



pay.uk

**Applicant Privacy
Notice**

October 2019

Introduction

Your privacy is important to us so we developed this Privacy Notice to explain how we manage and look after your information. The EU General Data Protection Regulation (the “GDPR”) and the Data Protection Act 2018, together known as Data Protection Legislation), provides individuals with a number of rights including right of access to their personal information, called a Data Subject Access Request (“DSAR”).

Scope

This notice applies to personal information relation to your application for full- or part-time employment with Pay.UK and its associated companies, under any of the following contract categories:

- Permanent and temporary employees;
- Fixed-term contractors;
- Agency workers;
- Day-rate, limited company or service contractors or consultants;
- Secondees; and
- Persons on an internship or industrial placement.

This notice applies to personal information relating to your prospective employment or engagement with Pay.UK Limited or its associated companies as data controllers, as described below.

This notice explains:

- What information we collect about you;
- How we will use that information;
- Who we will share it with; and
- What steps we will take to ensure it stays private and secure.

This Privacy Notice covers all aspects of your interaction with Pay.UK and its associated companies, in your capacity as an applicant, including recruitment and pre-employment screening. We may update this policy at any time.

Throughout this notice, when we say, “you” or “your”, this refers to you or any authorised person who engages with us on your behalf, such as recruitment agencies you have authorised to liaise with us on your behalf).

Throughout this notice, when we say “we”, this refers to Pay.UK and its associated companies (as detailed in Appendix A), which act as a data controller in respect of your personal data in your capacity as an applicant. The data controller for the purpose of this notice will be Pay.UK Limited unless otherwise stated below.

Should you wish to contact us, you may do so using the contact detailed set out in the “Who we are” section below.

Who we are

We are Pay.UK, the UK's leading retail payments authority.

Our business address is:

Pay.UK Limited

2 Thomas More Square

London E1W 1YN

Letters should be addressed for the attention of our Data Protection Officer.

You can contact us in the following ways:

- By speaking to your line manager;
- By writing to the above address;
- By emailing us at DPO@wearepay.uk;
- By telephoning us on 020 3217 8200.

Why Pay.UK collects and processes your personal information

We collect and ask for personal information about you in order to:

- identify you;
- administer your applicant relationship with us, e.g. schedule interviews, communicate decisions etc.
- consider any applications or requests for information or advice made by you;
- comply with our legal or regulatory obligations;
- protect our legal rights;
- pursue our legitimate interests and meet our business needs;
- carry out your instructions, e.g. with regards to any benefits selections you make;
- manage our relationship with you, including informing you of other roles and services we think may be relevant to you. You may opt out of receiving such notifications.
- prevent or detect crime including fraud and financial crime, e.g. financing for terrorism, human trafficking or market abuse;
- conduct applicant surveys and data analytics in order to better understand our recruitment reach; and
- for the purpose of converting an applicant to a colleague.

We also process your personal information for the following purposes:

- For service, system or product development and planning, insurance, audit and administrative purposes.
- For security, staff vetting or business continuity; and
- For risk management.

What personal information do we process?

We will collect and process personal information that you provide to us, e.g. as part of the recruitment and on-boarding processes, in line with relevant regulations and law. The information may relate to any of the roles you apply for, currently hold or have held in the past, both within and outside Pay.UK and its associated companies.

Examples of the categories of personal information we collect and process at various stages of your relationship with us are provided below. Please note this list is not exhaustive:

Employment stage	Examples of personal information processed
Application and vetting	Name and documentation confirming ID Contact details (home address, telephone number) Employment history National Insurance (NI) number Passport and other Right to Work documentation details
On-boarding (following offer of employment)	Bank details Date of birth Health information relevant to the role Next of Kin and Emergency contact details Beneficiary and dependant details for benefits registration Work-related contact information

Special Category data

Certain 'special categories' of more sensitive personal information (such as information about racial/ ethnic origin, sexual orientation, political opinions, religious/ philosophical beliefs, trade union membership, biometric or genetic data and health data) are given a higher level of protection by data protection laws.

The special categories of more sensitive personal information we may collect, store and use includes, but is not limited to, the following categories of information:

- Information about your race or ethnicity:
- Information about any criminal, court, and police records, including barred, and watch lists that pertain to you. This may include driving records, including driving licence details and copy, status, points, convictions, sanctions and restrictions; and
- Information about your health, including any medical conditions, medical history, health and sickness records, including results from occupational health assessments.

Health

Following your acceptance of our employment offer and prior to the commencement of your employment, we will ask you to complete a health questionnaire assessed by our occupational healthcare professional to advise us if any adjustments are needed to the work environment or systems so that you may work effectively. This may be undertaken by an authorised third party on our behalf with whom we will share any relevant personal information, including special category data as may be deemed necessary.

Once the assessment is complete, we will use it to make any necessary adjustments and it will be placed in your HR file. This data is processed on the basis of the contract between yourself and us. The outcome of this occupational health assessment is shared with Pay.UK.

Please note that Pay.UK may, in addition to the occupational health assessment, provide medical assessments to its employees from time to time. Any data collected and processed as part of any such medical assessment is done so by a third party provider under the terms of its privacy policy.

Race and ethnicity

We collect and process information on race and ethnicity of our applicants for the purpose of equal opportunities matters including the operation of an equal opportunities policy, identifying or keeping under review the existence or absence of the quality of opportunity, or treatment between persons of different protected characteristics, with a view to enabling such quality to be promoted, or maintained.

The lawful reasons for processing these are legitimate interest, legal obligation and in order to perform our contract with you. The lawful basis for processing, as defined in Art.6 will first be determined, following which the lawful basis for any special category data will be determined as defined in Art.10.

Vetting

When you apply for a role we request various information including your name, phone numbers, and email address. We will also request information about your previous experience, education, qualifications, most recent position, current employer, current compensation package and compensation expectations, skills, competencies, right to work information, CV and for answers to questions relevant to the role you have applied for. This applies only to colleagues directly engaged with Pay.UK, and therefore excludes colleagues engaged via a consultancy agreement.

We will use the information provided by you and others as detailed above to request, collect and process your personal data as part of our vetting procedures. This will be in order to confirm your identity, employment history and relevant qualifications with respect to a role, to comply with the law and for our legitimate interests to be able to assess and manage our risk.

We collect personal data for vetting through the application and recruitment process directly from applicants by the Pay.UK People team, who will have access to all of this information. Some of this information will also be made available to our hiring managers. Third party providers may also collect personal data for vetting purposes on our behalf.

The personal information we will typically collect, store, and use for vetting purposes will include the following categories of personal information:

- Personal contact details, e.g. name (full current and previous) legal names and alias, title, addresses, telephone numbers and personal email addresses;
- Information on family members and dependents;
- Date of birth and gender;
- National insurance number;
- Location of employment or workplace;
- Recruitment information, e.g. copies of documentation confirming your right to work in the United Kingdom, references and other information included in a CV or cover letter as part of the application process;
- Information concerning any qualification you hold, e.g. higher and further education, and professional certifications; and
- Employment records, e.g. job titles, work history, working hours, training records and professional memberships.

The vetting checks we perform may include:

- A right to work in the United Kingdom check, which includes documents to prove identity or address, and your immigration status;
- Verification of identity, which includes your Personal details such as your name (current and former), date and place of birth, gender or sex, address history, contact information, nationality, photograph, documents to prove identity or address, government-issued identity numbers;
- A credit reference check, which may include an Adverse Financial Check. Financial history checks may include credit reports, bankruptcy, court records, tax information, salary and income, real estate ownership, shareholding, financial sanctions;
- A conduct check, which may include a Criminal Records Check, court, and police records, including barred, and watch lists;
- Media coverage, including social media, politically exposed persons, press articles, press releases, internet activity (e.g. blogs, forums etc. used to express opinions);
- Professional credentials, designations, licences, memberships, associations, awards, sanctions or reprimands;
- Education history, including institution's name, period, status, location, performance, exam results, qualifications awarded, disciplinary or sanctions, supervisor, conduct, opinions about you;
- Employment / Occupational History Check; (including volunteering) and self-employment history, including employer's name, period, job title, status, location, duties, performance, compensation, disciplinary or sanctions, supervisor, conduct, reason for leaving, opinions about you;
- Gap history, including activities you have undertaken, period, documents to prove these, character referees, opinions about you;
- Conflict of interest checks; and

- Bank of England non-objections for certain senior positions.

We will only use your personal information for the purpose 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 reason, we will notify you and explain the legal basis which allows us to do so.

Please note that we may process your personal information without your prior knowledge or consent, where this is required or permitted by law.

Criminal convictions

We may request and process information about criminal convictions where appropriate and where we are legally able to do so. We may also collect information about criminal convictions to meet our legal obligations in respect of your application. We may collect information about criminal convictions in any country where you have resided for a period of six months or more within the last five years, where we are legally able to do so. We undertake Standard DBS vetting on our colleagues, which details spent and unspent convictions, cautions, reprimands and final warnings held on police records. You will receive a copy of the disclosure information we receive.

We have in place appropriate policy and safeguards which we are required by law to maintain when processing such data.

Credit Reference Checks

As part of your application, we may perform credit and identity checks on you with one or more credit reference agencies (CRAs). We will conduct credit reference checks with CRAs in any country where you have resided for a period of six months or more within the last five years.

To do this, we will supply your personal information to CRAs, and they will give us information about you.

This will include information from your credit applications and about your financial situation and financial history. CRAs will supply us with both public (including the electoral register) and shared credit information, financial situation, history and fraud prevention information.

We may use this information to:

- Prevent criminal activity, i.e. fraud
- Manage your application.

We will continue to exchange information about you with CRAs while you have a relationship with us, usually by means of biennial checks. This information may be supplied to other organisations by CRAs. Please refer to **Appendix B** for more details on CRAs.

Where we collect your personal information from

We may collect information from a range of sources, which may relate to any roles you apply for, currently hold or have held in the past, both within and outside Pay.UK, including its associated companies. We may also collect information about you when you interact with us, e.g. call us, visit our website or use services we make available to you in your capacity as a colleague.

- Some of this information will come directly from you, e.g. when you provide documentation to verify your identity or right to work.
- Such information may also come from your previous employers, including companies associated with Pay.UK, or sources from whom you have asked us to obtain information. We may also obtain personal information from publicly available sources.
- The information we collect may include:

Information that you provide to us, e.g.:

- Personal details, e.g. name, previous names, gender, date and place of birth, employment history;
- Contact details, e.g. address, email address, landline and mobile numbers;
- Next of kin and emergency contact details, including email address, landline and mobile numbers;
- Information concerning your identity e.g. photo ID, passport information, National Insurance number or equivalent tax identification number, National ID card, birth number (or equivalent) and nationality;
- Information pertaining to any qualifications you hold, i.e. further or higher education and professional qualifications / certifications;
- Health data including medical conditions, medical related absence records, health and sickness records or confirmation of whether you are able to perform a given position (as applicable), and information on any disabilities you may have;
- Market research, information and opinions expressed when participating in applicant surveys;
- Other information about you that you provide when completing forms or communicating with us, whether face-to-face, by phone, email, online or other means.

Information that we collect or generate about you, e.g.:

- Information we use to identify or authenticate you, e.g. your signature, or additional information we receive from external sources that we require for compliance purposes;
- Geographic information, e.g. about which Pay.UK building floors and sections you access. Please refer the “Monitoring” section below for further information;
- Cookies and similar technologies we use to recognise or authenticate you, or to remember your preferences and tailor the content we provide to you. Please refer the “Monitoring” section below for further information;

- Investigations data, e.g. due diligence checks, fraud, sanctions, and anti-money laundering checks, external intelligence reports, content and metadata related to relevant exchanges of information between and among individuals, organisations, including emails, voicemails, live chat and any opinions you express in relation to any issues that are the subject of an investigation;
- Complaints information;
- Application data including information about your individual performance in assessments or online tests;
- Records of correspondence and other communications between us, including email, live chat, instant messages and social media communications;
- Information that we need to support our regulatory obligations, e.g. information about transaction details, detection of any suspicious and unusual activity and information about parties connected to you or these activities (e.g. politically exposed person and sanction checks);

Information we collect from other sources, e.g.:

- Information you have asked us to collect for you, or which we collect as part of our vetting process as set out below, e.g. occupational health reports, work references from previous employers and information about your previous roles with Pay.UK and its associated companies.

Please note that the type of personal information we collect about you will depend to some extent on your personal circumstances, your role and our legal obligations.

How we use your information

We will only use your information where we have your consent or another lawful basis for so doing.

These reasons include where we:

- Need to pursue our legitimate interest, e.g. to assess your suitability for the role you are applying for. Where we rely on legitimate interests as the reason for processing personal information, we have considered whether those interests are overridden by any separate rights or freedoms of our workforce and have concluded that they are not.
- Need to process the information to comply with a legal obligation; or
- Believe the use of your information as described is in the public interest (e.g. for the purpose of preventing or detecting crime, or for equal opportunity monitoring or reporting purposes).

We may also process your personal information in the following circumstances, but this is likely to be rare:

- with your specific consent.
- where we need to protect your vital interests (or someone else's vital interests).

- Where we believe the use of your information as described is in the public interest (e.g. for the purpose of detecting or preventing crime).

How we make decisions about you

Your personal information is not subject to automated decision-making, including profiling. In some circumstances we may anonymise your personal information so that it can no longer be associated with you; in such circumstances we may use such information without further notice to you. Once you are no longer a colleague, we will retain and securely destroy your personal information in accordance with our data retention policy.

Who we may share your information with

We may share your personal information with others where lawful to do so, including where we or they:

- Have a public interest or legal duty to do so, e.g. to assist with detecting and preventing fraud, tax evasion and financial crime;
- Need to do so in connection with regulatory, tax or withholding reporting, litigation or asserting or defending legal rights and interests;
- Have a legitimate business reason for doing so, e.g. to manage risk, verify your identity, or to assess your suitability for roles;
- Have asked you for your permission to share it, and you have agreed;
- Need to do so in order to provide you with products or service you have requested, e.g. sharing your details with a private health insurance company.

We may share your information for these purposes with others including the following recipients:

- Law enforcement, government bodies, courts, dispute resolution bodies and agencies (e.g. HMRC for tax purposes)
- Our regulators (e.g. Payment Systems Regulator, Information Commissioner's Office, the Financial Conduct Authority), and any party appointed by a regulator to undertake an investigation or audit of our activities;
- Agents and sub-contractors who work for us and other Pay.UK associated companies, including their employees, sub-contractors, service providers, directors and officers). Said individuals help us provide services e.g. processing compensation, providing employee benefits, and performing legal and other professional services. Those companies and individuals have access to your data as needed to perform their functions, however they are not permitted to use it for other purposes;
- Your beneficiaries or intermediaries;
- Third party service and benefit providers (e.g. when we outsource some of the operations of our business to third party service providers. We restrict how such service providers may access, use and disclose your data);

- Tax authorities, trade associations, credit reference agencies;
- Legal and professional advisors, including auditors;
- The other parties involved or interested in a corporate transaction and their advisors;
- Courts, to comply with legal requirements, and for the administration of justice; and
- Anyone else where we have your consent or as required by law.

If we share your information, we will advise you at the time of who the data is being shared with. We will not share your data for marketing purposes.

The terms of our contracts with third parties include obligations on them in relation to what personal information they can process and what they can do with that information. All our third party service providers, professional advisers (and other companies associated with Pay.UK) are required to take appropriate security measures to protect your personal information in line with our policies.

We do not permit our third party service providers to use your personal information for their own purposes – they may only process your personal information for specified purposes and in accordance with our instructions.

Tracking or recording what you say or do

We may record details of your interactions with us, including conversations you have with us including phone calls, face-to-face meetings, letters, emails and recorded conference calls.

Closed Circuit Television (CCTV)

Closed Circuit Television (CCTV) is operated by Pay.UK and the in and around our building and these may collect photos and videos of you, or record your voice. The system operates 24 hours a day, 7 days a week, is monitored, and retained. All entrances and exits to each floor are monitored to ensure safety and security and are not used for active monitoring. The processing of your personal information will be carried out to pursue our legitimate interests and in a way that might reasonably be expected as part of running our business and does not materially impact your rights, freedom or interests.

Physical access to premises (door control)

Access in and around the building is provided, and controlled, by Pay.UK. The system operates 24 hours a day, 7 days a week, is monitored, and retained. Physical access is on the basis of role in the Company: there is general access to public areas; there is specific access to company areas. The processing is necessary for your safety and security, and for compliance with the Health and Safety at Work Act 1974.

Transfer of personal data outside the European Union (EU)

We are committed to implementing technical and organisational measures that, by default meet the requirements of the data protection legislation and the appropriate level of security. We will not share your personal data with a third party organisation without a valid business reason, a contract or Data Sharing Agreement in place, or without your consent.

Your information will not be transferred to, or stored in locations outside the European Economic Area (EEA), unless that country or territory can ensure an adequate level of protection in relation to the processing of your personal data. We may need to transfer your information in this way to carry out our contract with you, to fulfill a legal obligation, to protect the public interest and/or for our legitimate interests. In some countries the law might compel us to share certain information, e.g. with tax authorities. Even in these cases, we'll only share your information with people who have the right to see it.

How we protect your personal information

We use a range of measures to keep your information safe and secure which may include encryption and other forms of security. We require our colleagues and any third parties working on our behalf to comply with appropriate compliance standards including obligations to protect any information and applying appropriate measures for the use and transfer of information.

We have security measures in place to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, or inappropriately altered or disclosed. In addition, we limit access to your personal information to those who need to process that information for business reasons. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected information security breach and will notify you and any applicable regulator of a suspected breach as appropriate and in accordance with our legal obligations.

How long we will keep your personal information

We retain your data primarily to meet statutory and regulatory obligations. Your data is also retained to enable us to pursue our legitimate business interests in relation to our clients, our current and future requirements.

We keep your information in line with our data retention policy. For example we normally keep your core application data for a period of seven years from the end of our relationship with you. The data retention policy, and other colleague policies are available on request from the People or Legal teams.

This will be in line with our data retention schedule. This enables us to comply with legal and regulatory requirements or use it where we need to for our legitimate purposes such as dealing with any disputes or concerns that may arise. If you have applied for a job with Pay.UK or its associated companies, and are unsuccessful, we will retain any personal data collected for a period of 12 months from the date you are formally rejected. If you are required to complete an online assessment as part of your application, your test results may be valid for future job applications and we will keep them for a period of 12 months, after which your test results will be deleted and subsequent applications may require a new online assessment.

For successful applicants, we will retain your data in accordance with legal, regulatory and business requirements as set out in our data retention schedules - all of which you will have full access to upon joining us.

We may need to retain your information for a longer period where we need the information to comply with regulatory or legal requirements or where we may need it for our legitimate purposes,

e.g. to help us respond to queries or complaints, fighting fraud and financial crime, responding to requests from regulators, etc.

- If we do not need to retain information for this period of time, we may destroy, delete or anonymise it more promptly. We anonymise your personal information so that it can no longer be associated with you; in such circumstances we may use such information without further notice to you. Once you are no longer a colleague, we will retain and securely destroy your personal information in accordance with our data retention policy.
- We will only use your personal information for the purposes for which we collected it. If we need to use your personal information for an unrelated purpose, we will notify you and seek your agreement or consent, as appropriate.

We will only process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

Our retention schedules are available on request.

Your responsibilities

Please ensure you inform us of any changes to your personal information. This is in line with your responsibility to ensure that the information you give us is accurate and up to date.

The absence or inaccuracy of any records may affect the outcome of your application or we may be prevented from complying with our legal obligations.

Your rights

Data Protection Legislation gives you a number of rights regarding the information we hold about you:

- The right to be informed: our obligation to provide fair processing information;
- The **right of access** to the information we hold about you, and to obtain information about how we process it;
- The **right to rectification** allows you to request that we rectify your information if is inaccurate or incomplete
- The **right to erasure** allows you to request the deletion or removal of your personal data where there is no compelling reason for its continued processing. We may continue to process your information if we have another legitimate reason or legal obligation for doing so;
- The **right to restrict** processing allows you to 'block' or suppress processing of personal data in certain circumstances;
- The **right to data portability** - in some circumstances, the right to receive certain information you have provided to us in an electronic format and/or request that we transmit it to a third party;

- The **right to object** to, and to **request that we restrict**, our processing of your information in some circumstances. Again, there may be situations where you object to, or ask us to restrict, our processing of your information but we are entitled to continue processing your information and / or to refuse that request.

Requests, complaints or queries

We try to meet the highest standards when processing personal information. For this reason, we take any requests, complaints or queries we receive about this very seriously. We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading or inappropriate.

This Privacy Notice does not provide exhaustive detail of all aspects of our processing of personal information. However, we are happy to provide any additional information or explanation needed. If you want to make a query, request, or a complaint about the way we have processed your personal information you can contact us directly at the details set out above.

Alternatively you have the right to lodge a complaint with the regulator which oversees data protection law:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

SK9 5AF

Tel: 0303 123 1113

Changes to this privacy notice

Our Privacy Notices are reviewed regularly, and we will host the most updated versions on relevant internal and external webpages for colleague reference. Where an update to a Privacy Notice results in a change, this will be clearly identified by reference to the date of the notice.

Appendix A – Pay.UK and associated companies

Pay.UK Limited

New Payment System Operator ('NPSO')

Faster Payments Service ('FPS')

Cheque and Credit Clearing Company ('C&CCC')

BACS Payment Schemes Ltd ('BACS')

UK Payments Administration Ltd ('UKPA')

Appendix B – Credit Reference Agencies ('CRAs')

The identities of the CRAs, their role also as fraud prevention agencies, the data they hold, the ways in which they use and share personal information, data retention periods and your data protection rights with the CRAs are explained in more detail at:

- Call Credit–www.callcredit.co.uk/crain
- Equifax–www.equifax.co.uk/crain
- Experian–www.experian.co.uk/crain