# PayStream's Pre-employment Privacy Policy

PayStream Accounting Services Limited (part of My Max Holding Limited)

#### Introduction

We think it's great that you're applying for a role at PayStream! We want to let you know that any personal information that you provide to us during your recruitment process will be kept safe. We take data protection seriously and this policy will explain how we use any personal information that we collect about you.

# What personal data do we process and why?

Personal information that we may collect, use, store and transfer about you are as follows:

- Identification details: your name, address, contact details.
- Recruitment and candidate selection information: details of your skills and experience, education, qualifications, employment history, psychometric testing, interview notes, other employment details (where applicable), information relating to the outcome of your application, details of any offer made to you and any details obtained during social media screening.
- **Right to work information**: right to work verification.
- Enhanced employment checks: which could include ID confirmation, 5 years address history, right to work check, sanction check, bankruptcy/Insolvency/IVA CCJ (up to £10,000), five-year employment history, gap referencing.
- Information related to your engagement: employment references and character assessment (whether internal or external).

We may also collect, store and process the following special categories of more sensitive personal information:

- **Health information**: for example, where you notify us of a medical condition or disability that may impact the recruitment and selection process (e.g. your ability to complete the psychometric assessments).
- **Information about criminal convictions or offences:** for example, where you are offered a position at PayStream and this is applicable to your role. Criminal records basic disclosure.

Further information as to how we treat special category data is outlined in our **Special Categories of Data Policy**, which can be provided on request.

# How do we collect personal information?

Directly from you - when you complete our pre-employment questionnaire, send us your CV, provide any
information to us when applying for a position at PayStream or take part in our interview process.

From a recruitment business - if you have been referred by a recruitment business, they will have given us your name, email address and CV.



- From a third-party psychometric profiling company if your application is passed through to the next stage of the recruitment process, we will normally ask you to complete an online psychometric assessment and we currently use a company called Elenchus for this purpose. Please note, we share first name and email address only with this third-party provider. In regards to the online assessment, Elenchus use a combination of personality, aptitude and occupational preference assessments and provide a very comprehensive picture of a candidate, which will help us determine your suitability for working at PayStream. The assessments are free of bias and are administered, validated and results determined by a suitably trained person. If you do not complete the online assessment, we will not be able to employ you. Please refer to the Elenchus website if you require any information on their privacy policy <a href="https://www.elenchus.co.uk">www.elenchus.co.uk</a>
- During social media screening we may carry out social media screening if you are offered a role with us. The objective is to find out more about your past and establish if there is anything we should be aware of before hiring you that would impact your ability to do the role, or to highlight if values do not align. We will consider any behaviours that violate acceptable standards of conduct or that could negatively impact our reputation, brand, damage our culture and to protect our existing employees. This can include but is not limited to the sharing of illegal activities, offensive comments, violent or aggressive behaviour, sexually explicit material, or the sharing of confidential information and any information that could mean a threat to our data security. We consider that the social media screening of candidates following any job offer is a proportionate means to achieving this aim. In reviewing social media, we are also looking for reasons to hire an individual and will look for information to support a candidate's qualifications. The social media platforms of candidates also provide a means of checking the accuracy of some information provided by them, for example their CV history. It is only one part of the assessment process to determine the candidate's suitability for the role and will not in itself determine suitability. We will not retain any personal information obtained during social media screening, where a job offer is made.
- During enhanced employment checks for certain roles, where you may have access to sensitive data or have escalated systems permissions, we will conduct enhanced employment checks. Such checks must be completed prior to you starting employment with us. If you are offered a role where enhanced checks are required you will be given more information on these checks and what data will be collected at the offer stage. We share first name, surname and email address only with this third-party provider.
- Through our HR and onboarding system (CIPHR) as part of our onboarding and pre-employment process, we use CIPHR, a secure cloud-based HR system. You will be asked to log in to CIPHR to provide certain personal details, such as your contact information, bank details and other pre-employment forms. We share limited information with CIPHR to create your account and enable you to complete your onboarding tasks before your start date. CIPHR acts as our data processor and processes this information strictly in accordance with our instructions and the terms of our data processing agreement. All data is stored securely within the UK in compliance with the UK GDPR and Data Protection Act 2018. You can find more information about CIPHR's privacy practices here: <a href="https://www.ciphr.com/privacy-policy/">https://www.ciphr.com/privacy-policy/</a>
- From referees, either external or internal to be conducted following an offer of employment.
- From Occupational Health and other health providers to comply with health and safety laws.

### Lawful basis for processing your personal data

Depending on the processing activity, we rely on the following lawful basis for processing your personal data under the UK GDPR:

Compliance with our legal obligations: for example, we are required to check entitlement to work in the
UK, comply with health and safety laws (including assessing someone's fitness for work), and comply with
the Equality Act 2010 duties.



We collect information about you so that we can decide whether you are suitable for a role at PayStream. If you have been referred to us from a recruitment business, we may discuss your potential with your recruiter. We collect, use and retain your personal information for legal reasons. It is a statutory requirement and we act within the realms of employment law. It is important that we get the right candidate for the job.

- For the performance of a contract: for example, we require your personal details in order to enter in to a contract with you.
- Legitimate interests: for example, we may need to conduct enhanced checks where certain roles require
  elevated permissions or have access to financial and commercially sensitive data, or where we obtain
  occupational health advice to ensure we comply with duties in relation to individuals with disabilities. Or
  where we collect, use and retain psychometric data for the purposes of ensuring we get the right candidate
  for the job and so it is in our legitimate interests to do so.

## How long do we keep your personal data?

We will only retain your personal data for as long as necessary to fulfil the purposes for which it was collected.

If you are unsuccessful in this process, we will retain your personal information for 12 months (from the date of your application or the date that your details were sent over to us by the recruitment business), for legal reasons (for example to protect the business in the event of any discrimination claim) and because it is in our legitimate interests to do so (for example to monitor duplicate candidate applications and so we can fulfill our contractual obligations to recruitment agencies where applicable) then delete it. If your application is successful and you go on to join PayStream, your personal information will be processed in accordance with our Privacy Policy, which will be provided to you as part of your onboarding.

## Who will have access to your data?

Your personal data will be shared internally with members of the HR and Careers team. This will also be shared with the recruitment panel - for the selection to interview process.

We share your data with third parties in order to:

- Obtain psychometric testing results as part of the recruitment and selection process
- Obtain pre-employment references from other employers
- Obtain employment background checks
- Obtain criminal record checks

We use Adobe Sign, a secure electronic signature service to send and manage employment contracts. We share limited personal information (such as email address) with Adobe Sign for this purpose. Adobe Sign acts as a data processor and processes this data on our behalf in line with strict data protection and security standards.

#### International data transfer

Some of our third-party software providers may transfer data outside the UK, this may also be the case when we are providing information as part of an audit on our processes, a requirement for certain certifications or accreditations.

Where we transfer personal information to third parties outside of the UK, we have put in place procedures and safeguards to ensure the personal information receives the same levels of protection as if it were being processed inside the UK, such as the approved EU standard contractual clauses with the UK addendum or the international data transfer arrangements. Any transfer of your personal information will follow applicable laws and we will follow the guiding principles of this policy



## Your rights

You have a number of rights in respect of your personal information:

- The right to be informed: you have the right to be informed about the collection and use of your personal information.
- The right of access: you have the right to request a copy of the information that we hold about you.
- The right to rectification: you have the right to ask us to rectify any information you think is inaccurate. Please ask us to correct or remove information you think is inaccurate and we will let you know once we have done this.
- The right to erasure: We will only use your personal information as we have described in this Privacy Policy, but, in the unlikely event that we use it in a different way, you can ask us to delete it.
- The right to restrict processing: you have the right to ask us to restrict the processing of your information in certain circumstances.
- The right to object: you have the right to object to processing of your personal information in certain circumstances.
- **Right to request transfer**: you have the right to ask that we transfer the personal information you gave us to you or another person in certain circumstances.
- The right not to be subject to automated decision making and profiling: You have the right to not be subject to solely automatic decisions (i.e., decisions that are made about you by computer without any human input) in relation to any processes that have a legal or similarly significant effect on you. You will be notified if we make a solely automated decision which produces a legal effect or significantly affects you. We do not make any recruitment or onboarding decisions based solely on automated processing or profiling. All hiring decisions are made by our HR and recruitment teams, supported by human review. However, the law now allows some automated systems to be used more widely if we put the right safeguards in place. If we ever use automation that affects you for example, an assessment tool you'll be told and you'll always have the right to ask for a person to review or change the outcome.

If you would like to exercise any of these rights, please contact the HR department on hr@paystream.co.uk.

# Subject access request

If you would like to see the personal information we hold about you, you can make a **Subject Access Request (SAR)** by emailing **hr@paystream.co.uk**.

When we receive your request, we'll carry out a reasonable and proportionate search to find the information that relates to you.

If we need more details to locate what you're looking for (for example, specific dates or documents), we may pause the response timeframe ("pause the clock") until we have this information. We'll let you know if that happens.

We normally respond within **one month**, but if your request is complex or you've made several requests, this may take up to **three months**. We'll tell you within the first month if we need extra time.

If a request is unfounded or excessive (for example, if it repeats a previous request), we may refuse to process it, but we'll always explain why.

# Unsolicited Personal Data

If we receive CVs submitted on a speculative basis and/or at a time when we are not recruiting, please be advised that we, in line with our obligations under data protection law, will delete the personal information received.



## Changes to our Privacy Policy

We keep our Pre-employment Privacy Policy under regular review and should we change it during the recruitment process, we will provide you with an updated copy.

#### How to contact us

If you have any questions about this policy or the information we hold about you, please contact <a href="https://hream.co.uk">hr@paystream.co.uk</a> or write to HR Department at PayStream, Mansion House, and Manchester Road, Altrincham, WA14 4RW.

If you have a concern about how your personal data has been handled, please contact the HR team on the email above. We will log and investigate all data-related complaints and respond in writing.

The Information Commissioner Office regulates data protection. If you feel that your data has not been handled correctly, or you are unhappy with our response to any requests you have made to us regarding the use of your personal information, you have the right to lodge a complaint with the Information Commissioner's Office. You can contact them by calling 0303 123 1113 or visit the website.

For further information on data protection please visit the Information Commissioner Office (ICO) website.

