PAY DASHBOARD

Payslips and GDPR

Password-protected emails

Introduction

There is nothing in the GDPR legislation that states it is no longer permissible to email payslips. Article 32 of the GDPR states that "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk".

However, many companies are taking the stance that simply emailing a payslip to an employee does not show "appropriate technical measures" and are addressing the way that they distribute payslips to employees. One potential solution that has arisen is password-protecting payslips before emailing them to the employee. Arguably, this does show that the company has taken technical steps to improve data protection, and is certainly better than simply emailing unprotected payslips.

There are, however, still some GDPR compliance risks and other concerns when adopting this approach.

This guide will address these issues and provide a checklist of questions for companies to consider when reviewing their payslip delivery options and emailing payslips.

FIND OUT MORE:
www.paydashboard.com

PAY DASHBOARD

The BIG GDPR concern - how do you give an employee their password?

The biggest risk area that companies must address if they plan on emailing payslips with password-protection, is how they are going to tell their employees what their password is.

You can not email them the password!

Email is not secure. By transmitting both the password and the payslip via email to the same email address, you risk a data breach. You should either:

- Communicate the password to the employee in a different way - such as verbally or by post
- Email their password to a secondary email address not used for their payslips
- Let employees select their own password

The data protection concern - password access

There are data protection concerns if you choose to allow employees to set their own password. Despite advice to the contrary, many people use the same password or very similar passwords for more than one online account - their emails, social media, banking, online shopping etc.

If any employee sets their own password for their payslips, and then forgets it, they need some way to either reset their password or be reminded of it.

If the solution is that HR have access to passwords in order to remind employees of them, then this is a data protection issue. Your HR team will have access to unencrypted passwords on a per employee basis, and probably the employee's email address as well. This puts an unnecessary risk and strain on your HR team.

The security concern - password storage

You must securely store your employees' payslip passwords - and ideally encrypt them. If the database or file holding your employees' passwords were compromised then your company would be responsible for the data breach.

PAY DASHBOARD

The questions to ask when considering emailing password-protected payslips

How do we tell an employee what their password is?

Does an employee set their own password, or is their password auto-generated?

What are the complexity requirements of the password? (Complex passwords containing a mix of letters, symbols and numbers, upper and lowercase, and with a minimum length are most secure.)

What is the process if an employee forgets their password?

Can an employee automatically reset their password or get a password reminder?

What is the involvement of HR/Payroll Teams in password resets or reminders and what are the time implications of this?

How do you change the email address that an employee's payslips are sent to?

Can historic payslips be resent to an employee - for example if they lose access to the email account their payslip was sent to or accidentally deleted a payslip?

Is there an audit log available to HR showing which payslips have been delivered? Can you also track opens?

If an email address is incorrect and the payslip could not be delivered, are HR notified?

If a payslip could not be delivered due to a full inbox or temporary server unavailability - are HR notified?

FIND OUT MORE:
www.paydashboard.com

PAY DASHBOARD

In summary

1. While password-protected emailed payslips may be GDPR compliant, there is still danger around communication of passwords and data security.
2. You should be aware of the other implications of emailed payslips, particularly in terms of workload for your HR team.

The simple answer... If you are moving to a digital solution such as email, then you should consider a cloud-based portal like PayDashboard instead. Portals offer more convenience, reduced administration and better security than emailed payslips.

Ensure GDPR compliance when it comes to payslips

PayDashboard integrates with your existing payroll software in order to deliver payslips to your employees via an easy to use and secure online portal. We help you to meet your GDPR compliance obligations in the following ways:

1. PayDashboard allows users to access payslips via a secure cloud-based portal.
2. New users are sent an email to register their account, but must verify their identity during registration process by confirming a piece of personal information such as their NI number (preventing someone who intercepted the email from falsely accessing the account) before they set up a secure password.
3. If a user's email address is changed in the portal they must re-verify their details the next time they log in.
4. User passwords are stored in our database using hashing. Hashing is a one-way transformation of a password, turning it into another string of digits and making it practically impossible to turn the hashed password back into the original password. No PayDashboard users, including our development team, can access the original password.
5. Password resets in PayDashboard are fully automated and accounts are locked after too many failed attempts.
6. As a company we are ISO 9001 and 27001 certified, registered with the ICO, we comply with the Data Protection Act, and we are working with Nicholls Law to ensure ongoing GDPR compliance in all areas of our business.