Payroll Data & GDPR:

What you need to know about consent, emailing payslips, and your legal obligation

In this guide, we will specifically look at the impact of GDPR on your payroll processing and highlight the biggest areas of concern.

We will walk through some important steps to achieve GDPR compliance.

An Introduction

The General Data Protection Regulation (GDPR) was introduced in May 2018 with the aim of protecting individual's data in an increasingly data driven world. It requires businesses to protect the personal data and privacy of EU citizens for transactions that occur within the EU.

The GDPR involved an update to the Data Protection Act 1998 and applies to every company, including sole traders who process the personal data of individuals operating in the EU. Whilst the UK is set to leave the EU, it has been confirmed that post Brexit, GDPR and data protection rules will be incorporated into UK law.

Getting compliance right is a cause of concern for payroll bureaus who manage and process their client's payroll data. The GDPR makes every business (payroll client) responsible for any third parties (payroll bureaus) who process personal data on their behalf. Under the terms of the GDPR, bureaus now need to manage and store their client's information in a more secure environment. It is also important to keep a record of how you are storing this information and for what purpose should you ever be audited or reported.

In this guide, we will specifically look at the impact of GDPR on your payroll processing and highlight the biggest areas of concern.

We will walk you through some important steps to achieve GDPR compliance by examining the following topics:

What does GDPR mean for your payroll bureau service?

- Understanding GDPR
- The contract between payroll bureaus & clients
- Proof of compliance
- Securely storing employee data

Payslips & GDPR Compliance

- Employee consent
- Emailing payslips
- Recommended self-service access

Breaching GDPR

- Data breach plan of action
- Non-compliance and penalties

Online Self-Service Portals

- How BrightPay Connect can help

1 What does GDPR mean for your payroll bureau service?

Payroll bureaus process large amounts of personal data, not least in relation to their customers, their customers' employees and their own employees. Consequently, the GDPR affects most, if not all, areas of the business and the impact cannot be overstated. Bureaus must provide certain guarantees to clients that their data is being processed securely and responsibly under the GDPR.

Given technological advancements and recent cyber-attacks, an updated security process is definitely required by payroll bureaus to protect the personal data that they manage. The GDPR is not a new concept, it is simply a data protection process that has been upgraded to protect all individuals. The introduction of the GDPR involved an overhaul of the Data Protection Act, to change how we process, manage and store individual data.

Payroll bureaus are legally obliged to protect payroll information on behalf of their clients where you must:

- **Only collect information you need for the specific purpose of completing the payroll on behalf of your clients.**
- **Keep client and employee payroll information safe and secure.**
- **Ensure client's data is relevant and up-to-date for the purpose of processing the payroll.**
- **Only hold information you need and for as long as you need it to manage the payroll.**
- **Allow clients or their employees to view their personal information that is kept upon request.**

Understanding GDPR

Employers must provide employees and any job applicants with a privacy notice setting out certain details about how their information is managed. Employees now have greater rights to be informed about how long their information will be stored and how it is used.

Employees can request access to the personal information that is held on them where they can request to have it rectified, and in some cases where there are no compelling reasons to retain the data, they can request for it to be deleted. Employees now have the right to increased transparency to ensure their data is being managed correctly under the GDPR legislation.

There is a lot of information to digest and understand around the topic of the GDPR. Payroll bureaus should fully understand the concept of the GDPR and the impact it has on both their business and their clients.

There are three basic sets of rules relating to individual's payroll and personal data, as outlined on the following page.

Understanding GDPR

Data Management

Payroll and personal data must be processed lawfully, fairly and in a transparent manner. For payroll bureaus, client data must be collected for the legitimate purpose of completing the payroll on behalf of their clients. All of your client's payroll data must be kept up-to-date and accurate and only be used for processing the payroll. Bureaus must ensure that the client and employee payroll data is protected and adequately secured against loss, damage, unlawful access and cyber-attacks.

Transferring Data Internationally

Under the GDPR, it is prohibited to send your client's data outside the European Economic Area unless that country provides an adequate level of protection for the rights of individual's personal data. Transferring your client's data outside of the EU requires extra caution and must meet the specific criteria as set out in the GDPR regulations.

Data Processing

Processing data on behalf of your payroll clients is lawful as long as there is a written contract between you and your client. This contract represents a legal obligation for you, the bureau, to process data in order to complete your client's payroll and provide payslips as agreed each pay period. Payroll bureaus must only process data as per the written instruction of their client, hence it is of the utmost importance that a comprehensive contract is in place.

Additionally, the GDPR legislation sets out further requirements regarding what must be included in the contract between a payroll bureau and their client. These include, but are not limited to, confirmation of security, confidentiality and details of any sub-processor used.

The contract between payroll bureaus & clients

If a bureau is audited, they may need to provide certain information to prove their GDPR compliance such as:

Agreed Contract

There needs to be a written contract or letter of engagement in place between payroll bureaus and the client that covers GDPR. This contract would outline that employee's personal data is being provided to the bureau to process the payroll for the business. This does not mean a payroll client can simply hand over their employee's personal data to a bureau and then cast a blind eye. The payroll client must ensure that the bureau is also compliant with the GDPR.

Fulfilling the Contract

To fulfil the contract, payroll bureaus are required to hold certain business information, such as their employer PAYE reference number and their bank account details, which is all legitimately viable under the GDPR. Payroll bureaus need to hold this personal information in order to fulfil the agreed contract of processing the client's payroll.

Legitimate Reason

Every business needs to provide a legitimate reason as to why they hold an individual's personal details. Payroll bureaus are deemed as processors as they process client's and their employee's personal data. Payroll bureaus hold client and employee payroll information to complete the payroll, such as employee National Insurance numbers, tax codes, dates of birth, employee salaries and employer national insurance details. Under the GDPR legislation, this is classified as a valid and legitimate reason to hold this kind of personal payroll information.

Proof of Compliance

Payroll bureaus cannot just tell their clients that they are compliant with the GDPR legislation. They need to prove that they are securely protecting any data that they process and manage. Client's payroll records should be securely maintained where the information is adequately protected under the rules of GDPR. Should your bureau be subject to an audit or a GDPR breach, you will need to show evidence that demonstrates you have taken the appropriate actions to protect your organisation and your client's payroll information.

Securely Storing Employee Data

It is advisable to password protect any of your client's payroll reports and payslips that you may email out each pay period. Your payroll software supplier should provide a password protection feature for any client reports or employee payslips that are stored and exported from the payroll software.

Bureaus will need to provide detailed information on how long the personal data will be stored for. According to HMRC guidelines, you should keep payroll records for 3 years from the end of the tax year they relate to.

2 Payslips and GDPR Compliance

Businesses must provide their employees with information on what happens to their data, for example sharing employee's personal data with a third party (payroll bureau) who processes the payroll. Employee personal data can be stored and managed by a payroll bureau, bookkeeper or accountant for the sole benefit of correctly paying their wages, paying the correct tax and providing a payslip. All of this legitimately falls under the remit of the GDPR legislation.

By law, you must provide employees with payslips which include personal data such as proof of earnings, tax paid and any pension contributions. It is advisable that bureaus take steps to protect and securely send this payslip information.

Employee Consent

Many bureaus have expressed concern and confusion in relation to getting consent from client's employees and securely distributing payslips. Payroll bureaus do not need to seek consent from individual employees that the payroll is processed for. However, the employer needs to inform their employees that they are sharing their personal information with a third party. It is also an employer's responsibility to ensure that their payroll bureau or accountant is taking action to protect their employees' payroll information under GDPR.

An employee cannot withdraw their consent for their personal data to be used as part of the payroll processing. It should be noted that bureaus should keep only the personal data that is strictly required for the purpose of the payroll. This is referred to as data minimisation or privacy by default.

Posting Payslips

There is nothing in the GDPR legislation that states it is no longer permissible to post payslips. Payroll bureaus who post payslips will need to ensure that all appropriate security measures are in place to protect the payslip. This may include using security payslip envelopes, marking the envelope as 'Private and Confidential' and ensuring that it is addressed to a specific person. In some cases, you may decide to use registered post.

Emailing Payslips

There is nothing in the GDPR legislation that states it is no longer permissible to email payslips. However, payroll bureaus should take steps to securely protect each employee's payslip. When emailing payslips, bureaus should ensure that all payslips are password protected with a password that is uniquely chosen by the employee. The payslip should be sent directly to the employee's chosen email address.

Where a generic and identical password is used for all employees, this could be considered a breach of GDPR. In this scenario, the bureau could be seen as not taking sufficient steps to offer the most secure environment to protect employee's personal pay information.

Furthermore, your payroll provider should provide secure encryption on all payslips and automatically delete payslips that are being sent from their server. Check with your provider to be certain that they are offering this level of protection. If not, you should look for another payroll provider who does. For maximum security, it is recommended (but not mandatory) to offer a secure self-service portal to securely send and store payslips and other sensitive payroll documents.

Recommended Self-Service Access

The GDPR legislation includes a best practice recommendation for businesses to provide individuals with a secure self-service platform offering remote access to information held. On a self-service system, employees would be able to remotely access payroll information including payslips, contact details, and employee documents such as employee contracts and handbooks. Employees may also be able to request leave and view their annual leave entitlements including leave taken and leave remaining, which are also considered personal data.

According to the Information Commissioner's Office (ICO):

"The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information."

(Recital 63)

Recommended Self-Service Access

The employee self-service portal should be password protected for every employee. Again, identical or a generic password must not be used for all employees. Each employee's password should be unique, chosen by the employee and confidential, offering maximum protection. Accessing payslips and personal contact details through a remote access secure system will provide flexibility and full transparency for employees to retrieve their information at any time.

A self-service portal offers significant benefits for payroll bureaus to comply with the GDPR legislation. Remote access will provide clients and their employees with direct access to their payroll information anywhere, anytime. Clients can login 24/7 to view their employees' payslips, HR documents, amounts due to HMRC and other payroll reports.

Payroll bureaus also benefit as they can now automate the distribution of payslips and payroll reports. With some systems, payslips and payroll reports will be automatically available on the self-service portal as soon as the payroll has been finalised. This offers additional security against cyber-attacks and eliminates email hacks that could occur when sending payslips or payroll reports by email. Additionally, a self-service option allows payroll bureaus to keep their data updated and accurate as employees can edit their contact information.

3 Breaching GDPR

Businesses must issue notifications of valid data breaches to the local supervisory authority within 72 hours of becoming aware of them. Failing to report a breach can result in an investigation and/or penalties. Individuals also have the option to file a class action lawsuit if a business does not comply with the GDPR. The legislation applies to every business large and small in the UK - there will be no exceptions for small businesses.

Data Breach Plan of Action

There is a mandatory breach reporting requirement, where employers must report certain types of breaches to the data protection authority. A personal breach occurs where a business's security systems have been compromised leading to the '**accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data'**.

A business must determine the level of the breach's severity and the risk it could present to an individual's rights and freedoms. If it is considered a risk then you must notify the Information Commissioner's Office (ICO). If there is no risk then you do not have to report it. However, businesses who do not report a breach should keep a record and be able to justify their reasoning behind their decision not to report it and document those reasons.

Data Breach Plan of Action

Make sure you have suitable procedures in place to notify the regulator where breaches have been reported and identified. Inform all staff of the correct procedure to follow should a breach occur. Check with your IT team or staff to ensure your computer systems allow for your employees to securely delete and manage personal data in line with the GDPR legislation.

Non-Compliance & Penalties

The ICO is taking non-compliance very seriously with significant fines and penalties in place for businesses who breach the GDPR legislation. Fines will be incurred of €20 million or 4% of a business's turnover, whichever is the greater amount. The level of fine being imposed will depend on the type of breach that a business has committed. The fines are designed to punish any business that wilfully ignores their GDPR obligations. However, fines can be mitigated against if there is evidence that shows that a business has prepared and worked towards GDPR compliance.

4 How BrightPay Connect can help

As mentioned above, under the GDPR legislation, where possible the controller should be able to provide self-service remote access to a secure system which would allow the data subject with direct access to his or her personal data. BrightPay Connect is a self-service option which will give your payroll clients and their employees online remote access to view and manage their payroll data 24/7.

BrightPay Connect is tailored to help you and your clients overcome the challenge that GDPR presents. Furthermore, the cloud functionality will improve client collaboration with simple email distribution, safe document upload, easy leave management and improved communication with your clients.

As the pace of bureau/client interaction increases, the margin for error increases which could lead to a GDPR breach if your data is not up-to-date or accurate. Online synchronisation and automated backup of payroll data will maintain accuracy and improve efficiency of your client's data. By introducing payroll clients to a new way of remotely accessing information you will be taking steps to be GDPR ready and benefit from enhanced efficiencies through an integrated payroll system. Additionally, a self-service facility will remove the need to email payroll reports each pay period, automate payslip distribution, simplify and integrate leave requests and keep a secure backup of your payroll records.

Simplify your GDPR compliance with BrightPay Connect

Small and medium size businesses tend to look to their accountant or bureau for guidance when it comes to keeping their employee payroll data secure. The option of BrightPay Connect offers your clients added reassurance that you are taking action to be GDPR compliant.

The advantages of a cloud backup and self-service software are numerous, but mainly it significantly increases the efficiency and effectiveness of payroll work. Workflow is increased since payroll bureaus are no longer wasting time on manual data processing and therefore are working quicker, efficiently and more profitability within the remit of the GDPR guidelines.

BrightPay Connect is an online payroll and HR software solution that has been developed to help our customers with GDPR compliance. It removes the manual data entry requirement for annual leave management, entering employees' hours and payments, updating employees' details, re-sending payslips, backing up your data and HR processing.

Here are the Biggest GDPR Advantages of BrightPay Connect:

Bureau / Client Dashboard

Provide clients with online self-service access to payroll information. Clients will have remote and secure access to payslips, payroll reports, amounts due to HMRC, annual leave requests and employee contact details.

Employee Self-Service Portal

Invite employees to their own self-service online portal. This secure system would provide employees with direct access to his or her personal data. Employees can securely view and download payslips, P60s and P45s and easily submit holiday requests, view leave taken and leave remaining.

Integration with Payroll

BrightPay Connect is fully integrated with BrightPay's payroll software ensuring the payroll data is correct at all time. Any annual leave or other leave, changes to employee contact details, employee hours and payments and payroll reports are automatically updated and synchronised with the payroll software and BrightPay Connect.

Cloud Backup

Under the GDPR, it is important to keep a copy of payroll files safe in case of fire, theft, damaged computers or cyber-attacks. BrightPay Connect is powered using the latest web technologies and hosted on Microsoft Azure for ultimate performance, reliability and scalability. BrightPay Connect maintains a chronological history of your backups which you can restore or download any time keeping your records protected.

GDPR Advantages of BrightPay Connect

24/7 Online Access

BrightPay Connect allows password protected mobile and online access to client's payroll data anytime and anywhere. This fulfils the recommendation to provide remote access to a secure system where clients and their employees would have direct access to their personal data.

HR & Annual Leave Management

Clients can view all upcoming leave in the BrightPay Connect company-wide calendar where they can easily authorise leave requests with changes automatically flowing back to the payroll. Clients can upload sensitive HR documents such as employee contracts keeping confidential information restricted to each individual employee.

Reduce HR Queries

BrightPay Connect makes it possible to drastically reduce the number of HR queries you deal with such as access to view personal data, payslip requests, annual leave requests, managing employee contact information and employee payroll records.

Client Payroll Entry & Approval

Bureaus can request clients to securely send their employee's hours, payments, additions and deductions through their online portal. This offers an additional layer of protection for your clients' payroll information. Once the payroll is finalised, the bureaus can also send a payroll summary report to their client through the secure portal, which can then be approved or amended by the client. The automated process will eliminate the email and document exchange between you and your client offering a more secure and accurate recording of the employees' payroll information.

Book a BrightPay Connect Demo

Cloud advancements enables an interactive collaborative experience for bureaus, clients and employees. BrightPay Connect speeds up and transforms the bureau client relationship from a document exchange or transactional relationship to an instant access one. Book a demo today to find out how BrightPay Connect can help your bureau with GDPR compliance.

BOOK A DEMO