



Payslip Compliance with **GDPR**

**Ensuring your Payslips are
compliant with GDPR.**



GDPR changes

GDPR changes that came into effect in May 2018 updated the previous guidelines that were set in the 1998 Data Protection Act. As the payroll process manages sensitive employee information, the delivery of payslips could be impacted by the new changes to GDPR.

Frequently asked questions about payslips and GDPR

Can companies continue to email payslips to employees?

Companies are **legally required** to provide employees with payslips prior to or on payday. Most companies currently provide this information via email, so there is a concern that payslips contain private information and therefore should not be delivered using email. There is no definitive answer on emailing payslips, but there is a clause in the GDPR guidelines stating “**appropriate technical measures**” must be followed. Companies must ensure compliance with new GDPR regulations as they hold and process employee data for payslips, and make sure any supplier providing payroll services maintain GDPR compliance as well. Payslips present a potential risk to GDPR compliance since they contain personal and identifiable information, so this is one area we will need to watch after the GDPR changes.

Do I need employee consent before sending a payslip?

Since companies are **legally obligated** to provide employees with payslips, you do not need employee consent to send a payslip. You must demonstrate that the way you process and protect the employee data is GDPR compliant.

Will I be fined for a payslip breach?

In most cases, the largest fines for non-compliance will be for negligence in several areas of data privacy and protection. Payslips are just one part of GDPR compliance, so if your company had several breaches in addition to a payslip breach you would be more likely to get a fine than if you just had a payslip breach that was contained. In most instances, a company that is not following proper protocols will receive penalties, and if you are demonstrating the “**appropriate technical and organisational measures**” to ensure security, you will most likely not be fined.

The best way to manage GDPR compliance

- ✓ Start early
- ✓ Limit your potential liabilities
- ✓ Be prepared for an audit by the ICO

If you have proper measures in place to avoid a breach, you can demonstrate to the ICO that you are compliant with GDPR regulations and avoid penalties.

