GDPR FOR HR

SIX STEPS TO GDPR-READINESS

Preface

The General Data Protection Regulation (GDPR) is the new legal framework that will come into effect on the 25th of May 2018 in the European Union. EU regulations have direct effect in all EU member states, meaning the GDPR replaces the current Data Protection Directive and applies to all EU member states.

The GDPR's focus is the protection of personal data. In fact, GDPR is one of the biggest shake-ups ever seen affecting how data relating to an individual should be handled—and it affects not just companies but any individual, corporation, public authority, agency or other body that processes the personal data of individuals based in the EU.

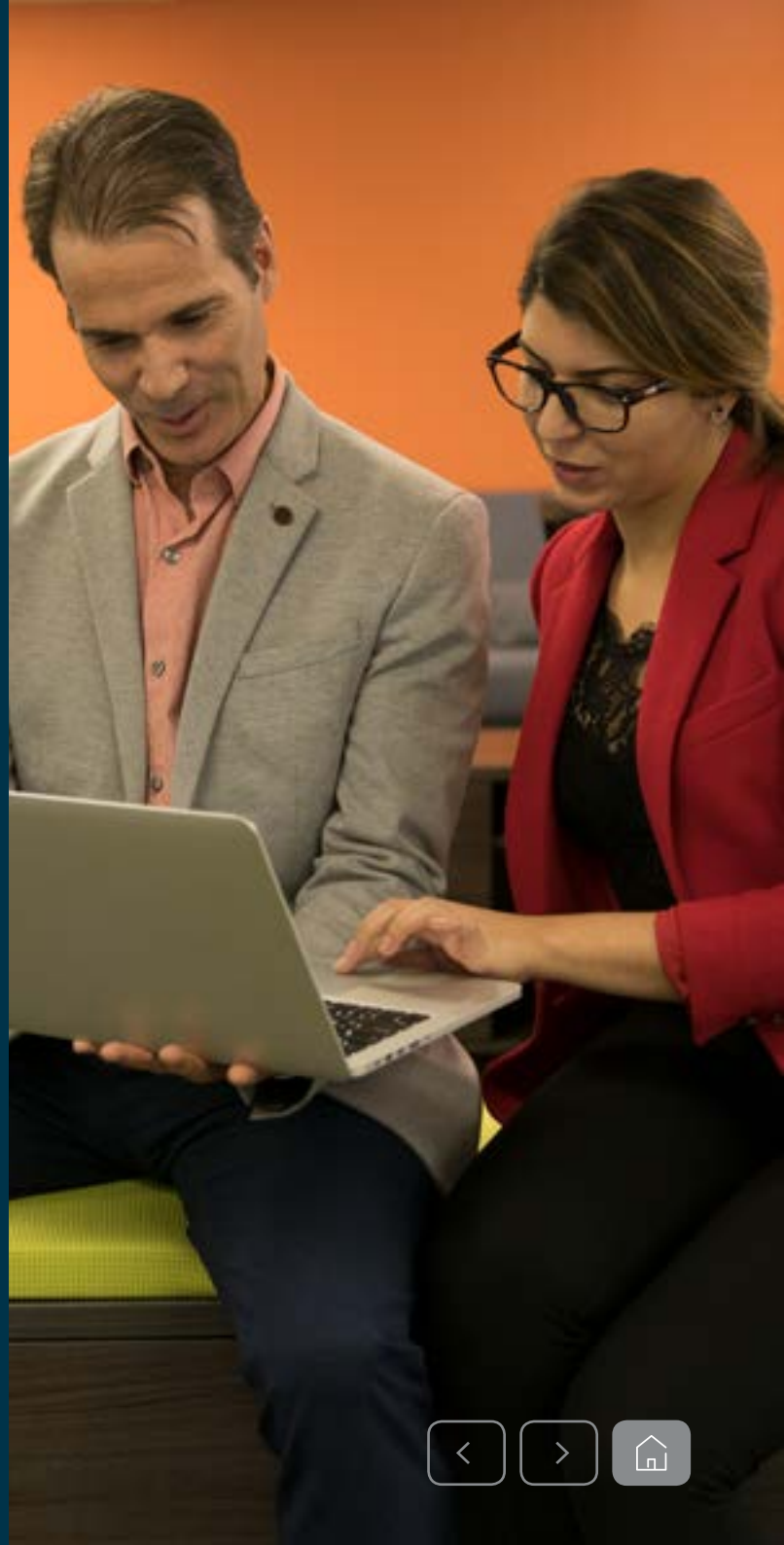
As gatekeepers and processors of personal data, HR and People teams have a crucial role to play in preparing for this step change. The rules on how data is kept and used will become much more stringent, and it's vital that HR and People teams become more transparent, communicating to employees exactly how their data is processed.

In a world where 2,500,000,000,000,000,000 bytes of data are created every day, and people's data are captured and used in ways they may not even realise, GDPR enables HR and People leaders to empower people to own their data in the workplace.

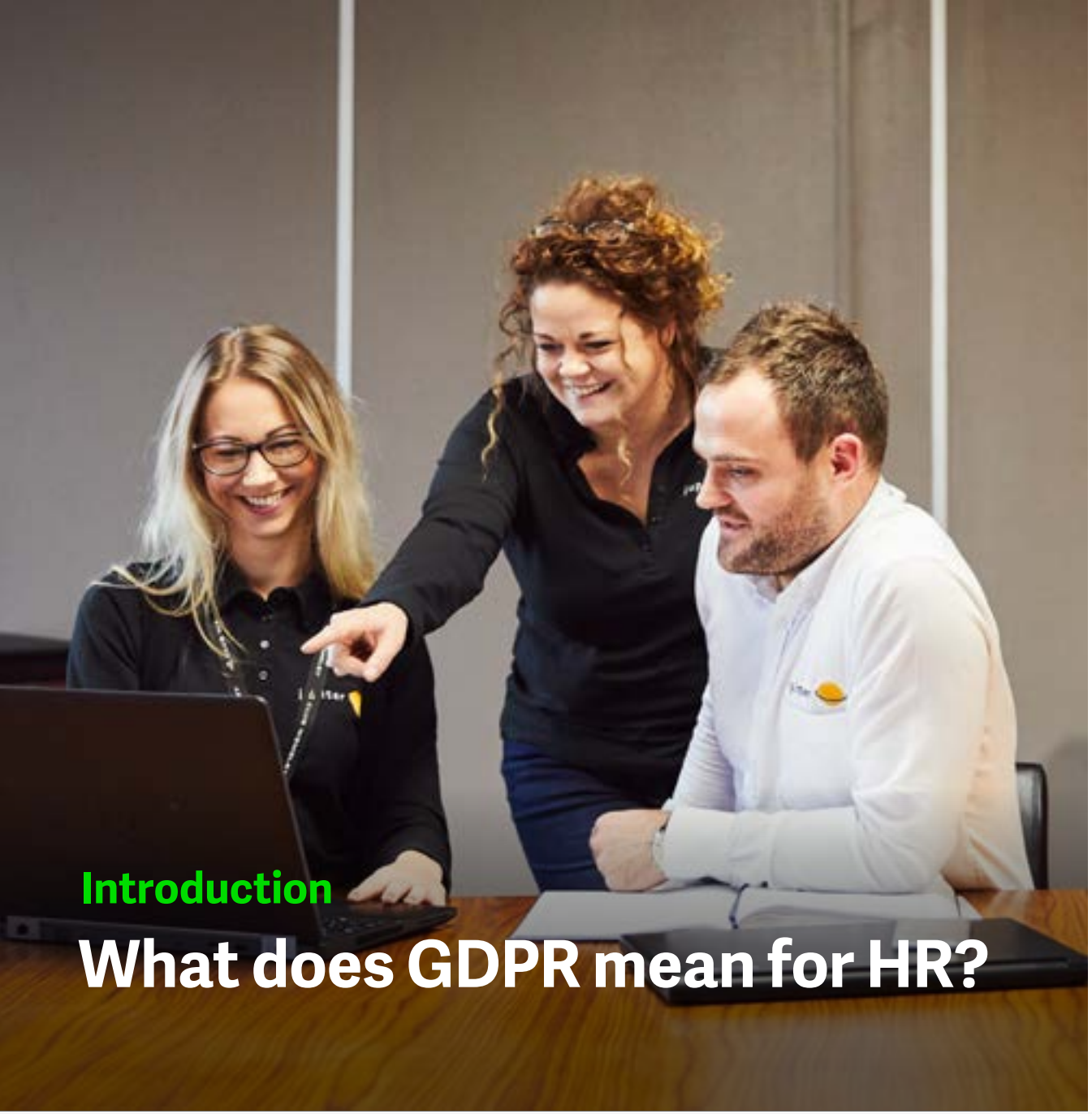
Yes, it needs preparation: but companies can either embrace the new rules, or run and hide. If it's the latter, then you better also prepare to be caught up by significant penalties.

Sage encourages every employer to obtain their own guidance, including legal advice, to ensure that all of your operations are ready for GDPR. In the meantime, this guide walks you through six steps to help HR and People teams prepare for GDPR.

This document is intended to be a concise and simplified guide for businesses. More information can be found via supervisory authorities, such as the Information Commissioner's Office (ICO) in the UK and its *Overview of the General Data Protection Regulation*. Please read the Sage legal disclaimer set out at the end of this guide.



Contents



Introduction

What does GDPR mean for HR?

What is GDPR?

The General Data Protection Regulation (GDPR) comes into effect on the 25th of May 2018 in the European Union (EU), affecting any individual, corporation, public authority, agency or other body that processes the personal data of individuals who are in the EU. It sets out the minimum requirements for the treatment of all personal data.

Personal data can be defined as any data identifying or relating to an individual in most ways, including things like physical appearance or even biometric data.

What's new?

As with existing EU data protection legislation, the GDPR restates three basic sets of rules relating to personal data: data protection principles, lawful processing, and restrictions on international transfers.

Most businesses and individuals should already be aware of these. However, the GDPR introduces several major new requirements, such as individual rights over the use of their personal data; the right to be forgotten; the right of data portability; and proof of compliance.

It comes down to increased protection of individuals' rights and greater accountability for companies and how they manage personal data.

It doesn't 'just' apply to EU companies

If your company has offices or employees in locations globally, and processes, stores or transmits EU citizens' personal data, then the GDPR will almost certainly apply to you. It applies to any organisation worldwide that handles the personal data of individuals who are in the EU, so there are likely implications for your entire global organisation, not just those located in EU member states.

Organisations with fewer than 250 employees are not required to maintain a record of processing activities unless this is likely to result in a risk to the rights and freedom of data subjects, the processing is not occasional, or the processing includes special categories of data (such as criminal convictions or offences).

How much could GDPR cost my business?

The cost of non-compliance is high. Your company could be fined up to 4% of your annual global turnover or €20 million (whichever is greater) for serious offences like not meeting the basic principles for processing, including not having obtained any required consents, or for breach of an individual's rights.

Smaller fines of 2% can be applied for failing to keep your records in order, failing to report a breach, or failing to conduct privacy impact assessments where the processing is likely to result in a high risk to individuals.

Equally, a data breach could result in a mistrust of your company, which could affect employee recruitment, engagement and retention. Are you ready for the GDPR?

What does the GDPR mean for HR?

As gatekeepers and processors of personal employee data, HR leaders and teams have a critical role to play.

By the very nature of their purpose, HR and People teams are already the key custodians for much of the personal data that companies hold about their employees.

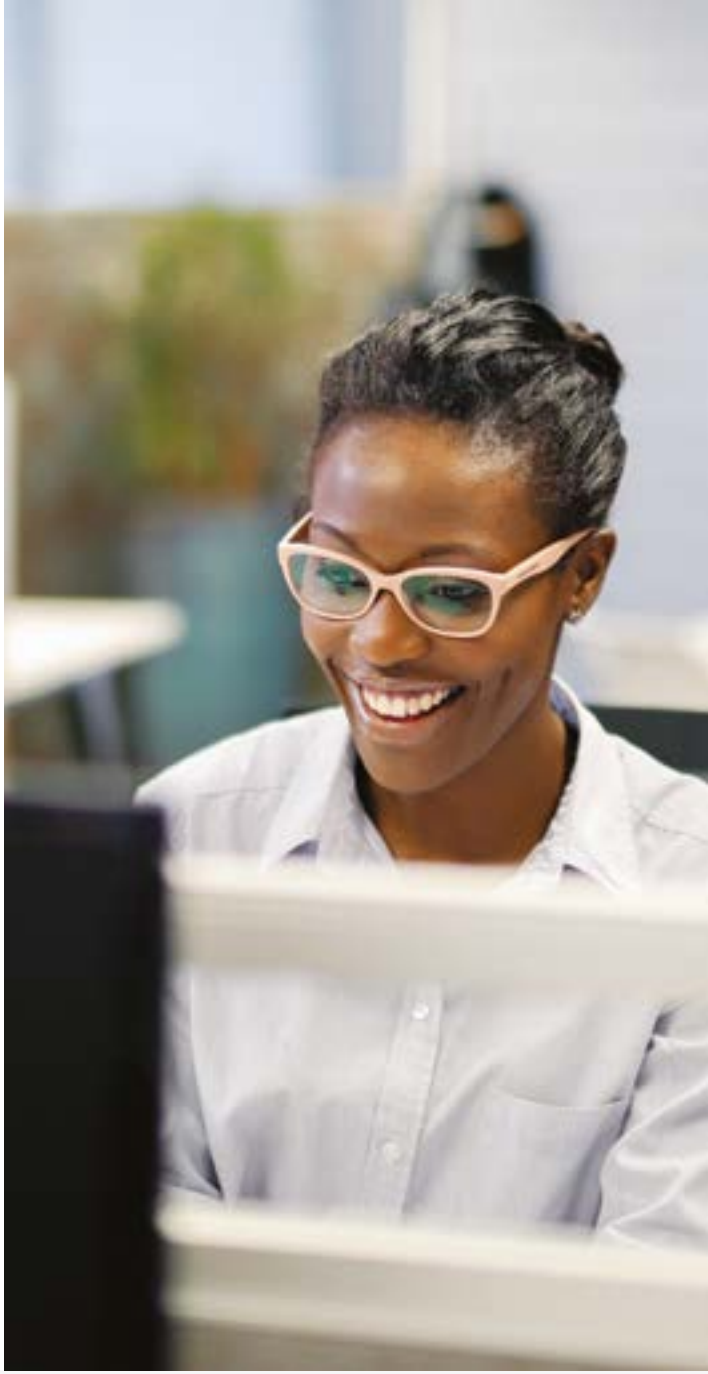
Data is captured throughout the entire employment journey, from a person exploring job opportunities as a candidate, right through to when someone leaves the organisation. Therefore, HR has the biggest role to play in ensuring the safe, secure and compliant processing of personal data for a company's workforce.

HR teams will need to thoroughly review how they manage employee data and requests, including how they:

- Identify the lawful basis required
- Capture any necessary consent from employees
- Protect individual employee data rights
- Allow for data portability
- Change or erase personal data
- Keep people data compliant, safe and secure

As the date for the GDPR approaches, it's time for HR and People teams to look closely at how they can manage their employee data processing.

To help you, we have identified six key steps to help HR prepare for GDPR.



Helpful GDPR classifications

Data subjects	Data controllers	Data processors
The GDPR is centered on protecting the rights of citizens residing in the EU who supply their personal data for some sort of business transaction.	A controller determines the type of personal data that is required, as well as the purpose and means of processing the personal data.	A processor is responsible for processing personal data on behalf of and as directed by the data controller. This includes actions like collecting, recording, storing and retrieving data.
Potential candidates and employees are examples of data subjects within the context of your organisation.	As an employer, you would be the data controller determining the purpose, reason and type of personal data you collect from your candidates and employees.	Sage Business Cloud People is a data processor for its customers, as our system helps to process the data they control and instruct us to collect.

6 steps to GDPR-readiness

Preparation starts with these key steps

1

Have a lawful basis for processing data

Know what data you need and how you are processing it

2

Have the right consents in place

Make sure you have the necessary consents for the personal data that you are holding

3

Ensure individuals' rights to access their data

Keep your people informed; give them visibility and control of their personal data

4

Allow for data portability

Allow your people to transfer their personal data and take it with them

5

Ensure the right to be forgotten

Allow for the deletion of personal data, whilst keeping data required for HR functions

6

Keep your people data safe and secure

Ensure that your people data is gathered in a single verifiable and consistent source of truth

Step 1

Have a lawful basis for processing personal data

Request a demo

Know what data you need and how you are processing it

As an employer, you must have a valid lawful basis to gather and process personal data. It is lawful if at least one of the following applies:

- the individual has given consent for one or more specific purposes
- it's necessary for a contract to which the individual is a party, or will soon be
- a legal obligation must be complied with (e.g. submission of tax records by a business)
- processing of the data is of vital interest in protecting someone's life
- there's a task that's in the public interest or is carried out in the interest of official authority
- it's necessary for legitimate interests except where overridden by the interests, fundamental rights and freedoms of the individual

This requirement is not new in some countries. In the UK, it replaces and mirrors the equivalent requirement under the 1998 Data Protection Act.

However, there is now more emphasis on accountability for, and transparency around, your lawful basis for processing. You will need to review existing personal data being processed, and check that an appropriate lawful basis applies.

Furthermore, you will need to inform employees upfront about your lawful basis for processing their personal data, as part of any privacy information and notices that you will have to provide to people.

This includes communication before the GDPR comes into effect, as well as inclusion in future privacy notices.

Documenting this information will help you demonstrate compliance in line with the GDPR.

The essentials

Compliance begins with having a lawful basis for processing personal data. Consider how you will:

- Capture and record the lawful basis underpinning personal data that you are processing
- Send communications to candidates and new hires advising of the lawful basis for processing their personal data
- Set up triggers to send communications to your entire workforce for any new lawful bases identified in the future
- Share privacy information and send privacy notices in advance to notify employees of their rights and details of how their personal data will be used

Step 2

Have the right consents in place

Request a demo

Make sure that you have the necessary consents for the personal data that you are holding

A lot of candidate and employee data captured for processing will be required for contractual, legal or legitimate interests, such as personal details needed for communication or tax and payment purposes.

In other cases, employers will need to review how they seek, manage and review any necessary consent, including consideration of whether existing consents need to be reviewed if they fail to meet GDPR standards.

From the moment a candidate submits a CV or application form, you'll have to start to record when and how you obtained this data, and on what lawful basis you hold it; this may be consent, in which case, have you documented that consent? In fact, employers with a keen eye on the talent pool regard even speculatively sent CVs as long-term assets in the battle to recruit the best people.

However, speculative CVs are just the tip of the iceberg, as HR departments will now have to link relevant personal data to a clear record of consent.

You'll also need to create clear and GDPR-compliant privacy notices to ensure you provide all the information that employees and candidates are entitled to under GDPR's requirement for transparency.

Employers will also need to ensure that employees know how they can make requests such as data access or rectification, and the process for doing so.

Remember that this applies to all members of your workforce, including candidates, employees, contractors and other contingent workers – anybody whose personal data you are capturing and processing.

The essentials

Ensure that you know clearly how you will collect, process, manage and share personal data, and more importantly, how you will capture and manage consent.

- Capture consent for individuals as necessary
- Ensure that your workforce have provided any necessary consents, and that they can view and access a record of this
- Allow employees to change and update consent for their personal data
- Add, track and report on additional consent checks where required
- Synchronise consent with the relevant information on the employee record
- Provide clear and tailored communication and privacy notices to help employees understand their rights and processes

Step 3

Ensure individuals' rights to access their data

Request a demo

Give your people visibility and control of their personal data

The GDPR provides a clear set of rights for your employees, including data rights to:

- be informed
- complain to supervisory authorities
- access, rectify or erase
- restrict and object to certain types of processing

This means you must give your people full visibility of the data you hold about them, and comply with any access requests within one month.

It's also your responsibility to keep them informed about their personal data. You'll be required to make certain pieces of information available, such as the identity and contact details of the data controller and any data protection officer; recipients of their data; how long you'll store the data for; and the rights of the individual employee.

It's important to be transparent if data is breached, and notify relevant authorities in a timely manner. For example, in the UK, companies must currently notify the Information Commissioner's Office (ICO) within 72 hours of any breach coming to light.

To support these requirements, you'll need an efficient way of enabling employees to see their data, change it where necessary and understand how it is being used. This is where self-service comes in.

Self-service is traditionally used as a way to automate key HR transactional tasks, such as booking and approving holidays, or capturing performance review information.

Progressive companies will already be one step ahead, using self-service to interact with their workforce and give them autonomy to view and update personal data themselves.

With systems like Sage Business Cloud People, companies can extend the use of self-service to help employees view and manage any personal data. Increased accessibility like this helps your employees to feel that they're in charge of their own data, whilst giving you a better understanding of your workforce.

The essentials

GDPR gives employees the right to see their data, know how it's being used, and ask to change it. As an employer, you'll need to protect and facilitate these rights.

- Enable employees to access and modify their personal data, records and documents, on any device at any time
- Capture, facilitate and track employee requests to view, change or erase personal data
- Identify and export personal data easily upon request
- Deliver tailored communications to inform employees of any privacy or data updates they might need to know about
- Link relevant policy documents and notifications with employee records
- Provide a trail of how data is being used and shared, for auditing and tracking purposes

Step 4

Allow for data portability

Request a demo

Allow your people to transfer their personal data and take it with them

EU citizens may, upon request, obtain and reuse their personal data for their own purposes. For example, they may wish to move, copy or transfer certain personal data to their next employer.

To comply, employers must provide the personal data in a format that can be easily consumed by other systems as required. The information must be provided free of charge.

When exporting and transferring personal data for a particular individual, take care that the data doesn't contain personal data or compromise data privacy for other employees.

For any requests that are submitted, you must respond as soon as reasonably possible, within one month of receiving the request.

You may have an extension of two months if the request is complex or you receive multiple requests.

If there is a legitimate reason for not taking action, you will need to provide an explanation to the individual while informing them of their right to complain should they wish.

However, the need for data portability only applies in cases where automated data is provided to controllers on the basis of consent or contract. It doesn't apply to manual records for example.

While communicating and enabling these rights present big challenges to HR, it's also true that GDPR offers every employer the chance to build a better workforce relationship by being totally transparent from the outset. Honesty isn't just the best policy, it's about to become the only option on the table.

The essentials

Companies will need to make personal data truly portable and easy-to-use by others, so that individuals are able to take it with them.

- Clearly identify all personal data and how it is being processed
- Set up processes for extracting and exporting personal data by those with the appropriate permission to do so
- Ensure that personal data can be exported to open machine readable formats such as CSV
- Automate workflows so that notifications are automatically sent to confirm the status of an employee's data portability request

Step 5

Ensure the right to be forgotten

Request a demo

Put a consistent policy in place for the deletion of personal data, whilst keeping data necessary for HR functions

Data subjects can, upon request, ask companies to stop processing and delete their personal data where consent was given, or where the data is no longer necessary for the purpose for which it was collected. This is the individual's right to erasure, also known as the right to be forgotten.

The right to be forgotten is one of the biggest changes brought by GDPR, as well as one of the hardest to manage.

Put simply, it means you'll need to have a consistent policy in place for the deletion of personal data when it is no longer needed. This might mean erasing some personal data as soon as an employee has left.

Is your IT system capable of locating and deleting that data? Just as importantly, who makes the decision about whether to comply with such a request?

HR and People teams might want to keep data on file for future references, or to decide whether someone is employable again at a later stage. And what if there was a chance of a future tribunal? It might be against your interests to delete data that related to disciplinary procedures.

The good news is that the right to be forgotten is not an absolute right, and you do not have to erase data if there is a lawful reason to keep hold of it for a longer period of time.

The essentials

The right to be forgotten is a key part of the new GDPR rules. You need to ensure that there is a consistent policy in place for the thorough identification and deletion of data.

- Be able to easily identify personal records and data points for every individual
- Ensure you can manually delete records on request, with additional checks in place (if needed) to ensure the correct data is being removed
- Hold the source of new candidate data when making new hires, and link this with their employee data when they join, to ensure a single employee record
- Be able to provide a trail of how data is being used and shared, for auditing and tracking purposes
- Ensure you can provide confirmation to the individual once personal data has been deleted

Step 6

Keep your people data safe and secure

Request a demo

Ensure that your people data is held in a single verifiable and consistent source of truth

To prepare for GDPR, you need to document and secure all of the personal data you hold, including information on where it came from and who you share it with. This is difficult when data is held across numerous spreadsheets when you use multiple products containing people data, such as payroll, workforce management or learning management systems.

So gathering and storing personal data in a single, secure database is the building block that everything else rests upon.

Once your people data is held in a single, secure and verified database, it becomes a definitive source of information for every data request, helping to streamline HR processes, as well as helping to meet some of your compliance obligations.

Your single source of truth must be held securely and transferred in encrypted formats where required, in case of data breaches.

How do you make it a fully consolidated and compliant source of truth that is GDPR-ready?

Built on the Salesforce App Cloud, Sage Business Cloud People customers have transparency and control of their data to accelerate compliance with regulations such as the GDPR, as well as benefitting from robust security measures that meet the highest standards in the industry.

Our solution is compliant with the internationally recognised ISO27001 legislation, enabling companies to meet data privacy and security obligations and ensure a level of security appropriate to the GDPR, such as detecting and reporting on security incidents.

The essentials

Establish a single source of truth that is safe, secure, consistency and verifiable.

- Store data in a single, cloud-based source of truth that enables every employee to access and manage their personal data with ease
- Tailor data access and control by role, as well as at global and local levels
- Enable cross-departmental visibility for HR teams wherever necessary to improve ease of data processing
- Easily identify personal data that might need to be removed, and distinguish from data held for legitimate purposes
- Ensure robust data integration, and imports and exports for linking people data seamlessly with third-party data sources

Your GDPR checklist

Request a demo

Now that you are more familiar with the GDPR, use this list of essential actions as your checklist for readiness in HR

Step 1
Have a lawful basis for processing data

Go to Step 1

- [ ] Identify the personal data to be captured
- [ ] Establish a clear and valid lawful basis for the personal data that you intend to process
- [ ] Clearly document your lawful bases for auditing and tracking purposes
- [ ] Provide clear communications and privacy notices to your employees advising of the details of how their personal data will be processed
- [ ] Complete these steps for all the personal data you hold today, ahead of the GDPR coming into effect

Step 2
Have the right consents in place

Go to Step 2

- [ ] Clearly identify any personal data that will require individual consent
- [ ] Ensure that consent is captured for each individual against their employee record
- [ ] Set up notifications to flag when personal data is updated or further consent is required
- [ ] Provide a mechanism or workflow to capture and record consent
- [ ] Ensure that consent can be tracked for auditing
- [ ] Allow employees to manage their consent via self-service

Step 3
Ensure individuals' rights to access personal data

Go to Step 3

- [ ] Identify and communicate key updates and information that your workforce need to know
- [ ] Ensure that all personal data is easily identifiable and accessible by employees via self-service
- [ ] Allow employees to view, change and request copies of their personal data via self-service
- [ ] Attach all personal data and documents to individual employee records for simple access
- [ ] Set up any processes required to ensure that data requests are managed quickly and efficiently

Step 4
Allow for data portability

Go to Step 4

- [ ] Ensure that personal data can be easily identified and exported upon on request
- [ ] Ensure personal data can be exported to open machine readable formats such as CSV
- [ ] Enable employees to make requests to export and transfer data via self-service
- [ ] Establish processes and workflows to ensure that communications and updates are delivered in a timely fashion

Step 5
Ensure the right to be forgotten

Go to Step 5

- [ ] Ensure that all personal data is easily identifiable
- [ ] Set up additional checks (if needed) to confirm that the correct data is being removed
- [ ] Ensure that all personal data records can be manually deleted on request
- [ ] Enable employees to make data erasure requests via self-service
- [ ] Provide confirmation once personal data is deleted

Step 6
Keep your people data safe and secure

Go to Step 6

- [ ] Gather all people data in a single source of truth
- [ ] Provide a trail of how data is being used and shared, for auditing and tracking purposes
- [ ] Tailor data access and control so only those with the permissions have access to personal data
- [ ] Clearly distinguish between consent data and data held for other legitimate lawful purposes
- [ ] Ensure that any integration of people data is secure

Get control of your people data with Sage Business Cloud People

The Sage Business Cloud People system helps you improve workforce visibility by automating people processes and enabling data reporting and analytics. With stronger insights, you'll transform the way you attract, manage, engage and retain your workforce. Sage helps HR and People teams automate the end-to-end employment journey, helping you adjust to the GDPR more easily.

Request a demo

To learn more about getting ready for GDPR with Sage, visit www.sage.com/en-gb/gdpr/

Sage legal disclaimer

The information contained in this guide is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. We would like to stress that there is no substitute for customers making their own detailed investigations or seeking their own legal advice if they are unsure about the implications of the GDPR on their businesses.

While we have made every effort to ensure that the information provided in this guide is correct and up to date, Sage makes no promises as to completeness or accuracy and the information is delivered on an "as is" basis without any warranties, express or implied. Sage will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information or from any action or decisions taken as a result of using this information.