

Privacy Notice

Last updated: September 2023

It is important that you read and retain this Privacy Notice, together with any other notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using that information and your rights.

Privacy Introduction

PayStream International LLC 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 LLC is a "data controller" and is responsible for deciding how it holds and uses personal information about you.

This Privacy Notice describes how PayStream International LLC and its subsidiaries, affiliates, sister companies and related entities (collectively, "PayStream International," "we," or "us") hold, collect and process Personal Data in accordance with data protection laws. It explains why we collect Personal Data, what data 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 in the recruitment process, during and after their employment; how to exercise those rights and what to do if more information is required or a complaint is made.

Any reference to "Personal Data" in this Privacy Notice shall mean any information relating to a living individual, from which that living individual can be identified directly or indirectly (in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person). We do not consider anonymous data, or data where the identity of the individual has been irretrievably removed, Personal Data.

PayStream International recognises the importance of Personal Data entrusted to us. We are committed to safeguarding the privacy and security of the information that we gather concerning our prospective, current and former employees for management, human resources, payroll and related purposes. All data will be treated with the utmost confidentiality and we take steps to ensure that all Personal Data we collect about you is adequate, relevant, not excessive, and processed for limited purposes. Whilst we may not seek explicit consent from you for processing your data, we will only process Personal Data in accordance with this Privacy Notice unless otherwise required by applicable law.

Data Protection Laws

This Privacy Notice applies to all Personal Data we hold in the context of an employment relationship with prospective, current and former employees located in the USA. This is for the purpose of administration and management and also in compliance with data protection laws and regulations.

PayStream International complies with data protection laws globally by ensuring the minimum standard we apply is that found within the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), which enhances privacy rights for individuals and provides a strict framework within which commercial organisations can legally operate.

Whilst the GDPR protects the Personal Data of European citizens and residents, to satisfy global data protection laws, the GDPR obligations are applied to PayStream International's global operations. Under GDPR, a data controller is required to notify you of the information contained in this Privacy Notice.

Why we collect your Personal Data

We collect your Personal Data so that we can manage our relationship with you, perform the employment offer, fulfil our contractual obligations to our customers and to otherwise improve and market our solutions.

During the course of your employment with PayStream International your Personal Data may be used for commercial, legal or performance reasons.

Examples of activities that we require Personal Data for include:

- Management of our relationship with employees as part of their employment offer.
- Provision of employment related services to employees, former employees and prospective 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 and legal requirements relating to your i-9 check, for example).
- Attendance tracking including holiday leave, sickness absence or other out of office absences such as home working and external office visits. Data generated in this manner is used for legal purposes associated with your absences or may be used towards an evaluation of your overall performance.
- Training and Competency records may be kept to maintain skills and competency levels associated with your role, and where pertinent, to record activity relating to legal compliance associated with business conduct.
- Health information and incidents which are recorded and reported in line with local laws and PayStream International's commitment to your safety and wellbeing during employment.
- System notes containing a record of discussions and/or agreements between you and PayStream International will be retained centrally on our global database.
- Communications, including those regarding the following:
 - Financial transactions; such as payroll and pension.
 - The employment offer.
 - Marketing emails, where you've consented for us to send them to you.
 - Other support and services we can offer you where we have a legitimate interest to inform you.
 - Commercial and legal communications associated with the business relationship such as contractual requirements, legal aspects arising from the services provided to you and as confirmation of assignment start and end periods.

What Personal Data we collect

We may collect and hold a range of information about you and will collect additional personal information in the course of job-related activities throughout the period of you working for us. The type and volume of data we hold is dependent on the services and relationship you have with us. Much of the information we hold will have been provided directly by you, but it may also come from other external sources, such as an end client, referees, employment recruitment agencies, colleague 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. So 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.

We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies.

Examples of the types of information we may collect and hold include:

- Personal identification information such as your name, address, gender, date of birth, marital status, Social Security Number ("SSN").
- Other information (such as telephone numbers and email addresses) which you have provided to allow us to identify and contact you.
- Your employment offer 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.
- Employment records (including job titles, work history, working hours, holidays, training records and professional memberships).
- Information you have provided in your Curriculum Vitae, or in an employment application, including details about your past employment history as well as references and other information included in a cover letter or as part of the application process.
- Timesheet and assignment information.
- Annual leave, pension and benefits information.
- All incoming and outgoing calls which 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 which are recorded for quality and training purposes and may be used where necessary when dealing with queries, complaints and legal issues if they arise.
- Internal notes which we log on our internal IT system called "Tifo". Tifo is used to log your journey with us, from when you join, your payments and end of employment. If, for example, you call up with a pay query, we will record this activity on the Tifo system for quality and audit purposes.
- Banking details that you have provided to facilitate electronic payments.
- Financial data in relation to payroll, salary, benefits and expenses, including tax status information.
- Right to work and identity information and documents (such as passport or driving licence).
- Career history (including start data, date of continuous employment, leaving date and reason for leaving) 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.
- User Feedback (while using our services, occasionally you may be asked to provide optional feedback).
- Technical data, which may collect when you visit our website, 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.
 - Please see our Cookie Policy on our website for further information regarding cookies.
- Transactional data relating to financial activities such as payments, deductions or benefits, and reporting linked to payments to ensure financial legal obligations are achieved.
- Location of employment or workplace and travel arrangements and profiles linked to your business travel preferences.

Collection and Use of Special Categories of Personal Data

The following special categories of Personal Data are considered sensitive 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

We may collect and process the following special categories of Personal Data for these legitimate business purposes: to carry out our legal obligations under employment law, for the performance of the employment offer, or as applicable law otherwise permits (for example, with your explicit written consent; where it is needed in the public interest, such as for equal opportunities monitoring; or, where it is necessary to protect you or another person from harm). Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public:

- **Biometric data and photographic images** either a physical or digital format as submitted by you or taken during a social or business environment used for security and identification information for instance, and for the purposes of checking eligibility to work and identity.
- **Medical data** that is relevant to the performance of your duties or to your entitlements and any other medical data that you choose to share with us. This includes details of absences (other than holidays) as well as 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 information that you have consented to provide as part of our equal opportunities or diversity and inclusion.
- **Criminal records data**, although we do not envisage that we will hold information about criminal convictions in most cases. We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so (this is usually where processing is necessary to carry out our obligations and provided, we do so in line with this Privacy Notice). Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us to verify that you are suitable for employment or continued employment, and/or to comply with legal and regulatory obligations to which PayStream International is subject.

Where we have a legitimate need to process any special categories of Personal Data for purposes not identified above, we will only do so only after providing you with privacy information 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 where there is a specific and legitimate purpose for sharing the data.

How we use your Personal Data

We will only collect and process your Personal Data where we have a legal basis to do so. 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, however most commonly, we will collect Personal Data from you when we: need your Personal Data to perform a contract with you; 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 freedom (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); or, we have your consent.

The following are the main ways that Personal Data may be used:

- To fulfil our contractual obligations with you, for example:
 - To notify you from time to time of any contractual matters pursuant to your employment offer with us.
 - For performance and development activities such as goals setting, development plans, training.
 - For administering 401(k) processes such as contributions or adjustment orders.
 - For processing in relation to salary, benefits, expenses and allowances.
 - For performance of an offer letter.
 - To manage employee relations.
 - To store externally certain types of documents (such as expense receipts, timesheet attachments, invoices/Credit notes and payslips. This may also be a legal requirement.
- To comply with legal or regulatory requirements, for example:
 - Completing an i-9 check, right to work, and/or identity checks (we may use external databases to do this) 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 prevent fraud and/or to demonstrate our compliance. This may include for example, sharing information in response to requests from recruitment businesses, end clients and/or other third parties who may, for example, be carrying out audits, due diligence, debt-collection or legal/tax investigations.

- This may include providing employment references and/or exchanging information on hours worked, payments and tax deductions, as well as evidence of right to work and identity checks.
- For the development, monitoring and enforcement of our policies and guidance.
 - To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
 - To protect the rights and property of PayStream International, our employees, customer and/or others.
 - During emergency situations or where necessary to protect the safety of persons.
 - 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.
- For our own legitimate interests, including for the following purposes:
 - To 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.
 - 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.
 - To conduct data analytics analyses to review and better understand employee retention and attrition rates.
 - For marketing and completion of voluntary surveys and rewards schemes. We use surveys, reviews and marketing tools to get feedback and make continuous improvements to PayStream International. 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.
 - We have your consent
 - In order for us to carry out certain activities using your Personal Data, we may need to ask for your consent. We do not need your consent if we use your Personal Data (including special categories of your personal information) in accordance with our Privacy Notice to carry out our legal obligations or exercise specific rights in the field of employment law or where the purpose of the processing is to protect you or another person from harm or to protect your well-being and if we reasonably believe that you need care and support, are at risk of harm and are unable to protect yourself.
 - In limited circumstances however, we may approach you for your written consent to allow us to process certain data. When consent is requested, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent and make an informed decision. 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. Whenever we have been provided with consent to perform activities, consent may be withdrawn at any time by contacting us requesting its removal.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information. We may also use your personal information in the following situations; however, these are likely to be rare:

- Where we need to protect your interests (or someone else's interests).
- Where it is needed in the public interest [or for official purposes].

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

We will only use your Personal Data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your Personal Data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Parties with whom we share information

We may have to share your data with third parties, including third-party service providers and other entities in those groups. We will only disclose your Personal Data to third parties where required by law, or, to our employees, contractors, designated agents, or third-parties 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.

We will also exchange 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.

We only permit third parties 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 who provide products or services to us that we use in conducting our business, including administering or managing our relationship with our employees. Personal Data you provide to us for instance will be shared with our payroll provider to ensure payments are made to you in line with our contractual obligations. 'Agents or Suppliers' may also include, but are not limited to, recruitment agencies, end clients, software providers, benefits administration providers (including those involved in 401(k)s), data storage or hosting providers, as well as our insurance broker, insurance underwriters and lawyers. In the unlikely event that you owe us money for instance, we will take steps to recover our funds which may involve sending your information to an external debt collection agency and/or tracing service.
3. **Other 3rd parties:** To fulfil our contractual obligations, such as pay you we may need to share your information with third parties, such as the recruitment business for example (or end client where there is no recruitment business in the contractual chain); this may include exchanging information on hours worked, payments and tax deductions. We may also need to share information with a third party to demonstrate our compliance. We may be required for example, to send a copy of your payslip to the recruitment business to show that correct deductions have been made. We may also be required to share your Personal Data when responding to requests from recruitment businesses, end clients and/or other third parties who may, for example, be carrying out audits, due diligence, debt-collection or legal/tax investigations. This may include providing employment references and/or exchanging information on hours worked, payments and tax deductions, as well as evidence of right to work and identity checks.
4. **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.
5. **Other external bodies:** in certain circumstances, we may be required by law to disclose Personal Data to external bodies, such as local authorities and government departments. 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.
6. **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 the employment offer. PayStream International's sister companies and related entities were incorporated and operate from England.

In certain circumstances, for purposes defined in the Privacy Notice, we may be required to share your Personal Data with other business entities, third parties or clients internationally. This includes data accessible by a member of our group of companies on our database and systems.

We have controls in place designed to protect your Personal Data when it is transferred to other countries by means of access and/or use for provision of services. We will only share or disclose information to third parties where it is necessary for their intended purpose (for example, in order for a supplier to provide the products or services), we require all third parties to ensure that the information is adequately protected and will ensure that all transfers are made in accordance with data protection law with appropriate or suitable safeguards put in place to secure the data.

How we protect your Personal 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. 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. Where we share data externally, we do this securely so as to reduce the likelihood of any data breach. We require third parties to respect the security of your data and to treat it in accordance with the law.

How long we keep data

Personal Data 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 Data will depend on the type of information and the purpose for which it was obtained.

To determine the appropriate retention period for personal data, we consider:

- The amount, nature and sensitivity of the personal data.
- The potential risk of harm from unauthorised use or disclosure of your personal data.
- The purposes for which we process your personal data and whether we can achieve those purposes through other means.
- The applicable legal requirements.

Where you do not join our employment, we will hold your Personal Data, 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 our employment, we will hold your Personal Data for the purposes outlined below for 7 years from the date of termination of your employment unless we are legally required to hold it for longer. 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

The rights we set out below are relevant to UK and European citizens and residents. If you are based internationally (for example, the USA), we will use our reasonable endeavours to uphold and offer you the same rights, where possible and at the discretion of PayStream International. Where local state law requires alternative or additional rights, we will uphold these accordingly.

Right of Access (Gaining access to and copies of your Personal Data): 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. We may also charge a reasonable fee if your request for access is clearly unfounded or excessive, or, we may refuse to comply with the request in these circumstances. We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

Right to Rectification (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.

Right of Erasure (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 will retain the data we need to fulfil our obligations. Individuals can request deletion of their Personal Data from our internal systems, by contacting our Privacy Team. We will respond promptly to your request, and provide reasons if we object to the deletion of any of your Personal Data.

Right to Restrict processing of your data: 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.

Right to Data Portability (Moving your data): where it is possible for us to provide it, to receive a digital copy of the Personal Data that you have provided to us.

Right to withdraw consent: In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal data for a specific purpose, to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Privacy Team. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

Rights in relation to Automated decision making and Profiling: We do not envisage that any decisions will be taken about you using solely automated means. Should this position change, you will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis and we have notified you. If we make an automated decision based on any sensitive personal information, we will request your explicit written consent unless this is justified in the public interest, with appropriate measures in place to safeguard your rights.

Marketing

Where you have previously engaged with us, and we have communicated with you in relation to our employment, or you have entered into a contract with us, we may contact you from time-to-time. There are various reasons why we may contact you in relation to your relationship with us and the services you have shown interest in, and not always in respect of marketing. However, our marketing team may contact you for legitimate reasons relating, but not limited to:

- The services we provide;
- Communication of newsletters, industry news or safety bulletins on local environmental issues;
- In relation to local events, holidays or festivals; and
- To understand your perceptions of our services from a business or legal aspect.

We may use your Personal Data to contact you via post, phone and/or email. If you don't want to receive marketing contact from us you can let us know at any time.

Changes to your Personal Data

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes. If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact the Privacy Team in writing.

How to contact us

We have a dedicated Privacy Team to oversee compliance with this Privacy Notice. If you have any questions about this Privacy Notice or how we handle your personal information, please contact the Privacy Team at PayStream

International. You can contact our Privacy Team by email to info@paystreaminternational.com or via post to: Privacy Team, PayStream International LLC, 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 Data, or you are unhappy in any way with the information we provide to you, we would like you to contact us directly so that we can address your complaint. You can contact us by email at info@paystreaminternational.com or via post at *Privacy Team, PayStream International LLC, Mansion House, Manchester Road, Altrincham, WA14 4RW, UK.*

Changes to our Privacy Notice

This Privacy Notice does not form part of any employment offer or other contract to provide services.

We reserve the right to update this Privacy Notice at any time and we will provide you with an updated copy of this Privacy Notice where we make any substantial updates and/or we may also notify you in other ways from time to time about the processing of your personal information. We encourage you to periodically review this Privacy Notice which is available to you on request, to be informed of how we use your information.

If you have any questions about this Privacy Notice, please contact the Privacy Team as outlined above.