An employers HR guide to GDPR.

The impact of GDPR on how businesses handle employee data and ways to stay compliant.

An introduction to GDPR

The General Data Protection Regulation, otherwise known as GDPR, was enforced on 25th May 2018 by the European Union (EU).

The aim of this new regulation is to improve the rights and security of European citizens' data. Any business who handles data must meet the strict standards of the new regulation. This includes being transparent, secure and accountable.

These regulations apply to any form of data connecting to employees, such as photos, names, address, bank details, email address, medical records or personal information.

Naturally, this stipulation has raised a few concerns among business owners. In essence, these stricter regulations have made it trickier to market and communicate to potential prospects, as well as introducing more steps in the HR process.

This stems from the whole key principle of responsibility being pushed on employers and HR teams – aka the data controllers and processors. GDPR means both the data controllers and processors are accountable for raising and identifying any compliance issues within their own business.

Furthermore, they are also responsible for analysing the private data held by the business and reviewing the consent procedures by potential customers and their own employees.

Yet despite the importance of GDPR, research reveals that 48% of consumers and employees still aren't sure where and how businesses use their personal data. This figure has risen from 31% when the same survey was conducted in 2016.

It was also discovered that just 16% of people agree that technology platforms treat personal data in an honest and transparent way.

On the other side of the coin, a vast number of businesses are also struggling to establish a firm grip on GDPR too, with 45% of them openly admitting that they are setting money aside in case of any potential fines.

Prior to GDPR becoming active, just 26% of business owners said they felt confident that they had the right procedures in place to be classed as compliant before the deadline. In fact, 61% of marketers said that they'd apply for a date extension if they could.

These findings are startling when you consider how detrimental GDPR could be to the longevity of a business.

What happens if a business doesn't comply with the new regulations?

Currently, the official GDPR website states that if an organisation fails to comply with the regulations, there will be "heavy fines".

To put this into numerical terms, a business could be fined up to 4% of their annual global turnover or €20 million – whichever is the greater sum. This would occur for major offences like not having consent for the data on file.

Alternatively, businesses can face a smaller fine of 2% of their annual global turnover for simply not keeping their records organised, failing to report a breach or not carrying out impact assessments.

The role of GDPR specifically in HR departments

While there are numerous implications for business' marketing and sales department, GDPR has also changed the way HR works within an organisation.

Similarly to handling customer data, employers are responsible for getting their employees to consent to the usage of their personal information.

It's significantly changed the face of subject access requests (SARs). SARs are used as leverage in employment disputes in demonstrating how an employee's data is being held.

GDPR has enhanced employees' rights to gain clear access to personal data from their employees and learn how it's being used and processed.

By having secure and compliant processes in place, this will reduce the time needed for employers to find and respond to a SAR. Previously, businesses had 40 days to comply with a SAR request, but now they have up to 30 days. However, this can be extended for a further two months if the case is particularly complex.

As a safety protocol, employers should draft template letters and conduct assessments to see how quickly they can access an employee's data. It's also highly recommended that HR staff are all trained around the subject so they know the legal implications and processes to complete the request quickly and lawfully. See 'Informing employees on GDPR' for more information on how to do this. (Top tip.)

The three principles to stay compliant

Head of content at XpertHR Group, Jo Stubbs, said: “The new GDPR means employers need to rethink how personal data is collected, used and kept.”

Before addressing the way a business’ HR team collect, use and keep employees’ data, it’s vital to understand the processes used before 25th May 2018. The implementation of GDPR doesn’t act as a clean slate, an employer needs to go back and review any data they had previously attained.

1. Firstly, an employer/HR team should review the data they have on file of current employees and assess the reason for having it. Any unnecessary or irrelevant data should be discarded.
2. Next, employers should look at employee data flows, where it’s stored and establish how many years it dates back to. For instance, there’s no need for a business to still have an employee’s information who left to pastures new over ten years ago.
3. Finally, employers should look at the current data protection policies and processes used to see whether they adhere to the new regulations. This includes contracts, documents and the HR system used.

How to rightfully collect employees’ data

According to the new accountability principles, an employer must give their employees a clear and lawful purpose from the beginning. Their exact wording is; GDPR lawful purposes for ordinary personal data include processing on the basis of:

- legitimate interest of the data controller;
- the necessity for the performance of a contract;
- compliance with a legal obligation;
- protecting the vital interests of the data subject or of another natural person; or
- the necessity for the performance of a task carried out in the public interest.

Employees need to make sure that their employees have opted in (this should be separate from the terms and conditions of their employment) and clearly understand what their data is being used for before consenting.

If an employer wishes to share their data with third-party companies, every business should be clearly labelled and the employee has a choice in the matter.

Employers should also advise from the start that consent may be withdrawn and state exactly how this would be carried out. All records of consent should be securely kept to show that the business is compliant.

How to use employees’ data

Once an employer states how they wish to use an employee’s data, they cannot then use it for other purposes.

GDPR is about being transparent and forthright with their employees.

However, there are more specific examples of data usage. For example, if an employer wishes to carry out a criminal record check, under GDPR, they can only do so if it's specifically authorised by law. To put this into context, a Disclosure and Barring Service Check might be needed for a position working with vulnerable adults and children.

However, this area is evolving and GDPR has enabled governments to take their own stance on the rule. Therefore, employers should keep an eye out on this as it progresses. Anecdotally, employers in the UK will more often than not still be able to carry out criminal record checks in most circumstances.

How to keep employees' data

All employers must identify an alternative legal basis for the processing of the data to safeguard it against a breach. It should also be kept up to date, therefore, it's beneficial to the welfare of the business to carry out routine checks to ensure all employees' information is correct.

A copy of the data held must be accessible on demand by employees and they also have the right to delete or block it in particular circumstances.

It's also worth remembering that employers should never keep personal data on file for longer than required.

Should a business find a discrepancy or any data breach, cases must be reported to the DPA within 72 hours. Any employee impacted by the breach needs to be notified immediately.

This is why it's of paramount importance for a business to review the current security processes in place. Does the HR system follow the rules of the regulation? Is it safe and secure?

The system should be robust and minimise the likelihood of personal employee data being accessed, lost, deleted or damaged unlawfully.

For best practice, employers may want to consider creating data privacy notices to inform their current and future employees about the process of their personal data. This will give them a clear and transparent overview of how their data will be kept. (Top tip)

Informing employees on GDPR

GDPR may already be in place, but businesses shouldn't be afraid to address their employees on the matter. A lot of the emphasis on the matter has been based around the impact on marketing and selling to potential customers.

However, there might be some confusion or lack of resource on the way they will be directly affected. After all, their data is just as important as a customer.

While running a professional training programme is one of the most thorough ways to tackle the topic, it might not be affordable or worthwhile for many smaller businesses.

Instead, it's worth creating some resources for every employee to keep and carry out a team meeting.

Here are some key areas to include:

- ✓ **What employee data will and has been processed** – including what's relevant and discarded.
- ✓ **Why an employer needs to process their data** – the details on GDPR and the impact it can have on the business.
- ✓ **How employees' data will be processed** – including whether it will be passed to any third-party companies or if it'll be moved outside of the European Economic Area (EEA).
- ✓ **What data the business will store** – address which information is needed and where it will be stored.
- ✓ **The process should they have any objections** – if an employee doesn't wish to have their data stored or processed, the employer should tell them how to tackle this and how the procedure works following the objection.
- ✓ **Who employees should get in touch with to make changes to their data** – depending on the size of a business, this will either be the HR department or manager.
- ✓ **How employees can access their data** – this depends on what software a business has in place. Some allow employees to access it online or via an app. While others may have to request it. In this particular case, it's important to be able to access an employee's data quickly on request.
- ✓ **Security risks employees should be aware of** – giving employees a broader understanding will give a business more sets of eyes to spot any discrepancies. This will enable them to report or amend the issues immediately. It's also worth mentioning who employees should inform if they notice any breaches.
- ✓ **The consequences of a breach** – include the financial implications and the impact it will have on the business' future. This may help employees understand the severity of GDPR.

Conclusion

While GDPR may be viewed as a hindrance to the way an HR department operates within a workplace, it can also have a positive impact on how employees view their employers as they are being more responsible.

As a rule of thumb, businesses should stay up to date with current developments to ensure they remain compliant. In some cases, hiring a compliance officer might be worthwhile, or promoting someone in-house to fulfil the role. This way, a business can become more robust and adaptable should any major changes occur.

The next consideration is software. A security breach of both customer and employee data can land a business a considerable 4% cut from their annual global turnover or €20 million fine. Investing in a secure HR system or app could feel like another cost, but in the long-run, it could save a company's reputation, profits and future existence.

About Flexr

Flexr is the 'game changing' employment management platform that redefines the engagement between employers and employees.

Since early 2018, they've revolutionised the way SMEs around the world operate their HR departments, introducing enhanced transparency between employees and employers while creating better working relationships.

Their platform is easily accessible through a smartphone app, online desktop portal and call centre.

For more information, visit www.flexr.com.

Sources

https://www.peoplemanagement.co.uk/experts/legal/what-hr-needs-to-know-about-GDPR

https://www.corehr.com/blog/gdpr-general-data-protection-regulation-everything-every-hr-leaders-needs-know/

http://plaintalkinghr.com/blog/gdpr-and-employee-data-are-your-hr-processes-compliant/

https://www.analyticsinhr.com/blog/general-data-protection-regulation-gdpr-impact-hr-analytics/

https://www.marketingweek.com/2018/05/28/gdpr-inflation-retail-sales-5-killer-stats-to-start-your-week/

https://www.econsultancy.com/blog/70031-the-best-gdpr-stats-surveys-we-ve-seen

http://smallbusiness.co.uk/ten-things-employers-need-know-gdpr-2541681/

https://www.ensighten.com/company/newsroom/almost-half-of-uk-marketers-are-setting-money-aside-for-gdpr-fines-amid-pre-deadline-jitters/

https://www.peoplehr.com/blog/index.php/2018/01/26/10-things-to-tell-your-employees-about-gdpr/