How To Prepare For The GDPR

The **Learn Payroll GDPR half-day course** has been specially designed to meet the needs of payroll and HR professionals and includes helpdesk support and a detailed user manual.

Call 01798 861111 or email **info@learnpayroll.co.uk** for more information.

Payroll Alliance
Learn Payroll

educating · informing · supporting

Tel: 01798 861111 **Email:** info@thelearncentre.co.uk

Web: www.learnpayroll.co.uk

1. GAIN BUY IN

Ensure that decision makers and key people in your organisations know about the impact of GDPR and get their support.

2. DOCUMENT THE PERSONAL DATA

Document what personal data you hold, how it is gathered, whether you have consent for processing, how you process it and who it is shared with.

3. REVIEW

Review your current privacy notices

4. IDENTIFY YOUR PROCESSING ACTIVITY

Identify the lawful basis for your processing activity, document it and update your privacy notice to explain it. If consent is a viable option, review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they dont meet the GDPR standard.

5. CHECK YOUR PROCEDURES TO ENSURE THEY COVER ALL INDIVIDUALS RIGHTS

Review procedures to ensure it is possible to determine where you may be required to restrict the processing of personal data, for example, when an employee contract is terminated.

6. IDENTIFY WHETHER ANY OF YOUR PROCESSING OPERATIONS CONSTITUTE AUTOMATED DECISION-MAKING

Consider whether you need to update your procedures to deal with the requirements of the GDPR.

7. PLAN HOW YOU WILL HANDLE REQUESTS FOR EMPLOYEE ACCESS TO DATA

If your organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly.

8. CHECK EMPLOYEE DATA INCLUDES CHILDREN UNDER THE AGE OF 16

Think now about whether you need to put systems in place to verify individual's ages and to obtain parental or guardian consent for any data processing activity relating to HR and payroll.

9

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.

10

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.

11

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).

12

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.

13

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.

14

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.

15

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.