GDPR

HR PERSONAL DATA BEST PRACTICES

EXECUTIVE SUMMARY

The EU data protection regulation GDPR comes into force on May 25th, 2018, organisations both within Europe, and those offering services to those based Europe must comply with the regulation or face the potential of large fines (the greater of €20m or 4% of annual global revenue).

HR departments, as holders of large amounts of personal data, need to ensure that they not only are aware of the GDPR but that they have systems, policies, processes and procedures that are demonstrably compliant with the GDPR.

The rest of this best practice guide will explain provide information about how HR the GDPR will affect HR departments, as well as provide direct guidance on aspects such as data retention, and what security features your HR system to have in order to help your organisation become and maintain compliance.

fifth STEP™

BACKGROUND TO GDPR

The General Data Protection Regulation (more commonly known as the GDPR, or less often by its official designation of Regulation (EU) 2016/679), builds on the Data Protection Directive which was adopted in late December 1995, but was actually implemented in 1998 (in the UK for example, it was enacted in the UK Data Protection Act 1998).

As with the DPD, there have been a number of years since the GDPR regulation was adopted (in April 2016) to when it will finally be enacted on May 25th, 2018.

The purpose of the GDPR (and its predecessor) is to ensure that those who provide their personal data to companies know what the data is going to be used for, to have to consent to the use of the data in that way, and to have rights to be able to control and monitor the way that their data is used.

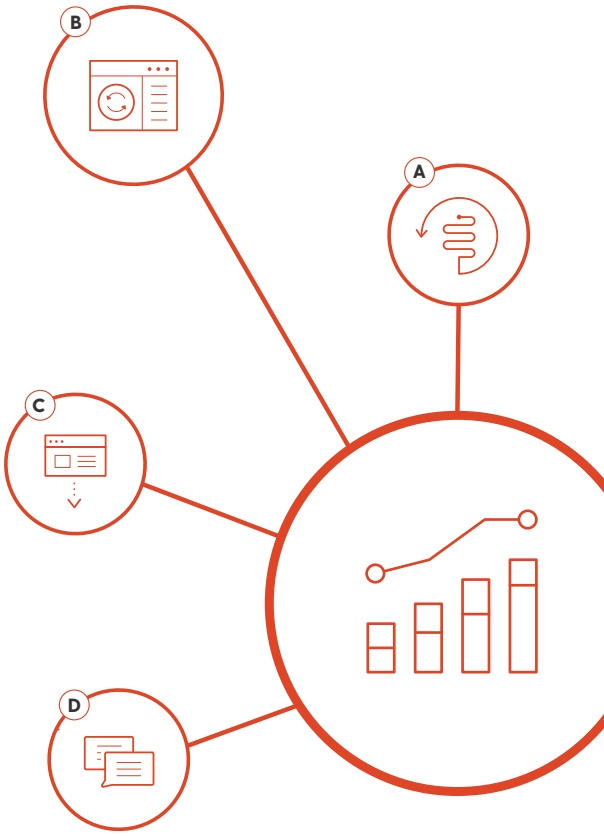
For those unfamiliar with EU Data Protection, it may be useful to consider personal data as an asset that the data subject (the person who the data is about) gives permission to use for a specific purpose. They can at any time request details about their personal data, and even withdraw their consent for its use, although the latter would be unusual in the case of personal data processed by HR departments.

TERMS AND TERMINOLOGY

As with any regulatory requirement there are terms and terminology that one has to know and understand, fortunately, in the case of the GDPR there are not too many, and they are not too complex:

.1

PROCESSING (OF PERSONAL DATA)



Processing of data is defined by the GDPR (in Article 4) as:

In relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- (A) Organisation, adaptation or alteration of the information or data,
- (B) retrieval, consultation or use of the information or data,
- (C) disclosure of the information or data by transmission, dissemination or otherwise making available, or
- (D) alignment, combination, blocking, erasure or destruction of the information or data.

Whilst only a short statement, this essentially says that anything that you are going to do with personal data is covered. So, processing includes the collection, storing, use, maintenance, archiving and deletion of personal data – This covers the entire data lifecycle.

.2

DATA SUBJECTS

The data subject is defined by the GDPR (in Article 4) as:

An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

This means someone who can be identified by their personal data either by the use of regular identifiers (name, address, etc.) or by the use of reference or identification numbers (passport number, bank account number, employ Id, etc.).

.3

DATA CONTROLLER

The data controller is defined by the GDPR (in Article 4) as:

A person who (either alone or jointly or in common with other persons) determines
the purposes and the manner in which any personal data are, or are to be, processed.

In the case of an organisation hiring an employee, the organisation is the Data Controller, they define the purpose and manner in which the data is processed

.4

DATA PROCESSOR

The data processor is defined by the GDPR (in Article 4) as:

Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

The data processor must be able to identify the data controller for any of the data in its possession, and must upon request be able to provide information such as:

- The identity of the data controller for the data
- The data controller's contact information
- The data processing purpose
- The category(ies) of data

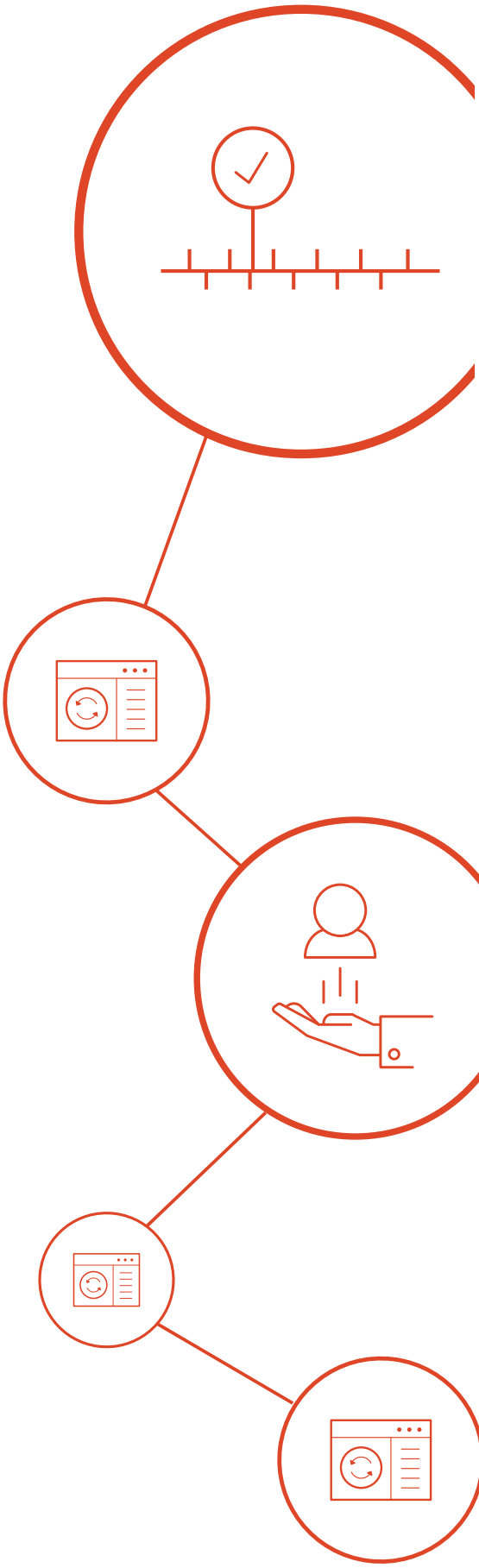
If an organisation outsources the processing of their payroll to another Acme Payroll Service, that company would become the Data Processor.

.5

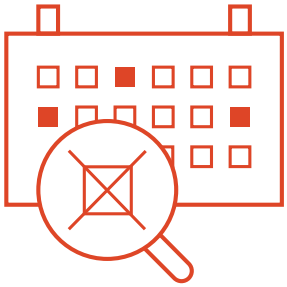
PERSONAL DATA

Personal Data is one of the most important tenants to the GDPR, it is similar to the definition of PII In the United States; however, the GDPR (Article 4) defines it as:

Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.



fifth STEP™



.6

PERSONAL SENSITIVE DATA

The GDPR (Article 4) defines Personal sensitive data as a special class of Personal Data, in that it is:

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

Genetic and biometric data are new additions from the DPD, recognising the developments in this field since the data protection directive came into force. Due to the type of information being captured organisations should consider the additional requirements for the protection of such data to ensure that it is appropriate (additional encryption etc.)

In the case of an organisation hiring an employee, the organisation is the Data Controller, they define the purpose and manner in which the data is processed.

.7

GEOGRAPHIC RESTRICTIONS FOR DATA EXPORT

Personal Data held by non-public sector organisations can be processed in any of the 28 (pre-Brexit) EU countries, it can also be processed in other countries that are deemed by the European Council to provide adequate protection, in 2017 these are:

Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay, United States (under EU-US Privacy Shield).

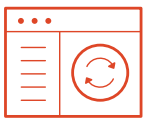
Data is considered to be exported if it is processed (including viewing) in a country that is not listed above, or in the case of the United States that the organisation is not part of the EU-US Privacy Shield. It is important to understand that these rules still apply if the data is being exported internally within the same company.

.8

GDPR AND BREXIT

With Brexit negotiations underway to determine exactly how and when the UK will leave Europe, some have questioned if UK based companies need to bother with the implementation of an EU regulatory requirement.

Unfortunately for those people, the UK will not leave Europe until well after the GDPR has been implemented, and the UK government have already said that the GDPR will apply even after the UK leaves the EU.



fifth STEP™

HR PERSONAL DATA AND PERSONAL SENSITIVE DATA

HR departments are very used to dealing with personal information, in fact in some organisations they may the largest collection of personal information.

PERSONAL DATA

Some examples of personal data that an HR department may process:

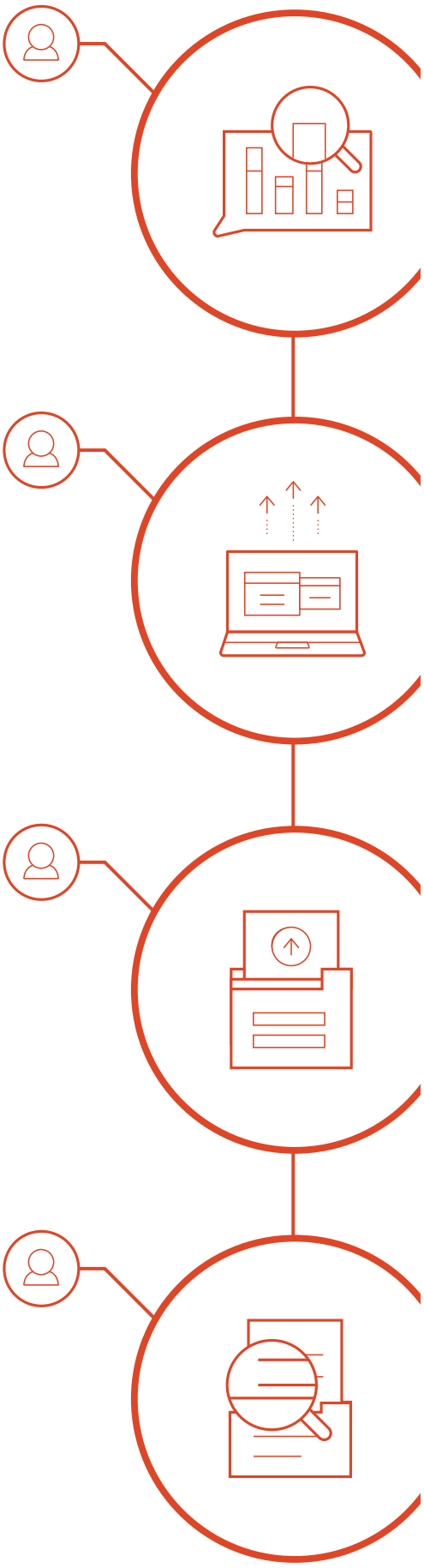
- Names
- Address
- Date of birth
- Employee Id
- Passport, identity card information
- National insurance/social security number
- Bank account

PERSONAL SENSITIVE DATA

Some examples of personal sensitive data that HR departments are likely to process:

- Ethnicity (in some countries this is a legal requirement, many organizations collect it to perform ethnicity monitoring)
- Details of trade union membership
- Religious or philosophical beliefs
- Medical information, including self-certification notes, and doctor's fitness to work letters
- Performance, annual review and assessment information
- Information about a person's sexual orientation

As the name suggests Personal Sensitive Information needs to be treated with additional care. This may mean that access to this level of information is further restricted to the most senior members of HR staff.



DATA SUBJECT'S RIGHTS

THE RIGHT TO BE INFORMED (ARTICLES 7 AND 13)

This right provides the data subject with the right to be informed about what their data is being used for. This will usually be a combination consent and the company's privacy notice.

For HR departments, this means having a clear policy for the collection and processing of personal data, as well as ensuring that the data subject is presented with, and consents to the data purpose before providing their information, no matter which use-case they are following.

THE RIGHT OF ACCESS (ARTICLE 15)

This right provides the data subject with access to their data. A data subject may request access to the personal data and sensitive personal data that your organisation holds on them. Following the request, the organisation has 1 month to respond, in complex cases, the organisation can extend the time, but this is to be the exception rather than the rule.

For organisations that are using a computer system that allows data subjects access to their data, they may be able to self-service this request, however, the organisation needs to have a process to produce a printed copy of the information.

Under the data protection act the organisation was permitted to charge a small fee to fulfill such requests, under the GDPR this has all but been removed.

THE RIGHT OF RECTIFICATION (ARTICLE 16)

A data subject, having identified errors in the personal data that an organisation keeps about a data subject, the data subject has the right for that information to be corrected.

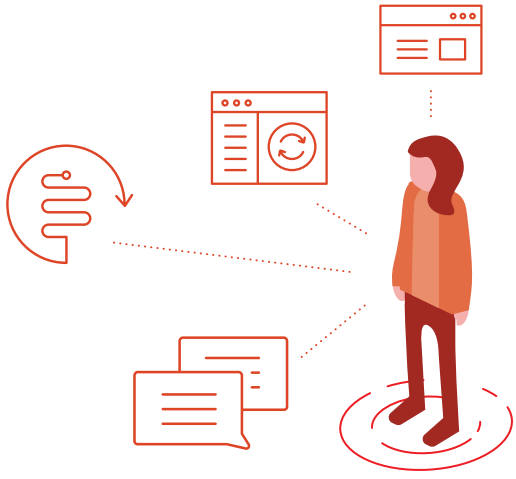
In an HR setting, it is best where possible to allow employees to update their own records directly in the HR system, this reduces the strain on HR departments; however if your HR system does not off offer such a facility, then the organisation must have a manual process to be able to complete the process.

THE RIGHT TO ERASURE (ARTICLE 17)

This right is often called the right be forgotten. A data subject can request that their personal data be removed from an organisation's computer systems. The organisation does have the right to refuse the removal of the information that is required for legal or regulatory purposes. Information should only be kept for the period required to provide the service or purpose for which it was collected.

In an HR scenario, an example may be where a former employee could request their medical data be deleted from your organisation's systems once they have left the organisation.

Whilst requests for erasure can be rejected, it this has to be on very good grounds (such as a legal requirements for example), a rejection is not an option to be taken lightly, if the data subject feels that it is unwarranted they can lodge a complaint with the data protection authority (e.g. ICO in the UK).



THE RIGHT TO RESTRICTION OF PROCESSING (ARTICLE 18)

If a data subject has requested a copy of their data and has identified errors or omissions in the data, they have the right not only to request that the data be corrected but also that the processing of that data is restricted until the issue has been resolved.

THE RIGHT TO DATA PORTABILITY (ARTICLE 20)

Data subjects not only have the right to request their data in a human readable form (the right of access), this right grants them access to their data in a machine-readable form (in an industry standard format, this may be CSV file, XML or another standard as may be agreed by the HR system developers).

In an HR setting, it is possible that employees, before they leave an organisation, will ask for a copy of their personal data to provide to their next employee.

THE RIGHT TO OBJECT (ARTICLE 21)

The right to object provides the data subject the right to object to the use or processing of their personal data in a particular way. This may be a request to stop using the data for marketing purposes for example.

This right is unlikely to be called upon in an HR setting, but it is possible, particularly if an employee feels that their data is being processed in a way that is not consistent with the data purpose.

THE RIGHT TO OBJECT (ARTICLE 21)

The right to object provides the data subject with the right to object to the use or processing of their personal data in a particular way. This may be a request to stop using the data for marketing purposes for example.

This right is unlikely to be called upon in an HR setting, but it is possible, particularly if an employee feels that their data is being processed in a way that is not consistent with the data purpose.

THE RIGHT TO MANUAL PROCESSING (ARTICLE 22)

The right to manual processing grants the data subject the right to have a process performed by a person rather than an automated process, where that automated process is making a significant decision.

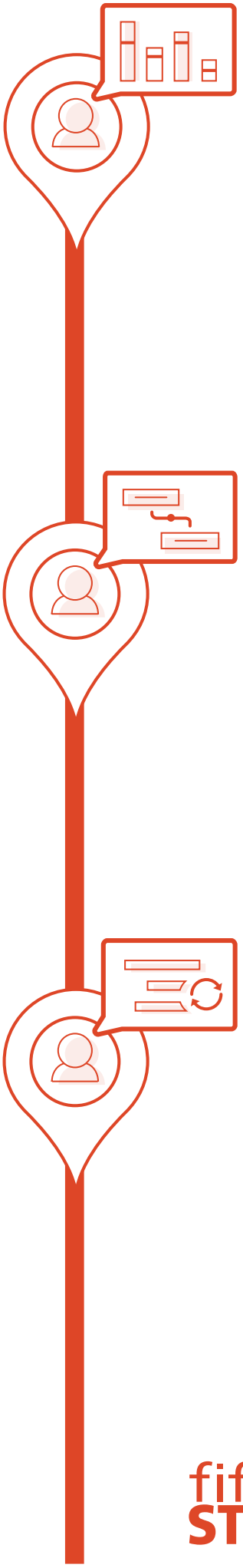
In an HR environment, this right could be used by an employee who objects to their bonus, salary increase or suitability for access to some company provided benefit being decided by a computer system. In such a case the company would have to be able to have a person perform the task, and have the ability to override the computer-based decision.

THE IMPORTANCE OF A PRIVACY NOTICE AND CLEAR DATA RETENTION FOR HR DEPARTMENTS

The privacy notice is the name given to the plain language description of why the data is being collected and how it will be processed. It must also include information about who to contact for more information, and how to exercise their rights in respect to this data. If the data is to be processed by any third parties, or in countries that are not considered to the European Commission to have adequate protection (see the section above on Geographic Restrictions for Data Export for details). The GDPR gives a full definition of a privacy notice in Article 13.

The data controller (this is the organisation hiring the staff) must define, maintained and adhere to the data purpose, as well as ensuring that any data processors perform their duties in accordance with the purpose.

Under the GDPR, personal data can only be processed (including stored) for an amount of time that is reasonable for the fulfilment of the purpose for which it was collected. HR departments do of course collect data for different purposes, and will, therefore, have to maintain different data purposes and also different retention policies.



PHYSICAL & DIGITAL DATA

It is a common misconception that the GDPR only applies to data that is stored on computers i.e. stored digitally. This is not the case; the definition of personal data makes no reference to how or where the data is stored.

This means that your physical files are as much in scope as your digital files, which in turn means that they may be needed to answer personal data requests, it also means that data irrespective of the method of storage must be stored in a secure manner (this will mean being stored in locked filing cabinets, which are only accessible to authorised staff), and that physical files need to be destroyed just as digital files are.

Security of physical files is nothing new to HR departments, but organisations need to ensure that they don't become complacent or too fixated on the processes and procedures that manage the digital data to the detriment of the physical data.

DIGITAL DATA STORAGE BEST PRACTICES

For your digital data storage, there are several best practices that your organisation should follow:

ENCRYPTION AT REST

An important part of the GDPR is maintaining the privacy of personal information. Part of this is ensuring that the information is secure, and cannot be accessed if a laptop is left on public transport.

Best Practice: Do not allow personal data to be extracted from your HR systems so that it is stored on the hard drive of laptops or other mobile devices.

Best Practice: Where data has to be stored outside of the HR system, ensure that all personal data is encrypted. Full drive encryption is the most convenient way to achieve this (this comes as an integral part of modern operating systems).

Best Practice: Do not allow personal data to be stored on removable media (i.e. USB drives).

CONTROL AND KNOW WHERE YOUR DATA IS STORED

As is was explained earlier in this document, data only be processed in a location, and by a service provider who has an equivalency with the GDPR.

Best Practice: Ensure that your organisation (in the shape of the Data Protection Officer and/or the Chief Information Officer) is only storing personal data in appropriate locations.

DATA QUALITY AND VERSION CONTROL

The GDPR mandates that steps are taken to ensure that information is kept up to date. It is not acceptable to continue using data that may be out of date.

This problem manifests itself in another form, that of version control. How often have you seen (or perhaps even done it yourself) files named: Salary Information Final, and another called Salary Information Final V1, and perhaps a third called Salary Information Final Final. Which one of these documents is the right one to use?

Best Practice: Have processes to help ensure that personal data is maintained. If your HR system supports self-service, encourage your staff to update their information on a quarterly basis. Where your HR system doesn't provide self-service, make sure your staff knows the process for updating their personal information.

Best Practice: If your organisation stores its documents in a document management system (DMS), it will likely manage version control for you, don't try and make it more difficult by adding version numbers or other annotation in the file name. If your organisation doesn't use a DMS then make sure that you have a file naming and versioning policy, and those old versions are placed in an archive folder so that it is very clear which version of the file is the current version.

OFFLINE ACCESS

Until access to the internet is fully ubiquitous people are always going to need access to files "offline". This typically means that files are stored on the hard drive of a laptop computer. The ability to download files and store them outside of the HR system needs to be carefully monitored and controlled on a case by case basis and avoided where possible.

Best Practice: Don't allow the storage of personal data on laptops other than by exception, and where there is a defined and definite need.

ENSURING SECURITY OF SCANNED DATA

Not all documents start life as digital documents, obvious examples are proofs of identity, and right to work documents (passports, work permits, visas, birth certificates etc.). These may be scanned or photocopied before making it into the HR system, or the company's document management system.

Best Practice: Have a defined process for the capture and destruction of paper copies of personal information. Where possible scan the information directly into the HR system or DMS. Limit the people who are allowed to perform such scans or copies. Ensure paper copies are destroyed securely once they're finished with.

DIGITAL DATA ACCESS BEST PRACTICES

When it comes to accessing digital data, ensure there are several best practices that should be followed:

MINIMAL ACCESS AND ACCESS REQUIRED FOR ROLE

By default, users should have the minimal access rights required to perform their role.

Best Practice: Ensure staff access rights are appropriate to their role. Access rights can be increased for a short period of time, for holiday cover for example but should be returned to their normal levels as soon as is appropriate.

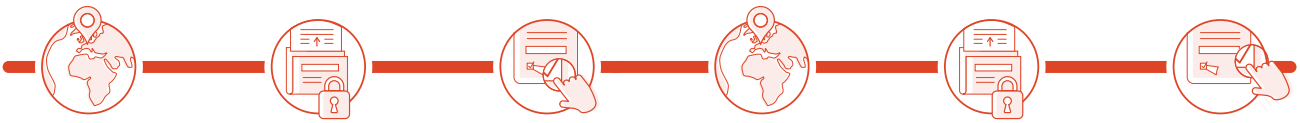
REGULAR ACCESS RIGHTS REVIEWS

Sometimes people's access rights change, or their role changes, their access rights should be changed to reflect the requirements of their role.

Best Practice: Regularly (no less than quarterly) ensure that access rights are appropriate to the role and that any leaver's access rights have been revoked. Ensure that your staff mover and leaver processes include steps to adjust access rights.

HR DATA USE CASES

The requirements of the GDPR can be rather abstract when reading on their own; this section aims to bring them to life a little more, by exploring common HR orientated use cases.



HIRING

A typical hiring process will follow the following high-level process:

- Role Created
- Role Advertised
- CVs/Resumes Submitted
- CVs/Resumes Reviewed and Shortlisted
- Shortlisted Candidates Interviewed

The personal data that is likely to be captured during this process is may include things like:

- Name
- Address
- Email address
- Telephone number
- Passport, identity card information (often required to evidence right the candidates right to work in the country where the organization is based)

Your organisation will require a data collection purpose that explains how the candidate's data will be processed, and how long it will be retained for (see the section below for best practise retention periods), this needs to be in plain language, and also give details about the data subjects rights and contact details for them to exercise those rights.

NEW JOINER

When a person joins an organisation, there is typically standard information that is collected about the person in order for the HR processes to function, and for the person to be paid etc.

New joiners should be made aware of the purpose for the data collection, how their data will be processed, details of any locations outside of the EU that their data may be sent to, and to provide consent for their data to be processed in this way.

Most organisations handle this process by having the new join provide their consent for their data to be processed as detailed, this can be by signing a physical document but is increasingly performed electronically.

The new joiner stage is where a lot of personal data is collected, although some may differ until the employee has completed their probationary period.

Examples of the personal data processed at this time may include:

- Names
- Address
- Date of birth
- Employee Id (usually assigned at this stage)
- Passport, identity card information (if not obtained during the hiring stage)
- National insurance/social security number
- Bank account
- Personal data about next of kin

Some organisations also use biometrics for security systems, as noted above, biometrics are treated as sensitive personal information, and would, therefore, need to be protected to ensure that the information was protected from misuse or leaking.

COMPLETION OF PROBATION

Most organisations use employee probation as a means to reduce the risks of employing a new member of staff. Different organisations will enable different services (and therefore collect different personal data) on the completion of probation. It is not unusual for services such as private medical insurance, and participation in the company pension to be restricted to those who have completed their probation. Examples of the personal data and sensitive personal data that may be collected during this stage may include medical data for the data subject, and potentially their family members.

DURING EMPLOYMENT

During the time that a person works with and for an organisation, more personal data is collected about them, this will include personal data such as:

- Performance and Annual Reviews
- Staff's family member's data for healthcare etc.

Personal data that has already been collected will also be maintained and kept up to date during this period.

LEAVERS

At the point that a person leaves the company, it is unlikely that there is any new personal information to be collected, this is, however, the point when the data retention clock(s) start to countdown.

PENSIONERS

Depending on the nature of your organisation's pension provisions, the person who becomes a pensioner may retire from the organisation, and become a pensioner, or they may have left some time ago but still benefit from the organisation's policy. Whichever case is closest to your organisation's situation there may be some additional information personal information that is required, at the very least, it is the best practice to contact the former employee to ensure that the information that your organisation holds is correct.

BEST PRACTICE DATA RETENTION PERIOD

There are at least three data retention periods in most HR processes, as with all data retention periods they need to be tailored to your organisation's specific requirements and practices; this section will put your organisation on the right path, and help you understand your organisation's data retention needs, as well as provide best practise guidance.

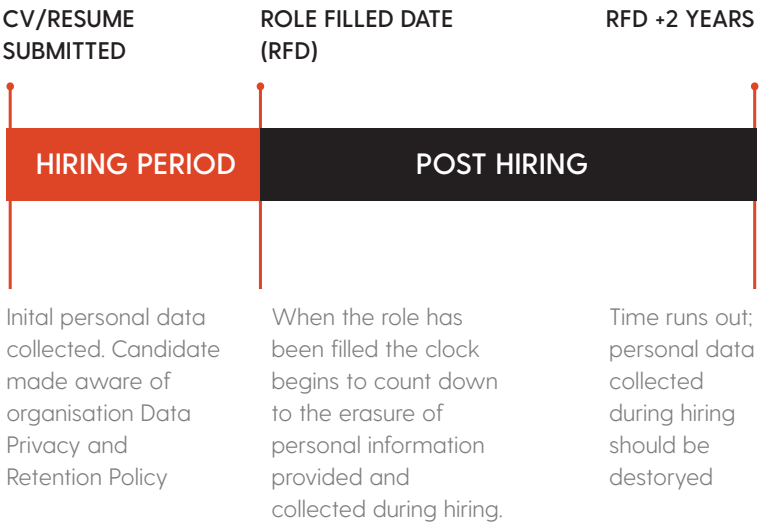
HIRING

As a best practice, your organisation should be deleting CVs submitted within two years of their submission.

Such a period would allow your organisation to revisit CVs that had been previously submitted, to contact people about similar roles. If this is not an approach that your organisation takes then consider reducing the retention period to meet your current or intended practices.

HIRING DATA LIFECYCLE SIMMARY

Note: Any time after the candidate (data subject) has provided their personal information they can exercise their rights, including asking for the data to be destoryed.



LEAVING

When an employee leaves your organisation, a clock needs to start ticking for the erasure of their personal data. HR data can be divided into three categories at this time.

Data Required to Evidence Employment and Compliance with the Law

Personal data that falls into this category will include:

- Name
- Address
- Email address
- Date of birth
- Passport, identity card
- National insurance, social security number
- Ethnicity (if required by law, or as part of diversity reporting)
- Employee Id

Sensitive Personal Data

This class of data contains information that may be required for a short period of time after the person leaves the company, but due to the sensitive nature of the data, and the fact that there is no need for the organisation to retain the information for an extended period of time:

- Medical information (including medical information provided for company pension or health care benefits)
- Trade union membership
- Details of religious or philosophical beliefs
- Information about their sexual orientation
- Details of next of kin

Best practice for this class of data is to delete it within 6 months of the person leaving the company. If the person should wish to apply for another job at the company at a later date much of this information can/should be re-provided as part of the employee's new contract/terms of employment.

Other Personal Data

Other personal data includes all the information that has been collected about the individual during their time with the organisation including:

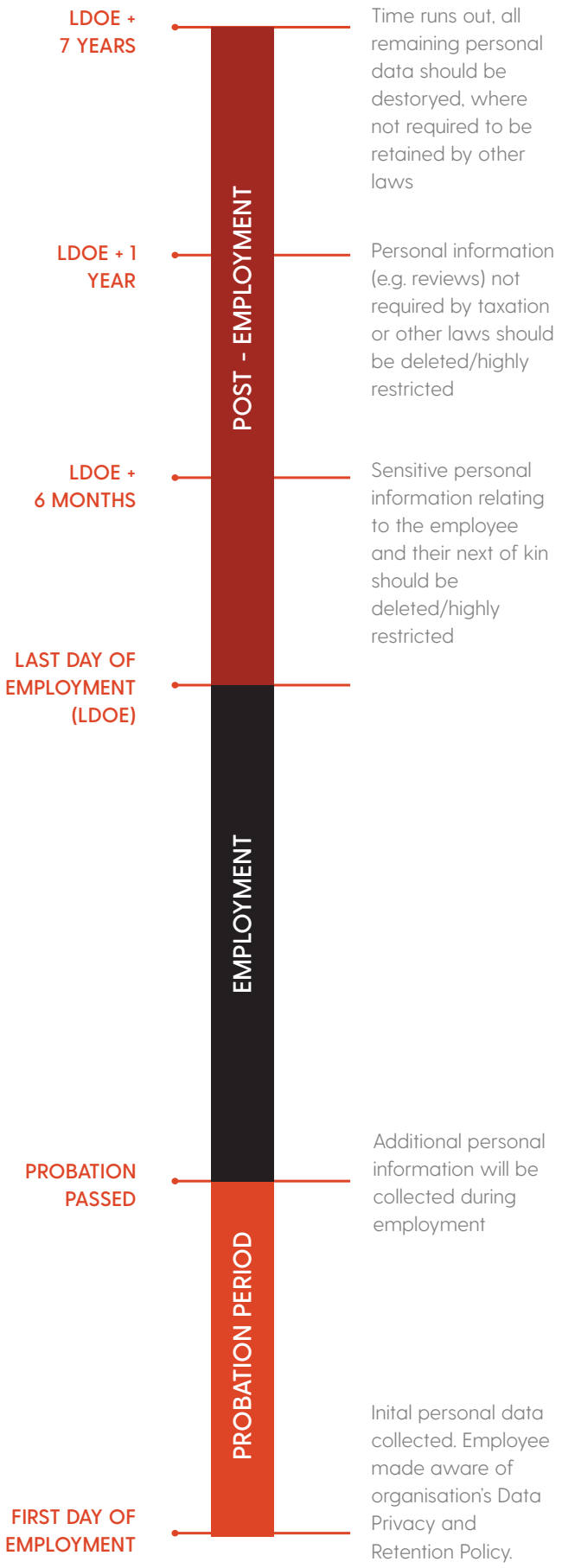
- Performance reviews, annual assessments, etc.
- Telephone number
- Bank account details
- Etc.

The best practice for this information is that it should be deleted within one year of the person leaving the organisation.

Access to Leaver's Personal Data

A further safeguard, to help protect the personal data of those who have worked for the organisation, particularly where their personal data is retained for an extended period; is to consider if access to the data should be further restricted, i.e. only senior members of the HR team are able to access information about those who have left the company.

Such an approach assists with compliance with both the GDPR and information security best practice, which together suggests that access to information should be minimised, it should only be given to those who require access as part of their role.



WORKING WITH YOUR DATA PROTECTION OFFICER

The GDPR requires some organisations to have a Data Protection Officer. Where the expertise and availability exist within the current staff then that role can be subsumed into the current capability. Where an organisation doesn't have the capacity in-house, then they have the option to either hire a data protection officer or to use a flexible and fractional service, such as the one offered by Fifth Step.

AN HR DATA CONTROLLER

The data protection officer is the person who is responsible for ensuring the organisation is GDPR compliant, and that staff has good levels of awareness of what data protection is, and what they should and shouldn't be doing. The Data Protection Officer is also the person who is responsible for working with the data protection authority should a data breach occur.

WHAT DOES A DATA PROTECTION OFFICER DO?

As detailed above the term data controller means the person or company who decides why, and the method and manner in which the data is collected. The idea behind the HR data controller is that they do this but within the specific scope of the HR department. This role might be undertaken by the head of HR and will require a close working relationship with the organisation's Data Protection Officer to help ensure that the HR department is maintaining compliance with the GDPR, in a demonstrable way.

REDUCING THE NUMBER OF EXPORTS & EXTRACTS

HR data, despite its sensitive nature, is very often extracted to be manually imported into other systems (payroll systems for example). Every such extract, export, and interface can increase the risks and the potential for a data breach.

When looking at your HR computer systems, and business processes, it is important to consider the number of extracts, along with the potential for a data breach or for data to be misused.

Where possible use integrated systems (combined HR and Payroll system for example), to minimise the number of opportunities for these kinds of issues to occur.

HR System Security Recommendations

The HR system that you have selected should help your organisation in its compliance with the GDPR the following are some of the security and compliance functions and features that your system should provide.

MULTI-FACTOR AUTHENTICATION

Multi-Factor Authentication is a means of adding security but requiring that the person enter a seemingly random group of numbers or characters that typically change every minute. This secondary code is typically provided by a smartphone application, by text message or by an electronic token.

Systems that store and provide access to personal data and sensitive personal data should adopt the highest levels of security, and therefore the ability for an HR system to support multi-factor authentication is highly recommended.

DATA ENCRYPTED IN TRANSIT

Data, when it's collected, or being moved between systems (in transit) should always be encrypted. This ensures that someone who is eavesdropping, will not be able to read the data without access to the decryption key.

The level of encryption applied should be sufficient, such that the decryption key cannot be easily guessed or broken. In practical terms, this means that web pages (for example) should be secured (https).

DATA ENCRYPTED AT REST

Data should be encrypted when it is stored on the hard drive of the computer servers, no matter if those servers are based in the offices of the organisation, or if they are part of a cloud service provides storage.

This requirement also extends to any data that is downloaded onto a user's computer. The data should be encrypted and inaccessible to an unauthorised user. In this case, the HR system should secure the files, but the organisation should also ensure that the hard drive is encrypted (FileVault on Apple computers or BitLocker on Windows computers).

PASSWORD POLICY

HR computer systems should ensure that the passwords selected by their users are complex enough that they cannot be easily guessed. This complexity and makeup of the password policy should ideally be configurable such that it can match the organisation's standards as they are applied to other corporate systems.

SESSION TIMEOUTS

Given the level of personal data that is accessible from an HR system, the system should not allow the user to log in and then remain inactive, without the system taking action and automatically logging them out.

COMPARTMENTALISATION OF DATA

Given that whilst much of the data collected by HR departments is personal data or personal sensitive data, there are different groupings within those categorisations. This means there is data that should be restricted to be accessed by only the most senior people within HR, and other data that a person's line manager may have access to. Equally as detailed in the best practices for data retention, data is likely to "expire" at different rates.

Your HR system should be flexible enough to accommodate all of these requirements, and ideally without major rework to the way the data is stored, structured or accessed.

DATA PRIVACY POLICY COMPLIANCE REPORTING

The more advanced HR systems are developing compliance reports that will allow your HR department to see and understand the exceptions to data privacy policy. For example, if data retention policies have exceptions, that may be fine if they're approved exceptions, if however, the policy breaches are as a result of a mistake, then such a report will provide actionable information that might otherwise not be spotted until the HR department was audited, or worse still it is discovered as part of a data breach investigation.