Privacy Notice

Data Classification	Public Data
Author	Head of Regulatory Compliance
Approval	Legal Director
Last updated	May 2024

This privacy notice applies to how we hold, collect and process Personal Data in the context of an employment relationship with prospective, current and former employees of PayStream International Limited located in Republic of Ireland. It explains what information we collect, how we use it, who we share it with and how we protect it. It also details the rights available to individuals in relation to how we hold and use their personal data, how to exercise those rights, and what to do if more information is required or a complaint is to be made.

Who are we?

The company named on your employment contract is PayStream International Limited ("PayStream International"). PayStream International employs individuals to provide services to third party clients during assignments and, through its internal business functions, processes information about employees in order to effectively manage and perform its obligations to them.

PayStream International is part of the PayStream group of companies, of Mansion House, Manchester Road, Altrincham, WA14 4RW, which we refer to as 'us' and 'we' in this Privacy Notice. Whilst the company named on your employment contract is the entity which employs you, PayStream Accounting Services Limited ("PAS") which is also part of the PayStream group, is the entity which employs internal staff to operate the running of the business and for making decisions as to the data we collect from employees and how such data is processed.

As such, PAS is a Data Controller as defined by Article 4(7) of the UK GDPR and on the instruction of PAS, we process data as outlined in the following privacy notice.

Privacy Introduction

PayStream International employs individuals who provide services to Clients during the period of an Assignment, and through our internal business functions we process information about our Employees in order to manage effectively our relationship with them. This is for the purpose of administration and management and also in compliance with applicable laws and regulations.

We are committed to safeguarding the privacy of the personal information that we gather concerning our prospective, current and former Employees for management, human resources, payroll and related purposes.

We will only process personal data in accordance with this Privacy Notice unless otherwise required by applicable law. We take steps to ensure that the personal data that we collect about you is adequate, relevant, not excessive, and processed for limited purposes. All data will be treated with the utmost confidentiality.

Why we collect your Personal Data

We collect your personal data so that we can manage our relationship with you, fulfil our contractual obligations to our customers and to otherwise improve and market our solutions. Activities that we require personal data for include:

- Management of our relationship with Employees as part of their employment contract
- Provision of employment related services to Employees, former Employees, and candidate-Employees
- Responding to employment related requests and providing employment related information

- A range of other employment related activities which we are obliged to undertake, or which we have gained your consent to perform
- Compliance with statutory obligations (e.g. Employment Law)
- Legal requirements relating to your right to work in Ireland

We ensure that the information we collect is appropriate to the purposes for which it is obtained. We are committed to safeguarding the privacy of the personal information that we gather concerning our prospective, current and former Employees.

What Personal Data we collect

The Company recognise the importance of Personal Data entrusted to us. We may collect and hold a range of information about you. Examples of the types of information we may hold include:

- Personal identification information such as your name, address, gender, date of birth, marital status, PPSN
- Other information which you have provided to allow us to identify and contact you
- Your contract of employment and any amendments to it
- Details that you have provided about your emergency contact(s), next of kin or other beneficiaries
- Employment identifiers such as staff number or business email address that you have provided, or have been assigned
- Information that you have provided about academic background or professional certifications
- Information you have provided in your Curriculum Vitae, or in an employment application, including details about your past employment history
- Information that you have consented to provide as part of our equal opportunities or diversity & inclusion programmes
- Photographic images used for security and identification information
- Timesheet and Assignment information
- All incoming and outgoing calls are recorded for training and monitoring purposes and may be used where necessary in dealing with queries, complaints and legal issues if they arise
- All incoming and outgoing emails that you send to us from a known email address are a recorded for quality and training purposes and may be used where necessary in dealing with queries, complaints and legal issues if they arise
- We have an internal IT system called "Tifo". This logs your journey with the Company, from when you join, your payments and end of employment. Internal notes may be made on this system, if for example you call up with a pay query, we will record this activity on the system for quality and audit purposes
- Banking details that you have provided to facilitate electronic payments
- Financial data in relation to payroll, benefits and expenses
- Medical data that is relevant to the performance of your duties or to your entitlements
- Other medical data that you choose to share with us
- Career history and performance data that is collected as part of our performance management activities including, where appropriate, disciplinary and grievance records
- Correspondence with or about you, for example a letter to your mortgage Company
- Personal email addresses for use in specific situations
- Criminal records data may be processed as part of onboarding processes and/or, where necessary, in the course of employment to verify that candidates are suitable for employment or continued employment and to comply with legal and regulatory obligations to which the Company is subject
- User Feedback: while using our services, occasionally you may be asked to provide optional feedback.

When you visit our website, we may collect technical data such as:

- Usage data: (if permitted) we may collect certain information related to your device, such as your device's IP address, what pages your device visited, and the time that your device visited our website
- Cookies: (if permitted) your IP Address and other information provided to us by cookies

Much of the information we hold will have been provided directly by you, but it may also come from other external sources, such as the Client, referees, employment recruitment agencies or a family member. Prior to your employment, in some cases, your recruitment consultant may have passed on your name and contact details so that we can contact you in respect of our employment offer. Alternatively, you may have contacted us directly, either via our website or otherwise. In order that we can get you set up quickly, we will call, text and email you reminders to join us and/or otherwise, to encourage you to accept our employment offer.

How we use your Personal Data

We will only collect and process your personal data where we have a legal basis to do so We will mainly use personal data for the management and performance of your contract of employment, though the legal basis for our collection and use of your personal data may vary depending on the manner and purpose for which we collected it. We will only collect personal data from you when:

- We have your consent to do so, or
- We need your personal data to perform a contract with you, or

  We are pursuing our legitimate interests in a way that you might reasonably expect to be a part of running our business and that does not significantly impact your interests, rights, and freedoms. For example, communicating with you if we have a sufficient legal ground based on the e-marketing laws in your country
- We have a legal obligation to collect or disclose personal data from you (for example, in suspected instances of fraud we may need to give personal data to relevant government bodies).

The following are the main ways that personal data may be used:

- Processing in relation to salary, benefits, expenses and allowances
- We will check on your identity and right to work and use external databases to do this
- For the performance of a contract: we need to fulfil our contractual obligations, such as to pay you and in order to do so we may need to share your information with the recruitment business (or client where there is no recruitment business in the contractual chain); this may include exchanging information on hours worked, payments and tax deductions if it is necessary to fulfil our contract. We may also notify you from time to time of any contractual matters pursuant to your employment with us
- To manage Employee Relations (e.g. grievance processes)
- Responding to queries and due diligence requests from recruitment businesses, end clients and/or third parties (who may for example, be carrying out audits, due diligence, debt-collection or legal/tax investigations). This may include providing employment reference and/or exchanging information on hours worked, payments and tax deductions, as well as evidence of right to work and identity checks
- For Performance and Development activities such as goals setting, development plans, training
- For administering pensions processes such as pension contributions, pension adjustment orders or pension retirement savings accounts
- To comply with legal or regulatory requirements
- In the development, monitoring and enforcement of the Company's policies and guidance
- We may need to share information on your hours worked, payments and tax deductions with the recruitment business to demonstrate our compliance and/or in order to fulfil our contractual commitments with the recruitment business. In order to do this, we may be required to send a copy of your payslip to the recruitment business. We will do this securely so as to reduce the likelihood of any data breach
- We will keep you informed of any news which may affect your employment with us or that, in our opinion, will improve our relationship. This may include, but not be limited to, enhancements to our TIFO portal or other IT capabilities

- To comply with legal obligations or valid legal processes such as search warrants, subpoenas, or court orders. When we disclose your personal data to comply with a legal obligation or legal process, we will take reasonable steps to ensure that we only disclose the minimum personal data necessary for the specific purpose and circumstances
- To protect the rights and property of us, our employees, customer and/or others
- During emergency situations or where necessary to protect the safety of persons
- If a business transfer or change in ownership occurs and the disclosure is necessary to complete the transaction. In these circumstances, we will limit data sharing to what is absolutely necessary, and we will anonymise the data where possible
- Where we need to fulfil our contractual obligations and/or to demonstrate our compliance. This may include exchanging information on your identity, right to work, hours worked, payments and tax deductions
- For marketing and completion of voluntary surveys and rewards schemes. We use surveys, reviews and marketing tools to get feedback and make continuous improvements and in doing so may share and/or collect information such as your name, email address, reference number and IP address. We use a third-party email and marketing automation provider and may choose to use Marketing Analytics Software via the use of a tracking cookie on our website
- To sanitise, secure and archive all inbound, internal and outbound emails. All emails undergo various best practices checks / processes and the content is scanned for malicious content / markers. We also use external document destruction services to ensure that client, employee and confidential business information is kept secure at all times
- To store externally certain types of documents (such as expense receipts, timesheet attachments, invoices/Credit notes & payslips)
- To communicate with you via text message

We may also process your personal data for our own legitimate interests, including for the following purposes:

- To prevent fraud
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution
- To support internal administration with our affiliated entities
- To conduct data analytics analyses to review and better understand employee retention and attrition rates

Activities that require your consent

In order for us to carry out certain activities using your personal data, we may need to ask for your consent. When consent is being requested, we will provide you with relevant options, such as the choice of whether we may contact you by phone, post, email, text or through other digital media. Where we require consent, we will explain why and provide sufficient information to allow you to make an informed decision. When we have been provided with consent to perform such activities, that consent may be withdrawn at any time by contacting us requesting its removal.

Should there be any reason for us to collect sensitive personal information (e.g., medical data or trade union membership) other than as outlined in your contract of employment, we ask for consent to collect it. Before consent is given, we explain what information will be collected and what we will use it for. Again, this consent can be withdrawn by contacting us.

Collection and Use of Special Categories of Personal Data

The following special categories of personal data are considered sensitive under the laws of your jurisdiction and may receive special protection:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs

- Trade union membership
- Genetic data
- Biometric data
- Data concerning health
- Data concerning sex life or sexual orientation
- Data relating to criminal convictions and offences may also receive special protection under the laws of your jurisdiction

We may collect and process the following special categories of personal data when you voluntarily provide them for the following legitimate business purposes, to carry out our obligations under employment law, for the performance of the employment contract, or as applicable law otherwise permits:

- Biometric data for the purposes of checking eligibility to work and identity;
- Physical or mental health information or disability status to comply with health and safety obligations in the workplace, to make appropriate workplace accommodations, as part of sickness absence monitoring, and to administer benefits
- Race or ethnic origin, religious affiliation, health information and sexual orientation to ensure meaningful equal opportunity monitoring and reporting
- Criminal records data to verify that candidates are suitable for employment or continued employment and to comply with legal and regulatory obligations to which we are subject

Where we have a legitimate need to process special categories of personal data for purposes not identified above, we will only do so only after providing you with notice and, if required by law, obtaining your prior, express consent.

We will only retain special categories of personal data for as long as necessary to fulfil the purposes we collected it for, as required to satisfy any legal, accounting, or reporting obligations, or as necessary to resolve disputes.

We will always treat special categories of personal data as confidential and we will only share such data internally where there is a specific and legitimate purpose for sharing the data.

We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure.

Parties with whom we share information

We will only disclose your personal data to third parties where required by law, or, to our employees, contractors, designated agents, or third-party service providers who require such information to assist us with administering the employment relationship with you, including third-party service providers who provide services to us or on our behalf. This includes exchanging information with other companies and organisations for the purposes of the detection and prevention of crime (including financial crime and fraud) and credit risk reduction.

Third-party service providers may include, but are not limited to, recruitment agencies, payroll processors and software providers, benefits administration providers, data storage or hosting providers, as well as our insurance broker, insurance underwriters and lawyers. In the unlikely event that you owe us money, we will also take steps to recover our funds which may involve sending your information to an external debt collection agency and/or tracing service.

If, as part of our legal obligations as your employer, we are required to investigate any reasonable adjustments which may be necessary for you whilst under our employment, then we may need to share personal information (including personal information in respect of any relevant medical conditions). For instance, if we need to carry out a desk assessment and/or an occupational health assessment for you then we will use an external body specialised in this area in order to do so. If any reasonable adjustments agreed require the purchase of any software, equipment or other similar services then again, personal information may need to be shared with third party vendors in order to facilitate this.

Third-party service providers used by us may be located outside of your home jurisdiction. We require our third-party service providers to implement appropriate security measures to protect your personal data consistent with data security obligations applicable to us as your employer. We only permit them to process your personal data for specified purposes in accordance with our instructions.

We may share your personal data with, or disclose your personal data to, the following categories of third party:

1. Your approved 3rd parties: where you have notified us that you wish us to provide information or payments to 3rd parties such as lending institutions or life assurance organisations, we will share the required information in accordance with your instructions
2. Agents or suppliers: these are persons or companies we have contracts with to provide products or services that we use in conducting our business, including managing our relationship with our Employees. In some cases, they may be outside of the EEA. We will only share or disclose to these parties the information that they need in order to provide the products or services, and will require those parties to ensure that the information is always adequately protected
3. Professional and other advisers: we may share or disclose personal data to professional advisers we may engage for any reasonable purpose in connection with our business, including assistance in protecting our rights
4. Other external bodies: in certain circumstances, we may be required by law to disclose personal data to external bodies, such as local authorities, government departments, Central Bank of Ireland, Regulatory Authorities or An Garda Síochána. In these cases, we will only disclose the minimum amount of information required to satisfy our legal obligation. However, once the information is disclosed, we will not be able to control how it is used by those bodies
5. Members of our group of companies (including outside of your home jurisdiction) for the purposes set out in this Privacy Notice and as necessary to perform our employment contract with you

How we protect it – Security of your Personal Data

We keep our computer systems, files and buildings secure by following legal requirements and international security guidance. We make sure that our staff, and anyone with access to personal data that we are responsible for, is trained on how to protect personal data. We ensure that our processes clearly identify the requirements for managing personal data and that they are up to date. We regularly audit our systems and processes to ensure that we remain compliant with our policies and legal obligations.

How long we keep data

Information collected by us will be held for as long as it is required to fulfil the purpose it was collected and to protect our business and our rights. We are required to keep certain types of information for a specific period of time in order to comply with legal requirements. The length of time we keep any part of your personal information will depend on the type of information and the purpose for which it was obtained.

Where you do not join PayStream International Limited's employment, we will hold your personal information, for the purposes of our legitimate interests for 12 months from the point we first attempt to contact you. We may contact you periodically within this period to re-offer our employment.

Where you do join PayStream International's employment, we will hold your personal information for the purposes outlined below for 7 years from the date of termination of your employment unless we hold record of accidents or dangerous occurrences or EU funding contracts, in which case your personal information will be held for 10 years, or, if we have record of any parental leave, force majeure leave, paternity leave or carers leave then your personal information will be held for 12 years. In all cases, bank details will be deleted after 12 months from the date of termination of your employment.

Under some circumstances we may anonymise your personal data so that it can no longer be associated with you. We reserve the right to use such anonymous and de-identified data for any legitimate business purpose without further notice to you or your consent.

How we address your rights

Although the Company needs to capture, store and process your personal information in order to carry out a range of services, you have a range of rights available to you to give you confidence that your information is appropriately managed.

The rights that you have available to you include:

Gaining access to and copies of your personal data: you are entitled to receive, on request and free of charge, a copy of all your personal data that we hold. There are some limitations to this right. For example, if the data also relates to another person and we do not have that person's consent, or if the data is subject to legal privilege. Where there is data that we cannot disclose, we will explain this to you.

Ensuring that your data is accurate: our aim is to ensure that the data we hold about you is correct and up to date. From time to time we may contact you to verify the information that we hold. You may also contact us to correct any errors that you notice or update the portal where your details are held.

Granting or Removing consent: where we require your consent for any processing, for example, to provide you with direct marketing communications, we will clearly explain what the consent is for, and any consequences of giving or refusing consent, and will provide that consent can only be given by way of a positive action by you. We will also ensure that you are able to withdraw any such consent at any time.

Restricting processing of your data: you have the right to request us to restrict the processing of your personal data in certain circumstances, for example, if there is a dispute over our rights to carry out specific processing activities, or where you do not want us to delete data. We will respond promptly to your request and will provide an explanation if we cannot fully comply.

Deletion of your data: in certain circumstances, you may have the right to have some or all of your personal data deleted from our records. This is sometimes referred to as the "right to be forgotten". This may occur if, for example, we retain data which is no longer required by us, or if you withdraw a consent. If you continue to have a relationship with us, we must retain the data we need to manage this relationship. We will respond promptly to your request, and provide reasons if we object to the deletion of any of your personal data.

Moving your data: where it is possible for us to provide it, you have the right to receive a digital copy of the personal data that you have provided to us.

International Transfers of Data

In certain circumstances, we may transfer your personal information internationally, including outside of the European Economic Area (EEA). Should we do this, we ensure that all transfers are made in accordance with data protection law and that your data it will be given an equivalent level of protection that it has when it is being managed in Ireland.

How to contact us

In relation to Personal Data Individuals have the right to be informed, the right of Access, the right to rectification, the right of erasure, the right to restrict processing, the right to Data Port, the right to withdraw consent and rights in relation to automated decision making and profiling. Our collection and use of your data are overseen by our Privacy Team. If you wish to contact our Privacy Team, you can email PrivacyTeam@paystream.co.uk or via post at Privacy Team, PayStream, Mansion House, Manchester Road, Altrincham, WA14 4RW, UK.

How to make a complaint

If for any reason you have a complaint about our use of your personal information, or you are unhappy in any way with the information we provide to you, you may contact us directly so that we can address your complaint. You can contact us by email PrivacyTeam@paystream.co.uk or via post at Privacy Team, PayStream, Mansion House, Manchester Road, Altrincham, WA14 4RW, UK. You may also contact the Data Protection Commission in Ireland about such matters on 1890 252 231, by email at info@dataprotection.ie or by postal mail at Data Protection Commission, Canal House, Station Road, Port Arlington R32 AP23, Co. Laois.

Changes to our privacy notice

We will occasionally update this privacy notice. Any changes will be emailed out, prior to implementing the changes, and, where appropriate, notify you using any of the contact details we hold for you for this purpose. We encourage you to periodically review this notice to be informed of how we use your information.