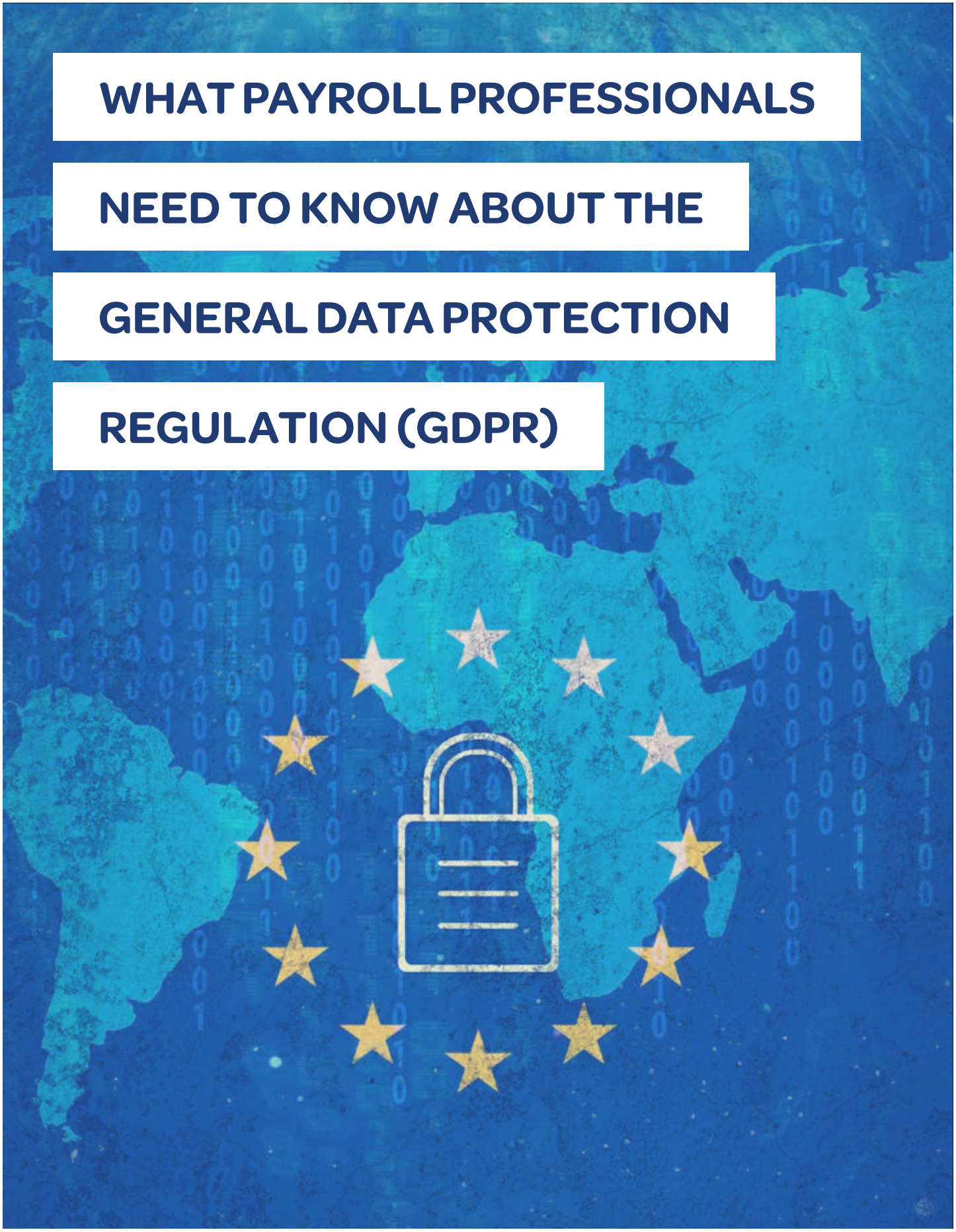
WHAT PAYROLL PROFESSIONALS NEED TO KNOW ABOUT THE GENERAL DATA PROTECTION REGULATION (GDPR)



Payroll Alliance
Learn Payroll

educating · informing · supporting

WHAT PAYROLL PROFESSIONALS NEED TO KNOW ABOUT THE GENERAL DATA PROTECTION REGULATION (GDPR)

Published by:

The Learn Centre

3a Penns Road, Petersfield, Hampshire GU32 2EW

Telephone: 01798 861111 Fax: 01798 861112

E-mail: info@learnpayroll.co.uk

Web Site: www.learnpayroll.co.uk

Contents

Introduction

This white paper examines the impact of the new General Data Protection Regulation (GDPR) specifically as it relates to HR and payroll professionals.

On 25 May 2018, the GDPR legislation will change the legal requirements of how all organisations in the EU (with a very few exceptions) will be expected to ensure the security of personal data. This will include owner-managed businesses, one-man bands and SMEs.

The GDPR will have far-reaching implications for all parts of the business, and significantly, also covers the protection of personal employee data handled by HR and payroll teams. In many cases these teams hold the majority of personal data, especially data classified as "sensitive".

Organisations that are already compliant with current data protection legislation will be in a good place from which to start implementing measures for GDPR compliance.

However, there are important new requirements that will involve high levels of resource.

To ensure compliance, organisations should already be assessing their own data handling procedures.

The impact of the GDPR on HR and payroll is wide reaching.

This is especially relevant for organisations where personal employee data is shared with other third parties such as:

- a parent company transferring data outside of the EU
- HR service providers such as payroll software companies, pension, company car, voucher scheme companies – including organisations where an employer shares personal employee data at the request of the employee, for example, to benefit from a salary sacrifice programme
- service providers for non-remuneration related purchases made by employees, such as business travel and company credit cards that are monitored by payroll to ensure P11D compliance and where employee data – such as credit card details – are provided to the third party
- future employers requiring evidence of an employee's remuneration, pay increases, bonuses etc.

In each of these cases, organisations must demonstrate that their own policies and procedures are adequate to ensure compliance with the GDPR. It is also the responsibility of the Controller to ensure that each third-party organisation is also compliant with the GDPR and that safeguards are in place to satisfy the requirements.

The only exclusion is where data is shared with a government organisation, such as HMRC, where compliance to the GDPR can be assumed through statutory controls and audits in place.

The impact on employee and payroll data should not be underestimated.

With compliance likely to require serious investment in terms of time and organisational resources, it is essential that organisations start preparing now to meet the 25th May 2018 compliance deadline. As part of this, HR and payroll teams must take specific action now to ensure that protection of employee data falls within the requirements of the GDPR.

The penalties for non-compliance are the same whether the breach relates to customer or employee data and can be a maximum of €20,000,000 or 4% of the company's turnover, whichever is the larger.

Organisations may also be subject to enforcement action, which could damage their public reputation and their business, if data protection is not made a cornerstone of their organisational practices.

This white paper provides an overview of the key requirements as well as guidance on key actions to be taken before 25th May 2018 to ensure payroll data is compliant with GDPR.

However, it cannot be used as a definitive guide.

It is essential that payroll professionals seek detailed advice and training from experts, throughout their preparation process, to ensure they are fully compliant.

Part I: Understanding GDPR

What is the GDPR?

The General Data Protection Regulation (GDPR) is new legislation introduced by the European Union which will take effect across the European Union (EU) on 25th May 2018.

At that point, all organisations in the European Union that handle personal information will be expected to be compliant with its regulations. They will be liable to sanctions if they have not taken steps to demonstrate how they are protecting personal data in relation to the terms of the GDPR.

The GDPR supersedes the UK's 1998 Data Protection Act although everything under the Data Protection Act we have today will remain.

Brexit does not change the introduction of the GDPR in the UK. The Information Commissioner's Office (ICO) has also confirmed that the GDPR will have a significant impact on the future development of data protection law in the UK and an act will be put in place to mirror the GDPR in the future for the United Kingdom.

Why was the GDPR introduced?

The goal of the GDPR is to protect individuals for example, employees and customers, and their data as it is held and processed by businesses, service providers and other organisations.

The GDPR aims to:

- keep pace with changes in the digital environment and in the types of personal data kept by companies, how it is shared and traded in a global economy
- create one consistent standard for data security across Europe
- improve customer and employee confidence
- simplify the free flow of personal data in the EU while ensuring its security and protecting privacy
- protect individuals when their personal data is transferred outside of the EU

Who is responsible?

The GDPR applies to 'controllers' and 'processors'. The controller decides how and why personal data is processed and the processor acts on the controller's behalf. The data controller will typically be your company but can be an individual – the data processor could be the organisation that manages company pensions or the network provider for company smart phones but could also be the payroll or HR assistant.

The GDPR places specific new legal obligations on processors: for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach.

However, if you are a controller, you are not relieved of your obligations where a processor is involved. The GDPR places further obligations on you to ensure your staff are fully trained to work within the obligations and contracts with processors and ensure they comply with the GDPR. It states: "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

What information does the GDPR apply to?

The GDPR is much more wide-ranging than previous legislation and applies to any 'personal data' that can identify an individual which could include online identifiers such as an IP address.

More significant than the changes to the types of data included, the most significant addition is the accountability principle. The GDPR requires you to show how you comply with the principles, for example by documenting the decisions you take about a processing activity.

The GDPR applies to both automated personal data and to manual filing systems where personal data is accessible according to specific criteria.

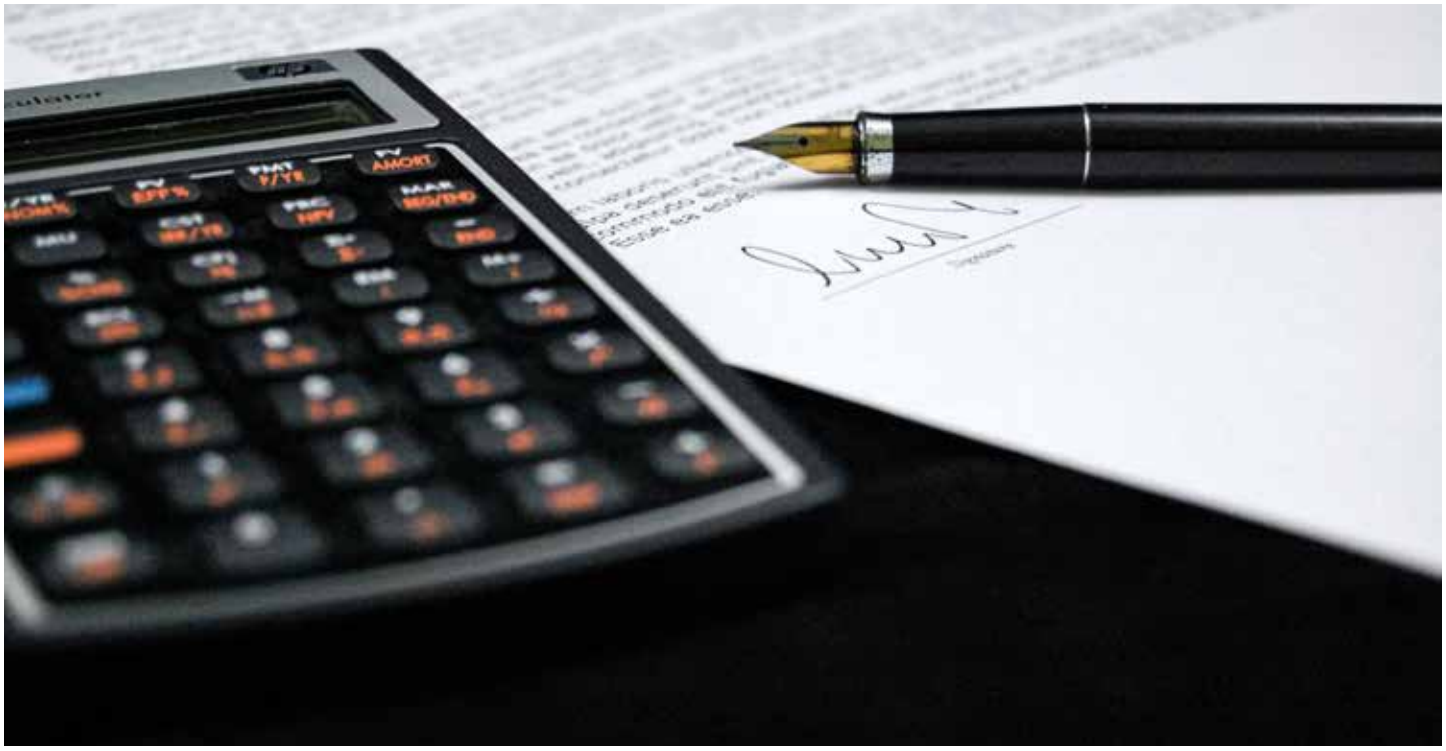
Personal data that has been pseudonymised, e.g. key-coded, can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to an individual.

The GDPR refers to sensitive personal data as "special categories of personal data" and expands the categories to include, for example, genetic and biometric data where processed to uniquely identify an individual. This constitutes the "highest" risk data to the individual should there be an issue or breach around its protection and with HR and Payroll could relate to health and sickness, ethnic origin, trade union membership as well as numerous other areas of sensitive data.

Personal data relating to criminal convictions and offences also come under this category and similar safeguards apply to their processing.

The GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- accurate and where necessary, kept up to date
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures



Is consent necessary?

You can rely on other lawful bases apart from individual consent, for example, where processing is necessary for the purposes of your organisation's or a third party's legitimate interests, as well as to fulfil a contract, which would be the normal reason with payroll and HR information.

If you use individual consent to process personal data, it must be verifiable, and individuals generally have more rights where you rely on their consent including the right to withdraw the said consent.

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action, or in other words, a positive opt-in, consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent. Public authorities and employers will need to take care to ensure that consent is freely given. With payroll and HR this will mean a review of your current privacy notice to not only your staff but also anyone sending in personal information looking for a job, including C.V.'s

Children's personal data

The GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking.

Payroll and HR departments will need to check and verify the age of individuals whose data they hold. This could be in relation to children on work experience or pension contacts as examples.

The GDPR sets the age of a child as under 16, although there is an option for EU countries to lower this to a minimum of 13 if required. If you hold personal data for someone under this age you will need to get consent from a person holding 'parental responsibility', a child cannot give their own "opt in" consent.

Consent must be verifiable and you will need to provide a children's privacy notice to the child in plain English, written in language the child can understand.

From a payroll perspective, ensuring protection of children's data could also be relevant for organisations that offer benefits such as childcare vouchers or childcare facilities at work.

Individual's rights

The GDPR significantly extends an individual's rights regarding their data and requires organisations to respond to requests from individuals free of charge and generally within 30 days:

- The right to be informed
  - Organisations are obliged to provide 'fair processing information', typically through a privacy notice depending on whether you obtained the personal data directly from individuals and how their data is being processed
- The right of access
  - Individuals will have the right to access their personal data and have access to 'supplementary information' to verify the lawfulness of the processing. Organisations will need a method of proving this information within the required timescales. This could be a key challenge within HR and payroll, firstly, to ensure the information can be provided within the timescales, but also that it could be held in a number of systems and resources which will need to be accessed and accumulated.
- The right to rectification
  - Individuals are entitled to have personal data rectified if it is inaccurate or incomplete. HR and payroll will be required to have a channel of communication should an individual request rectification and an audit process to ensure they changes are made and logged.
  - If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate and again payroll and HR will be required to have an audit log to show compliance. These could be payroll or HR providers, pension providers or private healthcare providers, to name just a few.
- The right to erasure
  - An individual may request the deletion or removal of personal data where there is no compelling reason for its continued processing, for example, where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed. The responsibilities and controls for this would be the same as rectification for the payroll and HR departments.

- The right to erasure (continued)
  - If you have disclosed the personal employee data in question to third parties, you must inform them about the erasure of the personal data.
- The right to restrict processing
  - Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future. The effect of this on payroll and HR could provide a challenge should data continue to be "stored". There will be a need to supress the data stored in payroll systems and alike to ensure they are not processed. An example could be a challenged NI number which a payroll department would not want to be included on reports or sent through the HMRC on RTI returns.
  - If you have disclosed the personal data in question to third parties, you must inform them about the restriction on the processing of the personal data.
- The right to data portability
  - Individuals may obtain and re-use their personal data for their own purposes by moving, copying or transferring it easily from one IT environment to another in a safe and secure way.
  - This right only applies to personal data an individual has provided to a controller, where the processing is based on the individual's consent or for the performance of a contract, and when processing is carried out by automated means. There may be a need to review payroll and HR systems to ensure there is a mechanism going forward to manage this requirement.
- The right to object
  - Individuals can object to personal data being used for:
    - processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling) if they can object on "grounds relating to his or her particular situation".
    - processing for purposes of scientific/historical research and statistics again if they have "grounds relating to his or her particular situation".
    - direct marketing (including profiling): you must stop processing personal data for direct marketing purposes as soon as you receive an objection. There are no exemptions or grounds to refuse
  - You must inform individuals of their right to object "at the point of first communication" and in your privacy notice.
  - The objection would only be valid with payroll and HR should you no longer require or have a legitimate reason for processing the data going forward from the objection.
- Rights in relation to automated decision-making and profiling
  - This safeguards individuals against the risk that a potentially damaging decision is taken without human intervention.
  - You must ensure that individuals are able to:
    - obtain human intervention
    - express their point of view
    - obtain an explanation of the decision and challenge it.
  - The right does not apply if the decision is necessary for entering into or impacts the performance of a contract between you and the individual, is authorised by law (e.g. for the purposes of fraud or tax evasion prevention) or is based on explicit consent.
  - The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of an individual, to analyse or predict the individuals:
    - performance at work
    - economic situation
    - health
    - personal preferences
    - reliability
    - behaviour
    - location
    - movements
  - As you can see from the examples, there are many automated processes within the HR and payroll environment and as such as part of the preparation for compliance there will be a need to review these and ensure there is availability of a manual or human intervention should it be required or requested by the individual.
  - When processing personal data for profiling purposes, you must ensure that appropriate safeguards are in place, for example, ensuring processing is fair and transparent.

Accountability and Governance

The new accountability principle requires you to demonstrate that you comply with the principles and states explicitly that this is your responsibility.

You are expected to put into place comprehensive but proportionate governance measures. Privacy impact assessments and privacy by design and default are now legally required in certain circumstances. It is key, therefore, that payroll and HR departments work with their data controller to ensure that all processes carried out are recorded, reviewed and where required impact assessments are completed to review compliance and to minimise risk to the individual especially when relation to special category data held.

You must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply.
- Maintain relevant documentation on processing activities. Organisations with more than 250 employees have additional obligations.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default.
- Use data protection impact assessments where appropriate both as part of archiving compliance but also going forward. A good example could be when changing payroll provider or system.

You can also adhere to approved codes of conduct and/or certification schemes.

What needs to be recorded

You must maintain internal records of processing activities. You may be required to make these records available to the relevant supervisory authority for purposes of an investigation.

You must record the following information:

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of the processing.
- Description of the categories of individuals and categories of personal data.
- Categories of recipients of personal data.
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place.
- Retention schedules.
- Description of technical and organisational security measures.

Data protection by design and by default – the DPIA

Organisations now need to demonstrate that they have implemented technical and organisational measures to show that they have considered and integrated data protection into their processing activities.

Data protection impact assessments (DPIAs) or privacy impact assessments (PIAs), can help organisations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA will allow organisations to identify and fix problems and risks at an early stage, reducing the associated costs and damage to reputation that might otherwise occur.

A DPIA is obligatory when:

- using new technologies such as payroll and HR systems
- the processing is likely to result in a high risk to the rights and freedoms of individuals such as storing and processing sickness certificates

- performing large scale monitoring
- processing large amounts of personal data regularly within an organisation. This could incorporate all data held and processed by an HR and payroll department in a large organisation

What information should the DPIA contain?

- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller.
- An assessment of the necessity and proportionality of the processing in relation to the purpose.
- An assessment of the risks to individuals.
- The measures in place to address risk, including security and to demonstrate that you comply.
- A DPIA can address more than one project.

Appointing a Data Protection Officer (DPO)

As part of the GDPR, you must appoint a data protection officer (DPO) if you:

- are a public authority (except for courts acting in their judicial capacity)
- carry out large scale systematic monitoring of individuals (for example, online behaviour tracking)

or

- carry out large scale processing of special categories of data or data relating to criminal convictions and offences.

Any organisation is able to appoint a DPO. Regardless of whether the GDPR obliges you to appoint a DPO, you must ensure that your organisation has sufficient staff and skills to discharge your obligations under the GDPR. The appointment of a DPO does not exempt individual within the payroll and HR teams of the responsibilities under the GDPR. The DPO however should be independent as the role requires the ability to have an overview of the entire organisations processes and as such would not be likely to be a role carried out by the HR or payroll department due to their involvement with the processing itself.

Codes of conduct and certification mechanisms

The GDPR endorses the use of approved codes of conduct and certification mechanisms to demonstrate your compliance.

Signing up to a code of conduct or certification scheme is not obligatory.

Codes must be approved by the relevant supervisory authority, and, where the processing is cross-border, by the European Data Protection Board (the EDPB).

Member states, supervisory authorities, the EDPB or the Commission are required to encourage the establishment of certification mechanisms to enhance transparency and compliance with the Regulation.

What if there is a breach?

The GDPR will introduce a duty on all organisations to report certain types of data breach to the relevant supervisory authority, and in some cases to the individuals affected, within 72 hours of discovery.

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation or financial loss.

This has to be assessed on a case-by-case basis.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you must notify those concerned directly.

There are several specific requirements for notifying a breach for example, the nature of the personal data breach, the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned.

It will be critical given the data processed that all payroll and HR staff are fully trained and aware of what a breach represents as well as the process that will be required should a breach occur.

Transferring data abroad

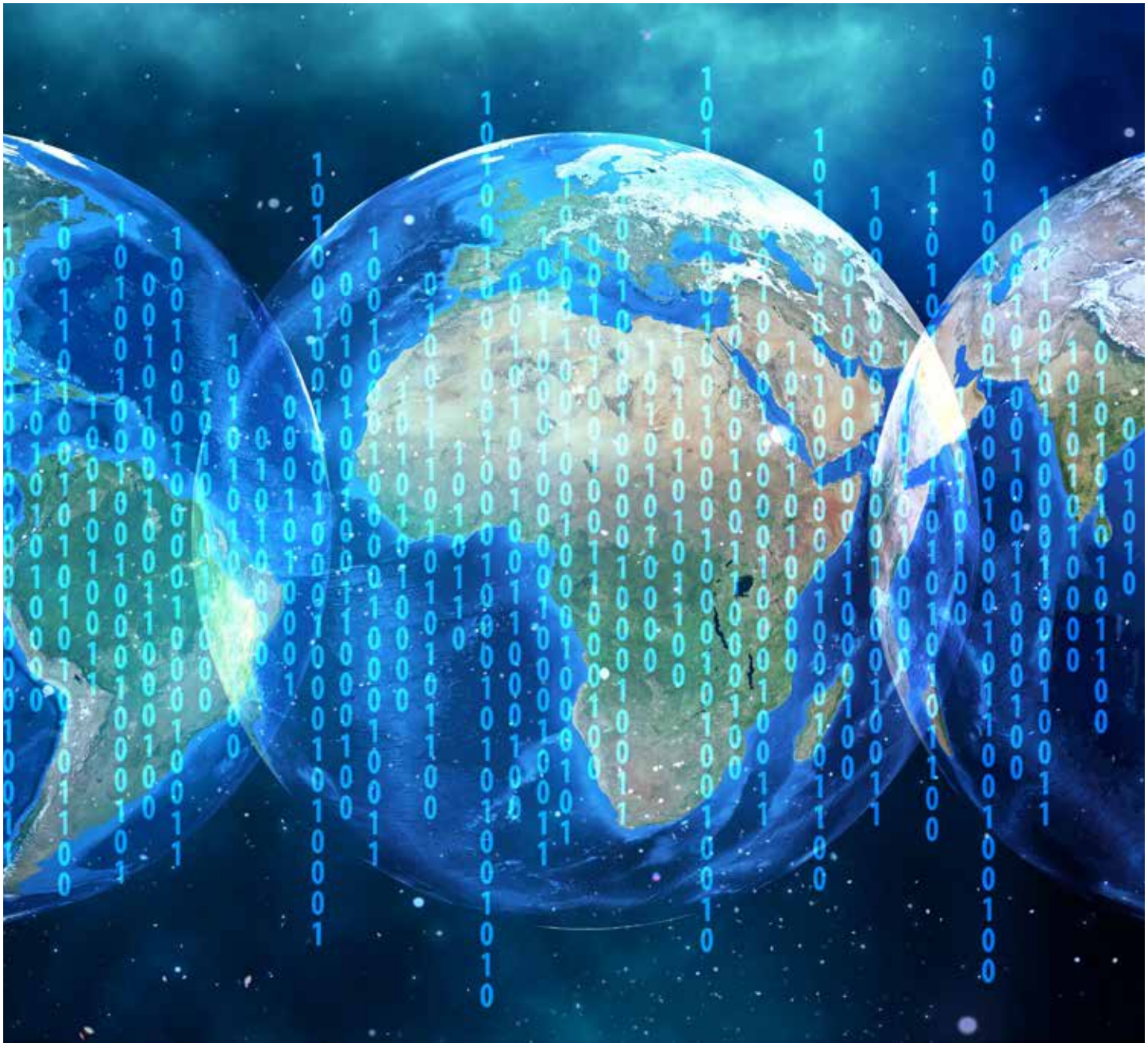
The GDPR restricts the transfer of personal data outside the European Union, to third countries or international organisations, in order to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

This includes transfers to a parent organisation based outside the EU.

Personal data may only be transferred outside of the EU in compliance with the conditions for transfer set out in the GDPR. Transfers may be made where the Commission has decided that a third country, a territory or one or more specific sectors in the third country, or an international organisation ensures an adequate level of protection.

You may transfer personal data where the organisation receiving the personal data has provided adequate safeguards. Individuals' rights must be enforceable and effective legal remedies for individuals must be available following the transfer.

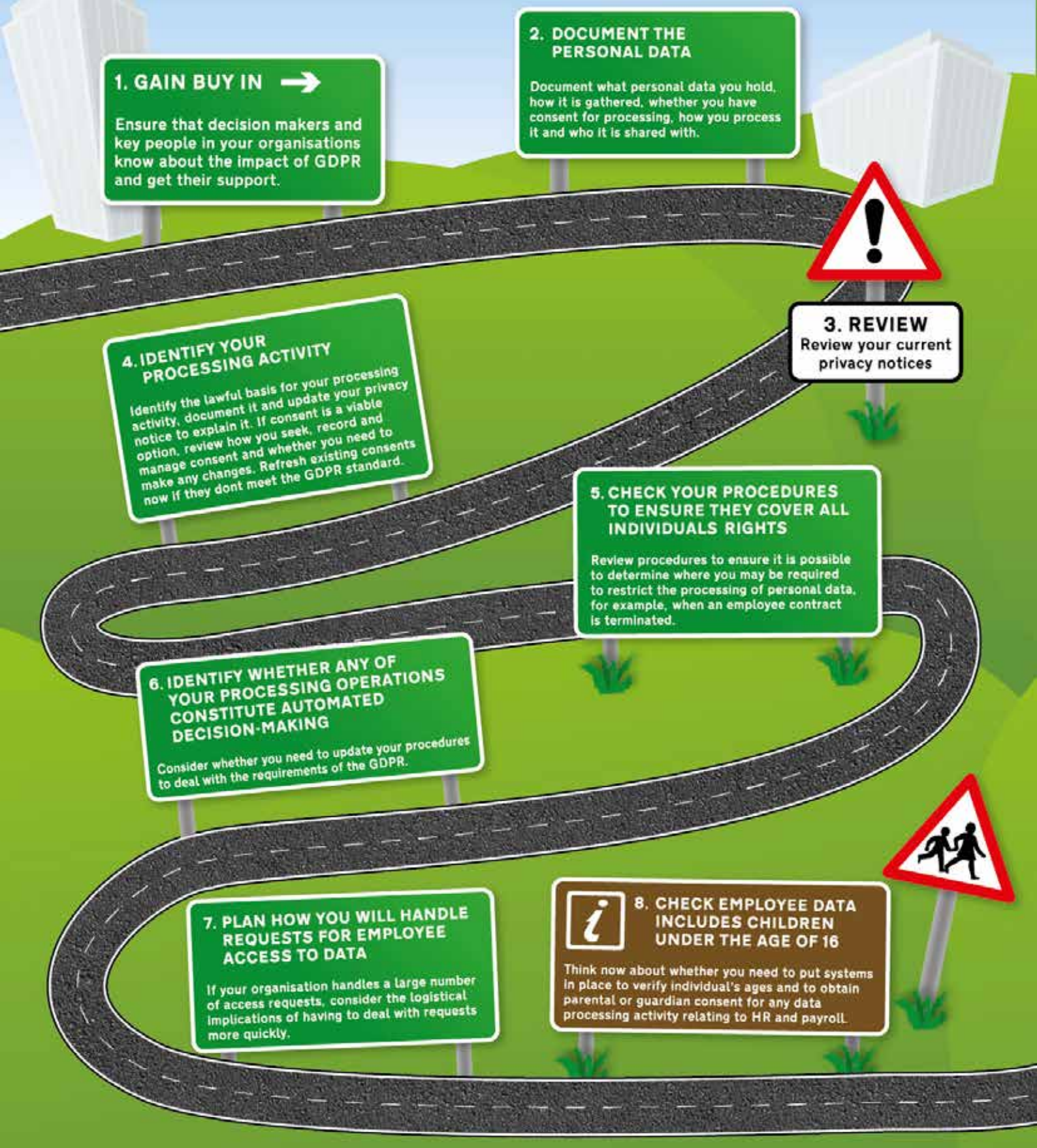
The GDPR provides derogations from the general prohibition on transfers of personal data outside the EU for certain specific situations, for example, where the transfer is made with the individual's informed consent or necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request.



Part II: How To Prepare For The GDPR

There are 15 steps you should take now to prepare for the General Data Protection Regulation (GDPR) that will apply from 25th May 2018.

It is essential to plan your approach to GDPR compliance now.



DETERMINE YOUR LEAD DATA PROTECTION SUPERVISORY AUTHORITY AND DOCUMENT THIS IF YOUR ORGANISATION OPERATES IN MORE THAN ONE EU MEMBER STATE.

If this applies to your organisation, you should map out where your organisation makes its most significant decisions about its processing activities. This will help to determine your main establishment and therefore your lead supervisory authority.

12

DESIGNATE SOMEONE TO TAKE RESPONSIBILITY FOR DATA PROTECTION COMPLIANCE AND ASSESS WHERE THIS ROLE WILL SIT WITHIN YOUR ORGANISATION'S STRUCTURE AND GOVERNANCE ARRANGEMENTS.

You should consider whether you are required to formally designate a Data Protection Officer (DPO).

11

ASSESS THE SITUATIONS WHERE IT WILL BE NECESSARY TO CONDUCT A DPIA AND ESTABLISH WHO WILL DO IT, WHO NEEDS TO BE INVOLVED AND WHETHER THE PROCESS WILL BE RUN CENTRALLY OR LOCALLY.

Ensure privacy considerations are embedded in both operational and strategic HR and payroll to demonstrate that you have data protection by design and by default.

10

ENSURE YOU HAVE THE RIGHT PROCEDURES IN PLACE TO DETECT, REPORT AND INVESTIGATE A PERSONAL DATA BREACH

Assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred.

9

REVIEW STAFFING REQUIREMENTS FOR DATA PROTECTION COMPLIANCE. PROVIDE TRAINING FOR ALL STAFF, AND SPECIFIC TRAINING FOR INDIVIDUALS WITH DATA PROCESSING RESPONSIBILITIES FOLLOWING THE INTRODUCTION OF NEW DATA PROTECTION POLICIES AND PROCEDURES.

This will include policies and procedures specifically related to data protection (e.g. employee data protection policies and subject access procedures), as well as all other HR policies and procedures that contain data processing elements (e.g. sickness absence policies, employee monitoring policies and employee reference policies). These will need to contain clear and practical guidance on GDPR compliance. Review information notices for employees and job applicants, and update them to comply with the more detailed information requirements under the GDPR.

13

ENGAGE WITH PRODUCT OWNERS/SUPPLIERS EARLY ON.

Review and audit commissioning software and data housing suppliers and other providers and update contracts. Also review and if necessary revise legacy contracts to consider mandatory terms. Consider negotiating on apportionment of liability.

14

IMPLEMENT REGULAR AUDITS AGAINST DEFINED METRICS.

For example the number of privacy complaints, completion of training and data breaches suffered to assess the ongoing success of the compliance programme.

15

Conclusion

The aim of this white paper has been to provide an overview of how the new data protection requirements of the GDPR will impact payroll departments and the steps they will need to take to prepare for the changes to ensure compliance.

The GDPR brings significant, new and onerous data protection responsibilities to all organisations based in the EU and the penalties for non-compliance to the new rules are severe.

It is vital that organisations act now, and where necessary, seek help and support from experts, to protect themselves from the risks of prosecution after 25th May, 2018.

In particular, ensure you offer training and support to payroll teams on the detailed requirements of the GDPR so that they are best placed to prepare adequately.

The Learn Payroll GDPR half-day certified course has been specially designed to meet the needs of payroll professionals, and includes helpdesk support and a detailed user manual. Call 01798 861111 or email info@learnpayroll.co.uk for more information.