



ARBUTHNOT LATHAM  
Bankers since 1833

# HR Privacy Notice

## Introduction

Arbuthnot Latham is committed to being transparent about how it collects and uses employee data to meet our data protection obligations under UK data protection law. This privacy notice sets out how we collect and process your personal data in order to manage the employment relationship.

This notice applies to job applicants, current and former employees and, where applicable, to data held in relation to workers and contractors.

When we refer to Arbuthnot Latham, we mean:

- Arbuthnot Latham & Co., Limited (registered with the UK Information Commissioner’s Office (ICO) as a data controller under registration number Z6024586); and
- Its business names, subsidiary companies, and its parent company. These include Arbuthnot Banking Group PLC, Arbuthnot Commercial Asset Based Lending Limited, Renaissance Asset Finance Limited, Gilliat Financial Solutions, and Tay Mortgages.

You can find out more information about us at <http://www.arbuthnotlatham.co.uk/>

## Our Data Protection Office

If you have any questions, or would like more details about how we use your personal information, you can contact the Data Protection Office using the details below:

Post	Arbuthnot Latham & Co., Ltd Arbuthnot House 20 Finsbury Circus London EC2M 7EA
Telephone	+44 (0)20 7012 2500
Email	<a href="mailto:DataProtectionOffice@arbuthnot.co.uk">DataProtectionOffice@arbuthnot.co.uk</a>

## What data do we collect about you?

We hold and process information about you for the purpose of your employment with us. This information is normally collected from yourself, through the application and recruitment process and the ongoing employment relationship. We may obtain additional information from third parties such as

employment agencies, former employers, credit checking agencies or other background checking agencies.

We may also hold and process information about you that does not relate to your employment with us, for example personal data provided for a specific project.

To view all of the data we collect about you please refer to HR Table 1 (HR Data Retention Table) below. This table also highlights any special categories of personal data we process, which is given a higher level of protection by UK data protection law.

## Why do we collect and process your personal data?

Most commonly, we will use your personal data in the following circumstances:

### 1. Where we need to comply with a legal obligation

For example, we are required to check your eligibility to work in the UK, to deduct tax, to comply with health and safety laws and to enable you to take periods of leave to which you are entitled. For example, as required under the Employment Rights Act 1996, the Equality Act 2010 etc.

### 2. Where we need to perform the contract we have entered into with you

For example, we need to process your data to provide you with an employment contract, to pay you in accordance with your contract and to administer benefit, pension and insurance entitlements.

### 3. Where necessary for legitimate interests which are not outweighed by your interests

We may ask for your consent to process your data where the basis for processing does not fall within the above three reasons. We may also, exceptionally, use your personal information where necessary to protect your interests (or that of another person) or where needed in the public interest.

## How we use your personal data

We will use your information primarily to allow us to comply with legal obligations and perform your contract of employment. The main circumstances in which we might process your information include the following. Those denoted with a (\*) indicate where we consider the legitimate interests ground applies (which may sometimes overlap with the other two grounds). Where this applies, we have outlined the legitimate interest relied upon in *italics* in brackets:

- To make decisions about your recruitment or appointment\* (*Necessary for our legitimate interest of managing a group-wide recruitment process*).
- To verify your identity.
- To determine the terms on which you work for us and administering your contract of employment with us \* (*Necessary for our legitimate interests in ensuring we employ staff on terms that fit our business structures*).
- To carry out appropriate checks on all relevant employees for fitness and propriety for the purposes of the Senior Managers and Certification regime.
- To carry out annual background checks on all non regulated employees.
- Checking you are legally entitled to work in the UK.

- Paying you, providing benefits to you and making appropriate deductions for tax and national insurance.
- Operate and keep records of other types of leave (including parental leave) to allow effective workforce management.
- Making decisions about salary reviews and compensation, promotions, or your continued employment or engagement\* (*Necessary for our legitimate interest to manage employee performance and career development*).
- Liaising with any third party provider of benefits (for example, pension benefits).
- Business management and planning, including accounting and auditing\* (*Necessary for our legitimate interest to ensure effective administration and management of your employment/ engagement, benefits, management of the business and business continuity*).
- Managing performance and conducting performance reviews\* (*Necessary for our legitimate interest to manage employee performance and career development*).
- For the purposes of grievances or disciplinary issues\* (*Necessary for our legitimate interest to ensure effective administration and management of your employment/ engagement, benefits, management of the business and business continuity*).
- Managing sickness absence and ascertaining your fitness for work\* (*Necessary for our legitimate interest to ensure effective administration and management of your employment/ engagement, benefits, management of the business and business continuity*).
- To comply with health and safety legislation.
- To prevent fraud\* (*Necessary for our legitimate interest to prevent fraud and prevent, detect, and investigate employee behavior, other malpractices or unsafe situations*).
- For education, training and development purposes\* (*Necessary for our legitimate interest to manage employee performance and career development*).
- To monitor your use of our IT systems and ensure compliance with any of our policies and procedures from time to time\* (*Necessary for our legitimate interest to manage and monitor use, maintenance and security of company network, data and systems and to prevent fraud and prevent, detect, and investigate employee behavior, other malpractices or unsafe situations*).
- To deal with any legal disputes which might arise involving you or other employees\* (*Necessary for our legitimate interest to ensure effective administration and management of your employment/ engagement, benefits, management of the business and business continuity*).
- Making arrangements for the termination of your employment or engagement\* (*Necessary for our legitimate interest to ensure effective administration and management of your employment/ engagement, benefits, management of the business and business continuity*).
- To provide references on request for current or former employees.
- To respond to and defend against legal claims\* (*Necessary for our legitimate interest to ensure effective administration and management of your employment/ engagement, benefits, management of the business and business continuity*).

- To provide equipment necessary to perform your role.
- To send you documentation and other materials, in relation to the administration of your employment or engagement or otherwise relating to your employment or engagement (including the conduct of your work activities) where it is not possible to do this using electronic means\* (*Necessary for our legitimate interest to ensure effective administration and management of your employment/ engagement, benefits, management of the business and business continuity*).

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.

## Special categories of personal data

In the case of the special categories of personal data identified in HR Table 1 (HR Data Retention Table) below, we may use this information for the following reasons:

- To comply with a legal obligation
- In the public interest, such as for equal opportunities monitoring
- To assess your working capability on health grounds, subject to appropriate confidentiality safeguards

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.

We will use this more sensitive personal information in the following ways:

- Relating to leaves of absence, which may include sickness absence information, to comply with employment and other laws
- About your physical or mental health or disability status, to ensure your health and safety in the workplace and your fitness to work, to provide appropriate workplace adjustments and to monitor and manage sickness absence and administer benefits; and
- About your ethnic origin, sexual orientation, religious beliefs or other protected characteristics, to ensure meaningful equal opportunities monitoring and reporting.

We will also use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our legal obligations.

In limited circumstances we may approach you to give your written consent to process special categories of personal data information which is not covered by the above reasons.

You should be aware that it is not a condition of your contract of employment with us that you agree to any request for consent from us.

## Where is my personal data stored/transferred and who will have access to it?

Internally, your data will only be accessed by the HR team for the purposes outlined above, and by other relevant staff where necessary as outlined below:

- Line managers &/or Executive Assistants
- Departmental heads
- Executive Committee/Board members

In all cases, we use appropriate technical and organisational safeguards to prevent your personal data from being accidentally lost, used, or accessed in an unauthorised way. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your information on our instructions in line with Data Protection Legislation.

We may also share your data with other entities in the Arbuthnot Banking Group, for example as part of regular reporting activities or company performance, or in the context of a business reorganisation or group restructuring, for system maintenance and the hosting of data.

Arbuthnot Latham does not transfer your data outside of the UK and European Economic Area; however, we do use third parties who may transfer your data outside of the UK and European Economic Area.

We share your data with third parties, including service providers where required to do so by law and where necessary for administering the employment relationship or where we have a legitimate interest in doing so. We require third parties to respect the security of your data and to treat it in accordance with the law.

Please refer to HR Table 2 (HR Data Storage/Transfer Table) below to see where we store or transfer your data to another organisation.

If we do transfer your information to our service providers, third party suppliers, agents or advisers that transfer your data outside of the UK and EEA, we will take steps to ensure that it is protected in the same way as if it was being used within the UK and EEA. We will use one of the following safeguards:

- There is UK 'adequacy regulations' about the country or territory where the receiver is located or a sector which covers the receiver.
- We have put in place one of the 'appropriate safeguards' referred to in the UK GDPR, such as the IDTA or Binding Corporate Rules. Read more about this on the Information Commissioner's Office website (ICO) – [here](#).
- Where appropriate we carry out a risk assessment and are satisfied that for the data subjects of the transferred data, the relevant protections under UK data protection regime will not be undermined.

If you have any questions, please contact the AL Data Protection Office.

## Fraud Prevention

The personal information we have collected from you will be shared with fraud prevention agencies who will use it to prevent fraud and money laundering and to verify your identity. If fraud is detected, you could be refused certain services, finance, or employment. Further details of how your information will be used by us and these fraud prevention agencies, and your data protection rights can be found on the CIFAS website: <https://www.cifas.org.uk/fpn> or by contacting the HR Department.

## Data Security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, or altered or disclosed. In addition, we limit access to your personal data to those employees, agents, advisers and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place processes to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## Data retention

### **How long do we keep your data?**

Please see HR Table 1 (HR Data Retention Table) below.

### **Retaining records when your employment has ended**

Once an employment relationship has ended, we have less reason to hold on to certain data and so we only retain relevant data. We retain your data following the end of the employment relationship for the following reasons:

- There is a legal obligation or legitimate interest to keep particular records relating to the employee for a specified period of time;
- We want to keep sufficient information to provide a reference relating to the employee to a potential future employer; and
- The data may be important evidence in any legal claim brought by the employee following the end of employment.

## Data portability

The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. This right applies to any data that you have provided to us either with your consent or for the purposes of performing a contract and is processed electronically. Please contact our Data Protection Office for more information.

## Automated decision-making and profiling

Our employment decisions are not based solely on automatic decision-making and profiling.

## What if you do not provide your data?

You have some obligations under your employment contract to provide us with data. In particular, you are required to report absence from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide us with data in order to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details, have to be provided to enable us to enter into a contract of employment with you. If you do not provide other information, this will hinder our ability to administer the rights and obligations arising as a result of the employment relationships efficiently.

## Recording phone calls

We record all external calls made to and from our landline telephones for training, quality control and monitoring purposes and to comply with applicable law. Only specifically designated personnel may listen to call recordings. There must be a justifiable business reason and an auditable record of the activity will be retrained. Mobile phone devices that have either been provided to or used by staff will be installed with a recording system so that calls relating to MiFID II client orders are routed and recorded through it.

## Personal data provided for a specific project

You may agree to provide personal data for a specific project. Examples of personal data that could be provided are film, photographs, videos and/or sound recordings of yourself, although this list is not exhaustive.

Any personal data provided for a specific project is subject to a Employee Release Agreement being signed.

Once the personal data has been provided to the Company, the Company will own the data moving forward.

## Withdrawing consent

Where you have given us consent to process certain data about you, you have the right to request to withdraw your consent at any time by emailing [HRData@arbutnot.co.uk](mailto:HRData@arbutnot.co.uk) or by any other means stated at the time your consent was requested. This does not apply where our reasons for processing your data fall under any of the other grounds for processing outlined in this privacy notice or as otherwise permitted by law.

## Your rights

You have the right in certain circumstances to:

- Access and obtain a copy of your data on request;
- Require us to change incorrect or incomplete data;

- Require us to delete or stop processing your data, for example where the data is no longer necessary for the purposes of processing; and
- Object to the processing of your data where we are relying on its legitimate interests as the legal grounds for processing.

If you would like to exercise any of these rights, please contact the Data Protection Office.

We want to make sure that your personal information is accurate and up to date and you can use our HR system's self-service to update some of your information including:

- Contact details
- Emergency contact details
- Dependent details
- Bank details
- Absence records

You may also object to the processing of your personal data in certain circumstances or request the restriction of processing of personal information about you. Should you wish to receive further information regarding any of these rights, please contact our Data Protection Office.

You will not have to pay a fee to access your data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

## Complaints

Should you have any questions about this privacy notice or how we process your information, please contact our Data Protection Office.

You also have the right to complain to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

The contact details for the Information Commissioner's Office are:

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF

Telephone: 0303 123 1113

Website: [www.ico.org.uk](http://www.ico.org.uk)

We will co-operate fully with the Information Commissioner's Office in the handling of complaints against us.

## Changes to this privacy notice

We reserve the right to update this privacy notice at any time and we will provide you with notice of any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.



HR Table 1 – HR Data Retention Table (\* denotes special category data but special category data may also exist in other listed documentation depending on the content)

Type of data/ employment record	Retention period
(*) Information collated via PeopleCheck from:1. successful candidates obtained during recruitment which is relevant to the ongoing employment relationship and 2. employees when completing annual background checks as required, which may include: <ul style="list-style-type: none"> <li>• Original job applications, copies of qualifications or certificates, skills, references experience and employment history, including start and end dates with previous employers, CVs</li> <li>• Basic disclosures or CRB and DBS certificates</li> <li>• Details of unspent convictions</li> <li>• Background checks summary report</li> <li>• Pre-certification background checks summary report</li> <li>• Financial check searches</li> </ul>	1 year from the date of completion of the checks within the portal and 7 years after employment ends on file
<ul style="list-style-type: none"> <li>• Copies of qualifications or certificates for FCA Specified harm function: Functions Requiring Qualifications.</li> <li>• Self-declaration form and FCA/ PRA Form A</li> <li>• Regulatory References</li> <li>• Fitness &amp; Propriety documentation</li> </ul>	During employment and 7 years after employment ends
(*) CV and job applications for unsuccessful candidates	3 years after notifying candidates of the outcome of the recruitment exercise unless the applicant opts out, but no less than of 6 months after the outcome of your application due to legitimate requirements
(*) Information of successful candidates obtained during recruitment which is relevant to the ongoing employment relationship that are held on S:Drive: <ul style="list-style-type: none"> <li>• CV</li> <li>• Interview notes</li> </ul>	During employment and 7 years after employment ends
(*) Background Screening Risk Assessment Form	1 year from the date it is signed off and uploaded in the portal
(*) Other recruitment records for unsuccessful candidates, including: <ul style="list-style-type: none"> <li>• References</li> <li>• Interview notes</li> <li>• Background screening Risk Assessment Form</li> </ul>	1 year after notifying candidates of the outcome of the recruitment exercise
(*) Immigration checks Identity documents (including passport copies, driving licence copies, NI Number/Form, birth certificates & visas), your nationality and entitlement to work in the UK	During employment and 7 years after employment ends
(*) Personnel records, including: <ul style="list-style-type: none"> <li>• Terms and conditions of employment (including offer letter and employment contract)</li> </ul>	During employment and 7 years after employment ends

<ul style="list-style-type: none"> <li>• Changes to terms and conditions</li> <li>• Name, address and contact details including email address and telephone number</li> <li>• Date of birth</li> <li>• Commencement date</li> <li>• National insurance number</li> <li>• Exit interview questionnaires</li> <li>• Resignation, termination and retirement</li> </ul>	
Emergency contact details	During employment and 3 months after employment ends
Death in service beneficiary details	During employment and 3 months after employment ends
Bank details	During employment and 3 months after employment ends
Private medical insurance data	During employment and 3 months after employment ends
Details of third party employment	During employment and 7 years after employment ends
Working time records, including days of work and working hours	During employment and 7 years after employment ends
Details of absence, including holiday and sickness absence	During employment and 7 years after employment ends
Disciplinary, capability and grievance records	During employment and 7 years after employment ends
Whistleblowing records	7 years from the date the investigation is complete
Assessments, capability and performance details, including <ul style="list-style-type: none"> <li>• (*) Appraisals, performance reviews and ratings</li> <li>• Training records</li> <li>• Performance improvement plans and related correspondence</li> <li>• Other performance data</li> </ul>	During employment and 7 years after employment ends
(*) Sickness and health data	During employment and 7 years after employment ends
(*) Health & Safety data (*) Accident records	During employment and 7 years after employment ends
(*) Statutory maternity/ paternity/ adoption pay / parental leave records, calculations, certificates (Mat B1s) or other medical evidence	During employment and 7 years after except for parental leave records which should be retained until the child is 18 years of age
Subject Access Request	7 years from the closure of the request

Redundancy details	During employment and 7 years from the date of redundancy
Trade union membership	During employment and 7 years after employment ends
(*) Gender and equal opportunities information, including information about your disability, race, age, gender, sexual orientation, religious or philosophical belief, gender reassignment, marital status	During employment and 7 years after employment ends
(*) PAYE, payroll and wage records, including income tax, bonuses, expenses, flexible benefits, Statutory Sick Pay, study funds, student loans	During employment and 7 years after employment ends
Data relating to fraud, including money laundering and economic crime	During employment and 7 years from the incident subject to industry requirements
(*) Pension and retirement benefits	During employment and 7 years after employment ends
Settlement Agreements	7 years from the date of signing or 12 years if is set up as a deed
Personal data provided for a specific project.	Company owns data so duration of project lifetime.

HR Table 2 – HR Data Storage/Transfer Table (\* denotes special category data)

Organisation type	Internal	Background Checks	Financial Check	Fraud protection	Solicitors*	Payroll	Learning Management System	Expenses System	Pension	Salary benchmarking	Other HR consultants	Benefits consultants	Regulatory/government bodies	Health Professionals	Insurance providers and brokers	Other external companies
External organisations and systems	E-file/Email/Teams/S drive/PXD/Arbuthnet	People-Check	Creditsafe/TransUnion via PeopleCheck	Cifas	Employment Immigration Legal advise provider	HR System	Skills Serve	SilExpenses	Pension provider (Hargreaves Lansdown)	McLagan Turning Point HR	Work Buzz H&S advisors	You At Work	FCA PRA ONS LSE NIN HMRC	E.g. GPs	Bupa Life Insurance Provider	Companies performing logistics and delivery services upon our behalf.  Marketing and Branding initiatives.
CV	✓	✓														
Financial Check		✓	✓		✓											
Passport copy or birth certificate or Visa	✓				✓											
Interview notes	✓				✓											
Details of unspent convictions (*)	✓	✓	✓	✓	✓											
Address history, date of	✓	✓	✓	✓	✓	✓			✓			✓	✓	✓	✓	✓

birth, email address, phone number																	
Driving licence	✓							✓									
Background checks summary report	✓	✓			✓												
Background Screening Risk Assessment Form		✓															
Basic disclosures or CRB and DBS certificates (*)	✓	✓	✓	✓	✓												
Employment contract and offer letter	✓				✓												
Death in service beneficiary details	✓								✓							✓	
Gender	✓	✓	✓	✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	
Ethnic origin, sexual orientation or religion or belief (*)	✓												✓				
Disability data (*)	✓				✓									✓	✓		
NI number	✓	✓		✓		✓		✓	✓								
Salary information	✓				✓	✓			✓			✓			✓		
Bank details, pay slips, student loan and other financial information	✓		✓			✓			✓								
Emergency Contact details	✓																
Other current employment data	✓				✓												
Private medical insurance data	✓					✓						✓		✓	✓		
Pension information	✓					✓			✓			✓					
Self-declaration form & FCA/PRA Form A	✓												✓				
Sickness or health data (*)	✓				✓	✓								✓	✓		
Other absences data	✓				✓	✓								✓			
Exit interview questionnaires	✓																
Training records	✓				✓		✓						✓				
Flexible benefits	✓					✓						✓					
Bonus information	✓				✓	✓						✓					
Performance data(*)	✓				✓		✓				✓		✓				
Misconduct data	✓				✓								✓				

Grievances Raised	✓				✓											
Redundancy consultation notes	✓				✓											
Copies of qualifications or certificates	✓	✓			✓											
Study funds	✓															
Changes to contractual terms	✓				✓	✓						✓				
Settlement agreements	✓				✓	✓										
Subject Access Request	✓															
Personal data provided for a specific project	✓															✓

