txt files are regularly accepted formats. This will allow you to manage the portability (i.e. transfer) of the data to the employee or to a future employer at their request.

There is another potential important question – where are the servers housed? If you store data on servers which are situated outside of the EU, you are transferring data outside of the EU and need to ensure adequate protection is in place.

5. Update data protection policies and employment contracts

You will need to update your data protection policies and inform your employees at every level of the business of any changes you make. You should communicate the changes in plain language. Five key policies to update include:

- Privacy notice to staff: this needs to tell your employees the types of data which you hold about them, your lawful ground for processing it, the purposes for which you will process it, and their rights with respect to their data.
- Data protection policy: this should set out the business' commitment to data protection and tell employees about their obligations relating to personal data which they will process in their roles. This will include security measures.
- Data breach reporting policy: you should have a comprehensive plan in place that follows the ICO guidelines for breach reporting. This needs to meet particular time frames and include all the relevant parties.
- Subject access policy: ensure you have the means to meet subject access requests in the specified time frame and are able to provide all the relevant data.
- Data retention policy: ensure you analyse how long you need to keep data and that it is then securely destroyed after the specified retention period.
- Other policies will also need updating (e.g. disciplinary policy)

Data protection clauses in employment contracts and individual contractor agreements will need to be changed so that they no longer seek to rely on consent as the lawful ground for processing.

6. Ensure staff have the correct training

Make sure all your employees receive an adequate level of training for handling personal data, specific to their job role. They must be informed of the correct policies and procedures. Training needs to be refreshed on a regular basis and you need to keep records of the training provided.

7. Health-check relationships with other group companies, other businesses, or services

- Check in with your HR software provider

Similar to your IT infrastructure, you need to check if the software you are using allows data access, restriction, objection and portability. If not, you may need to consider another provider. Before you do so you will need to undertake a data protection impact assessment. If you aren't using HR Software, you still need to be able to ensure the same individual rights are upheld.

- Check in with recruiting agencies/benefit providers/outsourced service providers

It is important any other entities with whom you share personal data also have stringent data protection policies in place and only process the personal data which you provide in accordance with your instructions. For example, if you use a recruiting agency to source your staff, then you need to find a secure way of sharing applicant information. You should ensure that all contracts with external providers (e.g. outsourced payroll services, pension providers, life assurance and private medical insurance companies) all contain adequate data protection obligations.

- Check in with group companies

Parent companies, where ever they are based in the world, often like to receive reports from their subsidiaries which often contain personal data. First, you need to assess whether there is a lawful reason to share this information. Secondly, you need to consider where your group companies are based – are they outside the EU? If so you can only transfer personal data if there is sufficient protection in place (such as the Privacy Shield with respect to US companies, a European Commission decision which confirms that the laws of the country are sufficient, or particular contractual clauses entered into between group companies).

This checklist is for general information purposes only and does not constitute legal or professional advice. It should not be used as a substitute for legal advice relating to your particular circumstances. Please note that, at the date this checklist has been prepared, the Information Commissioner has not yet published all of her Guidance relating to the GDPR.