PAY DASHBOARD
A part of experian

Payslips and GDPR

Let's get the facts straight

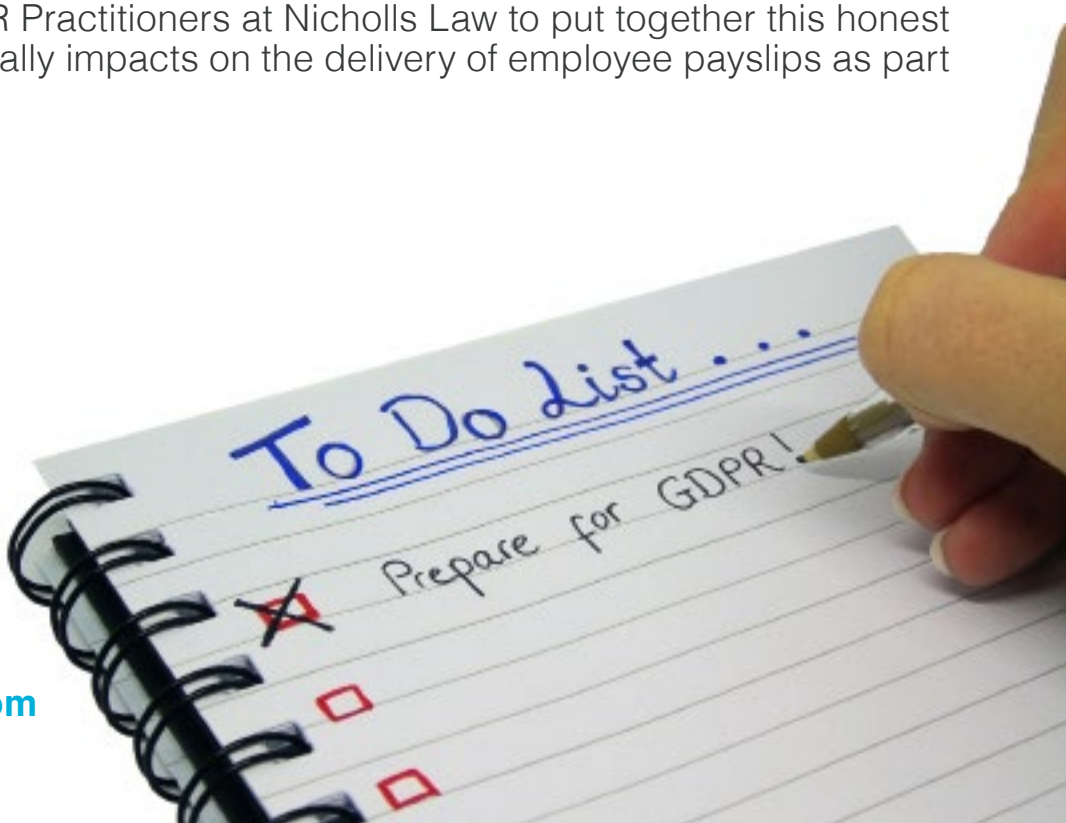
Introduction

While GDPR has been heralded as a huge change in the way in which businesses process data, the reality is far less dramatic than the headlines about multi-million pound fines. GDPR is not a revolution in data laws, it is just updating the guidelines set in the Data Protection Act of 1998 - a long overdue update given the changes in digital technology in last 20 years.

In this guide we will look at the impact of GDPR on payslip distribution including addressing the three biggest areas of concern:

1. Emailed payslips and their compliance status under GDPR
2. The potential fines for breach of data in relation to payslips
3. The lawful basis for handling data when delivering payslips

We consulted with GDPR Practitioners at Nicholls Law to put together this honest outlook on how GDPR really impacts on the delivery of employee payslips as part of the payroll process.



FIND OUT MORE:
www.paydashboard.com

PAY DASHBOARD
A part of experian

MYTH #1 - "Emailed payslips are not GDPR compliant."

THE FACTS:

Nobody has definitively said that emailed payslips are NOT GDPR compliant.

This is an assumption being made in the industry because Article 32 of the GDPR states *"the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk"*.

While there is a school of thought that email is probably not an 'appropriate measure' (more on this later), this has not been confirmed either way by anyone at this time.

MYTH #2 - "I'll be fined €20,000,000 for a payslip-related GDPR breach"

THE FACTS:

The biggest fines are extremely unlikely in the case of an employee payslip being delivered without appropriate technical measures.

These big fines will probably be for gross breaches of data protection and infringements to subject rights. The ICO have stated that fines will be used "proportionately and judiciously" - and not to make early examples of businesses for minor infringements.

So are you going to be fined £millions if an employee's emailed payslip is intercepted? In short, probably not - but we don't want to say definitely not in case we are proved wrong.

FIND OUT MORE:
www.paydashboard.com

PAY DASHBOARD
A part of experian

MYTH #3 - "You need an employee's consent to use any software to give them a payslip."

THE FACTS:

There are allowances for processing data under a lawful basis.

Much has been spoken about the need for consent in processing data. However, as you are legally required to provide an employee with a written pay statement on or before payday (Employment Rights Act 1996), this legal requirement precedes the need for employees to consent to you processing their data for the purposes of producing a payslip.

What you **must** be able to demonstrate is that the way that you hold and process this data is GDPR compliant, and this extends to the companies or suppliers that you outsource any of the payroll process to.

This doesn't mean that businesses should be complacent when it comes to payslip delivery

The ICO may take a dim view if a breach of employee pay data or payslips occurred alongside other breaches. Negligence in multiple areas of data protection has been identified by many sources as a potential scenario where larger fines might be levied, especially as it could be argued that the organisation was not "demonstrating compliance" - a key area of the GDPR.

It's a case of limiting your liabilities - where you can find an easy solution, it's best to do it. You then protect yourself from further scrutiny in the event of a breach elsewhere. The more that you can demonstrate GDPR compliance in your business, the better.

It means that should the ICO come knocking, you can show multiple areas of compliance with regards to taking appropriate technical and organisational measures.

FIND OUT MORE:
www.paydashboard.com

PAY DASHBOARD
A part of experian

MYTH #4 - "Multi-factor authentication is mandatory in ensuring GDPR compliance."

THE FACTS:

Multi-factor authentication is not mandatory, but is suggested

There are no technical requirements specified in GDPR, but a legal framework that requires that appropriate measures need to be in place to protect personal data. To that end, multi-factor authentication might be an attractive option as an added layer of security.

MYTH #5 - "AI lessens the potential of a data security risk."

THE FACTS:

Any system can be susceptible to a data security breach

Any system that possesses payslip data can violate GDPR's data protection requirements in the event of a security breach. However, AI can enhance data security measures, for example by detecting anomalies or predicting potential security breaches.

A few more things to note about AI and GDPR:

1. Organisations should only collect and process the minimum amount of data necessary for the intended purpose, (payslip processing) and ensure that AI algorithms are designed to focus on specific, legitimate purposes.

2. GDPR grants individuals rights regarding automated decision-making, including the right to human intervention, explanation of decisions, and the right to challenge automated decisions. If AI systems are used to make decisions based on payslip data, organisations must ensure that individuals' rights are respected and provide mechanisms for recourse if automated decisions have significant impacts.

3. AI-related payslip processing activities could potentially be a risk for individuals' rights. Therefore, a Data Protection Impact Assessment should be carried out prior to the deployment of any AI system to identify and address privacy risks associated with AI technologies.

For a more comprehensive look at AI and GDPR, please visit the **ICO website**.

There are no technical requirements specified in GDPR, but a legal framework that requires that appropriate measures need to be in place to protect personal data. To that end, multi-factor authentication might be an attractive option as an added layer of security.

Tick the GDPR box for payslip delivery and then get back to the bigger, more serious issues

Here's the GDPR payslip lowdown:

1. Payslips contain personal and identifiable information. Therefore the GDPR applies to payslip delivery.
2. Emailed payslips are not expressly forbidden. Whether they represent "appropriate technical measures" however, is questionable.
3. In the event of a breach or being audited by the ICO, you need to demonstrate compliance. Selecting a GDPR-compliant payslip delivery mechanism and supplier would be one easy way of proving compliance.

The simple answer... You can probably continue emailing payslips for now - but it is a potential area of risk, and there are easy solutions out there like the one offered by PayDashboard that will help you to tick off that risk area quickly and move on to bigger issues.

How PayDashboard ensures GDPR compliance for your business

PayDashboard integrates with your existing payroll software in order to deliver payslips to your employees. We help you to meet your GDPR compliance obligations in the following ways:

1. PayDashboard allows users to access payslips via a secure online portal.
2. PayDashboard does not email payslips, users receive email notifications that a new payslip is available but must login to view their payslips.
3. To register new users on the site we send them an email link to register. When they register they must confirm a piece of personal information such as their NI number, preventing someone who intercepted the email from falsely accessing the account.
4. PayDashboard users can enable additional multi-factor authentication upon login to further secure their account. Login is then only possible with the user's email address, password and a 6 digit code generated on their phone.
5. As a company we are ISO 9001 and 27001 certified, registered with the ICO, and an Experian product, ensuring we remain strictly compliant as mandated by the business.