



ARBUTHNOT LATHAM  
*Private Bankers*  
 Since 1833

# Recruitment Privacy Notice & Consent Form

## 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 recruitment process.

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, overseas branches, and its parent company. These include Arbuthnot Banking Group PLC, Arbuthnot Commercial Asset Based Lending Limited, Arbuthnot Specialist Finance 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 House, 7 Wilson Street, London EC2M 2SN
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 collect a range of information about you. This includes:

- Your name, address and contact details, including email address and telephone number;
- Details of your qualifications, skills, experience and employment history;
- Information about your current level of remunerations, including benefit entitlements; and
- Information about your eligibility to work in the UK.

We may collect this from a number of sources, including interview notes, Eploy (Applicant Tracking System) registration form, application form, CV, LinkedIn, job boards and any other correspondence and documents generated during the recruitment process.

Please refer to the HR Data Retention Table (HR Table 1) which explains how long we will hold your personal data.

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

We will collect your personal data to consider and process your application for employment as part of our recruitment and selection procedure. Your data may also be used for background vetting procedures.

In some cases, we will need to process your data to comply with legal obligations. For example, it is required to check a successful applicant's eligibility to work in the UK before employment starts.

We also have a legitimate interest to process and keep records of your personal data during the recruitment process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom to offer a job. We may also need to process data from job applicants to respond to and defend against legal claims.

## How we use your personal data

We use the following data collected about you during the recruitment and on-boarding process for the following purposes. This includes any special categories of more sensitive personal data denoted by (\*) below.

### **(a) Disability or health related information (\*)**

We ask whether you have a disability for which we need to make reasonable adjustments during the recruitment process.

Information you provide about any disability or medical condition will remain confidential unless it is necessary to disclose it to other members of staff or outside agencies to ensure the health and safety of yourself and others, or to implement the adjustments you require. In these circumstances, we will first discuss with you how and to whom the information may be disclosed.

### **(b) Background checks**

We believe it is our duty to ensure the highest standards of honesty and integrity. As a result, it is our policy to undertake appropriate background screening checks upon offer of employment. PeopleCheck, a background vetting Company, will conduct these checks on our behalf. Any information you provide on your application and during the recruitment process must be honest, accurate and not misleading. In the event that a discrepancy is discovered during the conduct of the background checks, an applicant may be given the opportunity to provide an explanation and will not necessarily be a bar to employment with us.

The checks include but are not limited to:

- ✓ Address confirmation/electoral roll checks.
- ✓ Address history checks.
- ✓ Alias check.
- ✓ Identity verification/passport validation/right to work check.
- ✓ Financial search including credit check, county court judgments, insolvencies and bankruptcy orders.
- ✓ Directorships search for any company listings or conflicts of interest.
- ✓ Checks with global sanctions, Office of Foreign Assets Control (OFAC) checks, law enforcement actions, black, watch and PEP (politically exposed persons) lists for involvement in/association with fraud, money laundering, or the funding of terror, drugs and related illegal activities.(\*)

- ✓ FCA registry check.
- ✓ Press analysis on a local, regional and international level for anything published about their professional or personal background that may be of concern or interest.
- ✓ Verification of professional qualifications.
- ✓ Employment verification - six years with references, with an explanation of gaps greater than three months.
- ✓ Educational verification to most appropriate level – normally highest level achieved.
- ✓ Standard DBS check. (\*)
- ✓ CIFAS check.

Additional checks may be carried out for some more senior, regulated or sensitive roles and these additional checks may include:

- ✓ FCA/PRA Form A (application to perform controlled functions under the approved persons regime).
- ✓ Regulatory References.
- ✓ Directorships.
- ✓ Declaration Form including confirmation of Statement of Professional Standing (if appropriate).
- ✓ Certificate from current employer to confirm Fitness and Propriety.
- ✓ Evidence of CPD.
- ✓ Copies of required qualifications.
- ✓ Mandatory paperwork returned and complete.

***Criminal convictions and pending proceedings (\*)***

In the event of a successful application, we will run a basic Disclosure & Barring Service check (DBS). We process this data in order to monitor and maintain the honesty and integrity of our workforce. Roles falling under the Senior Managers Certification Regime (SMCR) will be required to undertake a standard DBS check.

***Credit reference search***

We process this data in order to maintain trust for clients within the workforce and to minimise the risk of financial crime. We will ask your consent to conduct a credit reference search via Equifax Limited on behalf of Arbuthnot Latham. The data generated will be assessed by authorised personnel only and the application will be accepted or declined accordingly. Details of County Court judgements and bankruptcies are also searched. The information is available only for our own in-house purposes, therefore cannot be shared with the applicant.

***Fraud prevention (\*)***

The personal information we have collected from you will be shared with Cifas who will use it to prevent fraud, orther unlawful or dishonest conduct, malpractice and other seriously improper conduct. If any of these are detected you could be refused certain services or employment. Your personal information will also be used to verify your identity. Further details of how your information will be used by us and Cifas and your data protection rights can be found on the CIFAS website: <https://www.cifas.org.uk/fpn> or by contacting the HR Department.

***Equal opportunities monitoring (\*)***

We ask you for and use certain equal opportunities information (for example, as to your ethnic origin, sexual orientation, religion and disability status) for the purpose of ensuring meaningful and equal opportunities monitoring and reporting.

In line with the above, all offers of employment made by Arbutnot Latham are expressly conditional upon a satisfactory background check being completed in relation to each applicant.

If you fail to provide certain information we may not be able to take your application for employment forward.

## Legal basis for processing

At the recruitment stage we process the above personal information about you for the purpose of assessing your skills, qualifications and suitability for the role, to communicate with you about the recruitment process, and to comply with legal or regulatory requirements (for example, background and reference checks). We also need to process your personal information to decide whether to enter into a contract of employment with you. We will also process personal data to serve our legitimate interests as explained in the **Why do we collect and process your personal data** section of this notice.

This may overlap with any instances where we are processing your information to comply with legal obligations, such as those under the Equality Act 2010, to comply with health and safety legislation or FCA requirements, or where this is necessary to perform a contract entered into with you, or to allow equal opportunities monitoring in the public interest.

Less commonly, we may process your 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 may retain personal information for unsuccessful candidates for legitimate reasons as described below.

We may also request your consent for any processing activities that are not covered by the above lawful bases. This includes where we would like to retain some of your information to tell you about future employment opportunities.

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

Your data will be stored in the following systems:

- Eploy (The Applicant Tracking System), accessed only by authorised and relevant personnel such as the HR team, hiring managers or auditors.
- Internal servers, accessed only by the HR team for the purposes outlined above or relevant recruiting managers, or auditors.
- Third party platforms, as listed above for the purpose of background checking.

In all cases, we take all appropriate steps to ensure documents are stored securely and access is restricted only to employees with a legitimate purpose in line with UK data protection law.

In a limited number of cases, your personal data may be transferred to other third parties (for example, immigration solicitors).

We do not transfer your data outside of the European Economic Area, with the exception of data for our staff based in our branch in Dubai. Third parties (including PeopleCheck) may transfer your data outside of the European Economic Area.

If we do transfer information to our agents or advisers outside the EEA, we will make sure it is protected in the same way as if it was being used within the EEA. We will use one of these safeguards:

- Transfer it to a non-EEA country with privacy laws that give the same protection as the EEA.
- Put in place a contract with the recipient that means they must protect it to the same standards as the EEA. Read more about this on the European Commission Justice website.
- Transfer it to organisations that are part of Privacy Shield. This is a framework that sets privacy standards for data sent between the US and EU countries. It makes sure those standards are similar to those used within the EEA.

You can find out more about data protection on the [European Commission Justice website \(https://ec.europa.eu/info/law/law-topic/data-protection\\_en\)](https://ec.europa.eu/info/law/law-topic/data-protection_en).

## How long will we store your data?

### Successful applicants

In the event that your application for employment is successful, this data may also be retained and processed for the purpose of the on-going employment relationship in line with our HR Privacy Notice, a copy of which will be provided to you at the on-boarding stage if you are selected.

### Unsuccessful applicants

If your application is unsuccessful, we may keep your personal data on file in case there are future employment opportunities for which you may be suited. We will ask for your consent before we retain your data for this purpose and you are free to withdraw your consent at any time. If you consent to your CV being retained by us, we will ask for your consent on a regular basis (annual basis) to retain your CV for talent pooling purposes and to inform you of future opportunities.

We retain relevant data for unsuccessful applicants for a legitimate interest, namely establishing that due process has been followed and recording any decisions taken and reasons for those decisions for an appropriate period (see HR Table 1 below) and also for the purpose of defending any legal claims.

## 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 recruitment processes are not based solely on automated decision-making and profiling.

## What if you do not provide your data?

You are under no statutory or contractual obligation to provide data to us during the recruitment process. However, if you do not provide the information, we may not be able to process your application properly or at all.

## 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 retained.

## 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

As a data subject, you have the right on certain circumstances to:

- Access and obtain a copy of your data on request;
- Require the organisation to change incorrect or incomplete data;
- Require the organisation 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 the organisation is relying on its legitimate interests as the legal ground 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 the self-service system on Eploy (the applicant tracking system) to update your basic contact information and job alert preferences. 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 further information regarding any of these rights, please contact our Data Protection Office.

## 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
Credit history reference searches	Not retained past the point of recruitment
(*) Information in respect of successful candidates obtained during recruitment which is relevant to the ongoing employment relationship, including: <ul style="list-style-type: none"> <li>• Original job applications, interview notes, 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> </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
(*) Other recruitment records for unsuccessful candidates, including: <ul style="list-style-type: none"> <li>• References</li> <li>• Interview notes</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 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> <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>• Self-declaration form and FCA/ PRA Form A</li> <li>• Exit interview questionnaires</li> <li>• Death in service beneficiary details</li> <li>• Resignation, termination and retirement</li> </ul>	During employment and 7 years after employment ends



Emergency contact details	During employment and 6 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
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
(*) Private medical insurance data	Duration of the policy plus the applicable period for any run off arrangements and coverage of insured risks
(*) 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
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	During employment and 7 years from the incident subject to industry requirements
(*) Pension and retirement benefits	During employment and 7 years after employment ends (we will not retain any certificate of birth provided to us but will retain a record of the date of birth).
(*) Bank details	During employment and then deleted as soon as practicable after the employment ends and the final salary payment has been made
Settlement Agreements	7 years from the date of signing or 12 years where signed as a deed
Accident records	During employment and 7 years after employment ends (at least years from the date the accident report was made)

# Document Change Record

Date	Version	Updated By	Change Details
May 2018	1	HR Team	<ul style="list-style-type: none"> <li>Recruitment Privacy Notice issued in line with GDPR</li> </ul>
October 2019	2	Saisha Uddin, HR Advisor	<ul style="list-style-type: none"> <li>Added Arbuthnot Specialist Finance Limited</li> <li>Under recording phone calls, included a justifiable business reason to retain recordings</li> <li>Removed reference to Recruitment Retention Table and changed to HR Data Retention Table</li> <li>HR Data retention table updated to align with changes to the HR Privacy notice</li> <li>Included a document change record</li> <li>Removed historic Internal Fraud Database wording and included new wording under fraud prevention</li> </ul>