

The Access Bank UK Ltd - Privacy Statement

This Privacy Statement explains how The Access Bank UK Ltd obtains, uses and keeps your personal information confidential.

The Access Bank UK Ltd may act as the 'data controller' and/or 'processor' of the personal information you provide to us, for purposes of the UK General Data Protection Regulation (UK GDPR). Our company registration number is 06365062 and the registered address is 4 Royal Court, Gadbrook Way, Gadbrook Park, Northwich, Cheshire CW9 7UT.

If you have any questions about our Privacy Statement, you can write to: The Data Protection Officer, The Access Bank UK Ltd, 4 Royal Court, Gadbrook Way, Gadbrook Park, Northwich, Cheshire CW9 7UT.

How we use your personal information

In order to provide you with products and services we need to collect, use, store and share personal information about you. This includes information which we:

- Obtain when you provide it to us (e.g., where you contact us via email or telephone, or by any other medium).
- Obtain from you or from third parties, such as employers, joint account holders, credit reference agencies, fraud prevention agencies or other organisations, when you apply for an account or any other product or service, or which you or they give to us at any other time; or
- Collect in the ordinary course of your relationship with us. For example, we learn from the way you use and manage your account(s), from the transactions you make such as the date, amount, currency and the name and type of supplier (e.g. supermarket services, medical services, retail services) and from the payments which are made to your account.
- Obtain when you visit any of our internet sites (such as IP address, device type, operating system, browser type, browser settings, language settings, dates and times of connecting to a site and other technical communications information), some of which may constitute personal information.

Why we use your personal information

We will use your information to manage your account(s), send you account statements and provide our services, for assessment and analysis (including credit and/or behaviour scoring, market and product analysis), to prevent and detect fraud, money laundering and other crime, carry out regulatory checks and meet our obligations to any relevant regulatory authority, and to develop and improve our services to you and other customers and protect our interests.

Personal information and the law

We can only use your personal information if we have a proper reason to do so. This includes sharing it outside of The Access Bank UK Ltd. The law stipulates we must have one or more of the following legal reasons:

- To fulfil a **contract** that we hold with you, or a contract you are applying to enter into; or
- When we have a **legal or regulatory obligation**, or
- When it is for **legitimate reasons**, or
- When you **consent** to it.

A legitimate reason occurs when we have a business or commercial reason to use your information. But even then, it must not unfairly go against what is right and best for you. If we rely on legitimate reasons we will tell you what that is.

The table below lists all the ways that we may use your personal information, and the legitimate and legal reasons for doing so.

How we use your personal information	Our legitimate reasons
<p>In order to manage our relationship with you</p> <p>In developing ways to meet the requirements of our customers and to grow our business.</p> <p>In assessing how customers use our products and services.</p> <p>In providing information about our products and services.</p>	<p>Keeping our records up to date.</p> <p>Developing products and services, and what we charge for them.</p> <p>Defining types of customers for new products or services.</p> <p>Fulfilling our legal and regulatory obligations.</p>
<p><u>Our Legal Reasons</u></p> <ul style="list-style-type: none"> • Your Consent (this applies to any information that we request which is optional, and where this applies we will make this clear when we make the request) • Meeting contractual requirements • Our legitimate reasons • Due to our legal and regulatory obligations 	
<p>In order to develop our business and the products and services that we offer.</p> <p>In assessing new products.</p> <p>In respect of other companies that provide services to us and our customers.</p>	<p>Developing products and services, and our charging structure</p> <p>Determining the market for our new products or services.</p> <p>Fulfilling our legal and contractual obligations.</p>
<p><u>Our Legal Reasons</u></p> <ul style="list-style-type: none"> • Meeting contractual requirements • Our legitimate reasons • Due to our legal and regulatory obligations 	
<p>In respect of the delivery of the full range of products and services that we offer.</p>	<p>Complying with regulations that apply to us.</p>

<p>In the process of performing transactions for our customers.</p> <p>In the course of the application of fees and charges and interest to customer accounts, where applicable</p> <p>In the course of collection and recovery of monies owed by customers to the Bank</p>	<p>Fulfilling our legal and contractual obligations.</p>
<p><u>Our Legal Reasons</u></p> <ul style="list-style-type: none"> • Meeting contractual requirements • Our legitimate reasons • Due to our legal and regulatory obligations 	
<p>In respect of the work that we undertake to protect the Bank from financial crime and terrorism financing, and effectively assess and mitigate risk to our bank and our customers.</p> <p>In the course of meeting all regulatory requirements.</p> <p>In the complaints handling process.</p>	<p>Meeting our legal and regulatory obligations to ensure that we have, and continue to develop, our systems and controls to combat financial crime and terrorism financing.</p> <p>Complying with regulations</p> <p>Fulfilling our legal and contractual obligations.</p>
<p><u>Our Legal Reasons</u></p> <ul style="list-style-type: none"> • Meeting contractual requirements • Our legitimate reasons • Due to our legal and regulatory obligations 	
<p>In the course of managing all aspects of our business including corporate governance and audit processes.</p>	<p>Complying with regulations.</p> <p>Fulfilling our legal and contractual obligations.</p>
<p><u>Our Legal Reasons</u></p> <ul style="list-style-type: none"> • Meeting contractual requirements • Our legitimate reasons • Due to our legal and regulatory obligations 	
<p>In respect of our rights and obligations in agreements or contracts that we hold.</p>	<p>Fulfilling contractual obligations.</p>
<p><u>Our Legal Reasons</u></p> <p>Meeting contractual requirements</p>	

Categories of personal information

The personal information that we obtain and process fits into a number of different categories.

Category of personal information	Description
Financial and Transactional	The financial information that we hold for you as a customer of the Bank, including your financial position and status, and details about transactional activity on the accounts that you hold with us.
Core personal information including social relationships	This refers to information that we hold in respect of your address and contact information, national identifiers such as National Insurance and Tax identification numbers, and also includes information relating to your family and associates.
Demographic, educational and employment information	This refers to information that we hold in respect of your profession, nationality and education.
Usage and contractual information	This information relates to the way in which you use our products and services that we provide to you.
Location and technical information	Information that we obtain about your location, for example in respect of your usage of our website through your internet connection and the technology that you use.
Communications	The information you provide to us in any medium, for example your communications by telephone, letter and email, noting that we record telephone calls to confirm details of our conversations, for your protection and in order to identify and address staff training needs.
Information in the public domain	Information about you that is available in the public domain from all available sources including the internet.
Documentary information	Information about you in documents such as your Passport, Driving licence or utility bills that you provide to us, whether original or copy documents.
Consents	Any permissions, consents, or preferences that you provide to us.

Sources of personal information

- We collect personal information about you from a range of sources explained in this section:

Information that you provide

- In respect of our products and services
- In the course of your communications with us
- When using our website and online banking system
- In meetings with your Relationship Manager

Information we collect

- Payment and transactional information.
- Data we obtain from the way in which you use our online banking and telephone banking services. For example, your personal profile and how you identify yourself when you connect to these services and other information about how you use these services. We use cookies to collect this type of information from devices you use to connect to our services, such as computers.

Information and third parties:

We may obtain information about you from third parties, these include:

- Employers
- Credit reference agencies (who may search the Electoral Register)
- Fraud prevention agencies or other organisations, when you apply for an account or any other product or service, or which you or they give to us at any other time;
- Introducers
- Land agents
- Public information sources e.g. Companies House, Her Majesty's Land Registry
- Government and law enforcement agencies.

We may provide information about you or share your personal information with third parties, for legitimate business reasons, in accordance with applicable law. This may include disclosing your personal information to:

- You, and where appropriate, your family, your associates and your representatives
- HM Revenue & Customs
- Our regulators and other competent authorities
- Statutory bodies such as Financial Services Compensation Scheme (FSCS) – scheme applies in the UK
- Credit reference agencies
- Fraud and crime prevention agencies
- Introducers who have introduced you to us
- Companies or individuals that you ask us to share your personal information with
- The Direct Debit scheme, if you authorise direct debits on your account with us
- Other lenders who also hold a charge on your property where you have a loan or mortgage with us secured on the same property
- Any third party to whom we transfer or may transfer our rights and obligations as a result of any restructure, sale or acquisition of any company, provided that your

information is used for the same purposes as it was originally supplied to us and/or used by us.

- Account information service providers or payment initiation service providers that you have authorised.
- We may also give out information about you if we have a duty to do so, for example, to any relevant party for the purposes of prevention, investigation, detection or prosecution of financial crime or if the law allows us to do so.

We will only conduct information sharing activity with a third party if they agree to keep your information safe and confidential.

Joint accounts

If you have a joint account, or you have authorised another person to operate your account, we may disclose to any of you any information we hold about the account.

Transfer of personal information overseas

If we transfer your personal information to a person, office, branch or organisation located outside of the UK or the EEA, we will make sure that they agree to apply the same levels of protection in line with applicable legal requirements, and to use your information strictly in accordance with our instructions.

We would only share your personal information outside of the UK or the EEA if:

- You have explicitly consented to the transfer;
- The transfer is necessary for the performance of a contract between you and the Bank or in order to enter into a contract at your request;
- In order to comply with a legal duty;
- To protect the vital interest of you, or another, where you are physically or legally incapable of providing consent;
- To adhere to a European Commission adequacy decision that the country outside of the EEA ensures an adequate level of information protection;

If we do transfer your personal information to a person, office, branch or organisation outside of UK or EEA, we will ensure that it is protected in line with the applicable legal requirements by using one of the following safeguards:

- Transfer it to a country which has privacy laws that give the equivalent required protection.
- Ensure there is a legally binding contract between the Bank and the recipient of the personal information requiring the same level of protection of your information.

Fraud Prevention Agencies (FPA's) also send your personal information to countries outside the UK or EEA. Where they do so, they will ensure there is a legally binding contract in place to make sure the recipient protects the information to the same standard required under applicable legal requirements.

Automated decisions and personal information

The Bank does not use your personal information to conduct automatic 'profiling' decisions. However, we do use third party organisations who use automated 'decision' making in relation to identification checks only, as part of the account opening process. You have the right to object to an automated 'decision', and ask that a person reviews it.

Some of the personal information we hold – or are allowed to obtain from others – about you may be used to assist us in our decision making process. For example:

Account opening

The Bank will use the information you have provided to ensure that the product or service is relevant and that meets the conditions needed to open the account.

Identifying fraudulent activity

The Bank has in place systems and controls to prevent fraud, money laundering and terrorism financing, and we may use your personal information to decide if your account is being used for these purposes. If we think the account is being used to facilitate such offences we may block the account and refuse access to it.

Credit Reference Agencies (CRAs)

We may use Credit Reference Agencies (CRAs) for prospective and existing customers of the Bank. We conduct identity checks when you apply for a product or services for you or your business. Where we are unable to verify your identity by this means, we will ask you to provide physical forms of identification and may contact you in this respect.

We may share your personal information with CRAs and they may provide us with information about you, including:

- Personal details including name, address and date of birth
- Credit status
- Details of credit you may hold with a joint account holder
- Financial information and history
- Information sourced from the public domain such as the electoral register and Companies House.

Such information may be used for the following purposes:

- Check details on applications and meet our regulatory requirements to fully identify our customers;
- For the prevention of fraud, financial crime and counter terrorism offences;
- Recovery of debts owed to the Bank;
- Check details of job applicants and employees;

Information held about you by a CRA may already be linked to records relating to your partner or members of your household where a financial 'association' has been created. Any enquiry we make at a CRA may be assessed with reference to any 'associated' records. Another person's record will be 'associated' with yours when:

- You make a joint application;
- You advise us of a financial association with another person;

- The CRA have existing, linked or 'associated' records. This 'association' will be taken into account in all future applications by either or both of you and shall continue until one of you applies to the CRA and is successful in filing a 'disassociation'.

The Credit Reference Agency which provides services to the Bank is Equifax, and further information can be found at the following location: <https://www.equifax.co.uk/crain>

Fraud Prevention Agencies (FPAs)

We may also process your personal information in accordance with applicable law, and share it with Fraud Prevention Agencies (FPA's), as required, to help detect fraud, financial crime and counter terrorism offences. This will include information such as:

- Personal information and documentation that you provide to us, such as your name and date of birth and images of Passports, Driving licences and signatures, Tax identification numbers, copies of utility bills and other documents, your residential address including address history, and your contact details including email address and telephone number
- Information obtained from the public domain or third parties that we work with.
- Financial information
- Information relating to your products or services
- Employment details
- Information which identifies your computer/ device used to connect to the internet, for example Internet Protocol (IP) address.

Any sharing of such personal information with an FPA will only occur if we have a proper reason to do so. We or an FPA may allow law enforcement agencies access to personal information provided if it is for a legal duty or a legitimate reason, as defined below, and such information may be retained for up to 6 years.

Legal duty:

- Where a law enforcement agency requires access to and use of this personal information subject to the appropriate legal safeguards and regulatory requirements;
- If false or inaccurate information is provided or fraud is suspected, we may pass details to FPA's.

Legitimate reason:

- To confirm your identity
- To fulfil any contracts that you hold with us.

If you choose not to give personal information

As already stated in this notice, we may collect personal information on several bases including with your consent, for our legitimate reasons, due to legal or regulatory obligations, or under the terms of a contract we have with you. If you choose not to provide us personal information, it may delay or prevent us from meeting our obligations. It may also mean that we cannot perform services needed to run your accounts. It may also result in the cancellation of a product or service you hold with us.

Should any information collection be considered optional, we would specify this clearly from the outset.

Records and retention of personal information

The Bank will store all personal information as securely as possible, in a confidential manner.

We will only retain your personal information for as long as you are a customer of The Access Bank UK Ltd or otherwise for a limited period of time as long as necessary to fulfil the purposes for which we have initially collected it, unless otherwise required for legal, regulatory or fraud prevention purposes.

After account closure, or if your application has been declined or not progressed for any reason, we may retain information about you for up to 10 years where necessary for one of the following reasons:

- To respond to any information requests or complaints.
- To maintain records according to regulations or legal requirements that apply to us.

We may keep your information for longer than 10 years if we are prevented from deleting it for the above mentioned legal, regulatory and fraud prevention reasons.

If we have not contacted you during this retention period, we will delete your personal information at the end of this period.

Your rights regarding your personal information

The right of access to your information that we hold:

Under the UK General Data Protection Regulation (UK GDPR) you have a right to see a copy of the information we hold on you. You can ask for a copy of this information by making a Subject Access Request (SAR) to us. This request can be made by email to info@theaccessbankukltd.co.uk or in writing to:

Data Protection Officer
The Access Bank UK Ltd
4 Royal Court
Gadbrook Way
Gadbrook Park
Northwich
Cheshire
CW9 7UT

Should you make such a request, the Bank will supply you with this information within one month of the request (extended for a further two months for complex/numerous requests in which case we will advise you of the extension within the one month period). We may charge you an administration fee (based on the administrative costs of providing the information) for this service, or refuse to respond, where a request is 'manifestly unfounded or excessive'. If we refuse to respond, we will explain to you the reason why the request has been refused and inform you of your right to complain, within one month of the receipt of the request.

In cases where large amounts of personal information are processed by us about you, it is permissible under UK GDPR for us to ask you to specify the information to which the request relates.

Further information regarding making a SAR can be obtained from the Information Commissioners Office (ICO) on 0303 123 1113 if you are calling within the UK. If you are calling from outside the UK please call +44 1625 545 700.

The right to rectify inaccurate information:

If any information we hold for you is incorrect, you may request us to rectify this at any time by contacting us by email, telephone or in writing to the Data Protection Officer at the above address. Taking into account the purposes of the processing, you have the right to have incomplete personal information completed, including by means of providing a supplementary statement.

If we have disclosed such personal information to a third party we will inform them of the rectification where possible and inform you of the third parties to whom the inaccurate or incomplete information has been disclosed, where appropriate.

The right to restrict or object to the processing of information:

You may ask us to restrict the processing of your personal information at any time, or you may object to our continued use of your information by contacting us by email, telephone or in writing to the Data Protection Officer at the above address. You may do this in the following circumstances:

- Where you contest the accuracy of the personal information, we must restrict the processing until we have verified the accuracy of the personal information.
- Where you have objected to the processing (where it was necessary for the performance of a public interest task or a purpose in our legitimate interests), and we are considering whether our legitimate interests override your own interests.
- Where processing is unlawful and you oppose erasure and request restriction of processing instead.
- Where we no longer need the personal information but you require the information to establish, exercise or defend a legal claim.

This does not affect any processing that has been carried out prior to your request being received. If you have requested or objected to processing of your personal information, this does not prevent us continuing to store the information.

Where we have disclosed personal information we hold about you to a third party we will inform the third party of any restriction on the processing of that personal information.

We will inform you when we decide to lift a restriction on processing of personal information we hold about you.

The right to information portability:

You may ask us to move, copy or transfer your personal information directly to another organisation if this is technically feasible to do so in a safe and secure way. You can request this by contacting us by email, telephone or in writing to the Data Protection Officer at the above address.

The right to have your information erased:

Also known as the 'right to be forgotten' this allows you to request that we delete any or all personal information that we hold about you where there is no compelling reason for its continued processing, for one of the following reasons:

- Where the personal information is no longer necessary in relation to the purpose it was originally collected/processed;
- Where you withdraw consent;
- Where you object to processing and there is no overriding legitimate interest for continuing to process the information;
- Where the personal information was unlawfully processed (e.g. otherwise in breach of UK GDPR);
- Where the personal information has to be erased to comply with a legal obligation; or
- Where the personal information is processed in relation to the offer of information society services to a child

You make this request at any time by contacting us by email, telephone or in writing to the Data Protection Officer at the above address.

We can refuse to erase personal information we hold about you where it is processed for the following reasons:

- To exercise the right of freedom of expression and information.
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority.
- For public health purposes in the public interest.
- Archiving purposes in the public interest, scientific research, historical research or statistical purposes.
- The exercise or defence of legal claims.

If we erase personal information we hold about you, we will inform any third parties about the erasure unless it is impossible or involves disproportionate effort to do so.

The right to withdraw your consent:

You may withdraw your consent at any time. This will not affect any usage of your information carried out up until that point but would have immediate effect from when we receive your request. Please contact us by phone, email or in writing to address above if you wish to do so.

If you withdraw your consent, we may not be able to provide certain products or services to you. If this is so, we will tell you.

Marketing

The Bank has made a policy decision that we will not send unsolicited marketing material to you.

If you wish to make a complaint

If for any reason you are unhappy with our use of your personal information and you wish to lodge a complaint, please contact us by email, telephone or in writing to the Data Protection Officer at the above address.

You also have the right to complain to the Information Commissioner's Office. You can find out how to do this on their website: <https://ico.org.uk/concerns/handling/>

Cookies

Information about how we use Cookies is provided on the Bank's website at the following location: <https://www.theaccessbankukltd.co.uk/cookies/>