# PRIVACY NOTICE

## How your Personal Information is used by Brown Shipley

We are committed to protecting and respecting your privacy.

This privacy notice is to let you understand how we look after and process your personal information, including what you tell us about yourself and what we learn about you as a visitor to our website, as a prospective client or as a client, or as an employee, shareholder or agent of a corporate client of Brown Shipley. This notice explains how we do this and tells you about your privacy rights and how the law protects you.

Your information will be held by Brown Shipley which is a wholly owned subsidiary of KBL European Private Bankers S.A. ("KBL") based in Luxembourg. As such, Brown Shipley is part of the KBL group and is the UK member of the KBL group of companies ("Group").

For the purpose of the General Data Protection Regulation 2016 ("GDPR") and the Data Protection Act 2018 ("DPA"), the data controller is Brown Shipley & Co Limited (company number 00398426) of Founders Court, Lothbury, London EC2R 7HE.

### 1. What GDPR & DPA mean to you

In addition to our commitment to protect and respect your privacy as detailed in this Privacy Notice, it is also protected by law. The GDPR and DPA state that we are only allowed to use personal information if we have a proper and lawful reason to do so; the following reasons are the main ones upon which we base our processing:

- To fulfil a contractual agreement with you, or take necessary steps before entering into a contractual agreement with you e.g. to carry out an initial risk profile and needs assessment, provide investment advice to you, manage your investments, execute your instructions, make and manage payments due to you, administer loans and mortgages, deliver other services, manage fees, interest and charges on your accounts or exercise rights set out in contractual agreements. Please note that if you do not agree to provide us with requested information, it may not be possible for us to continue to operate your account and/or provide products or services to you.
- When we or a third party have a legitimate interest, such as a business or commercial reason where it is necessary to use your information. It is in our interests to ensure that our processes and systems operate effectively and that we can continue operating; make our services more efficient; create new products and services or carry out fraud prevention activities.

  Calls to our offices, emails, text messages or other communications may be recorded and monitored to check your instructions to us; to analyse, assess and improve our services to our clients; for training and quality purposes; for preventing or detecting crime (including fraud); to help us investigate any complaint you may make and as evidence in any dispute or anticipated dispute between you and us.

This may include processing your information to:

a. monitor, maintain and improve internal business processes, information and data, technology and communications solutions and services;

b. ensure business continuity and disaster recovery and responding to information technology and business incidents and emergencies;

c. ensure network and information security, including monitoring authorised users' access to our information technology for the purpose of preventing cyber-attacks, unauthorised use of our telecommunications systems and websites, prevention or detection of crime and protection of your personal data;

d. provide assurance on the bank's material risks and reporting to internal management and supervisory authorities on whether the bank is managing them effectively;

e. perform general, financial and regulatory accounting and reporting;

f. protect our legal rights and interests;

g. manage and monitor our properties (for example through CCTV) for the purpose of crime prevention and prosecution of offenders, for identifying accidents and incidents and emergency situations and for internal training;

h. enable a sale, reorganisation, transfer or other transaction relating to our business and

i. send you relevant marketing information (including details of other products or services provided by us or other Group companies which we believe may be of interest to you);

j. to invite you to events.

- When it is our legal duty to process your data to comply with the law e.g.

a. to confirm your identity, including using biometric information, for example fingerprint verification, iris and face recognition technology, where we do so with your explicit consent;

b. undertake money-laundering checks, provide information to HMRC and regulators such as the Financial Conduct Authority;

c. share data with police, law enforcement, tax authorities or other government and fraud prevention agencies where we have a legal obligation, including reporting suspicious activity and complying with production and court orders;

d. perform checks and monitor transactions for the purpose of preventing and detecting crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption and international sanctions. This may require us to process information about criminal convictions and offences, to investigate and gather intelligence on suspected financial crimes, fraud and threats and to share data with law enforcement and regulatory bodies;

e. deliver mandatory communications to clients or communicating updates to product and service terms and conditions;

f. assess affordability and suitability of credit for initial credit applications and throughout the duration of the relationship, including analysing client credit data for regulatory reporting

g. investigate and resolve complaints;

h. conduct investigations into breaches of conduct and corporate policies by our employees;

i. manage contentious regulatory matters, investigations and litigation;

j. perform assessments and analyse client data for the purposes of managing, improving and fixing data quality;

k. provide assurance that the bank has effective processes to identify, manage, monitor and report the risks it is or might be exposed to;

l. investigate and report on incidents or emergencies on the bank's properties and premises;

m. coordinate responses to business disrupting incidents and to ensure facilities, systems and people are available to continue providing services; and

n. monitor dealings to prevent market abuse.

- When you give consent to us to process your data for one or more specific purposes e.g. to send you certain marketing materials.

At every stage during our relationship with you, at least one of the above reasons will be applicable to each way in which we use your personal information. The overarching purpose of processing your information is to enable us to manage our relationship with you so as to provide advice and guidance tailored to your circumstances.

Where we are processing any special categories of personal information, that is information revealing racial or ethnic origin, political, religious or philosophical beliefs, trade union memberships, genetic data, biometric data used to uniquely identify you, or information about your health, sex life or sexual orientation, we also need a further lawful reason upon which to base our processing. The following reasons are the main ones upon which we rely to process special categories of information:

- When you give us explicit consent to process your data for one or more specific purposes e.g. to consider certain health conditions or needs when carrying out wealth planning.
- Where you have made the information public e.g. if you have been profiled in a newspaper or magazine.
- Where it is necessary for us to establish, exercise or defend legal claims.
- For reasons of substantial public interest e.g. carrying out fraud prevention activities or obtaining insurance cover for you.

Where we are processing any information that discloses your criminal convictions or offences, e.g. in order for us to perform checks to prevent and detect crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption and international sanctions, the main lawful reasons upon which are relied on for this processing are:

- Preventing or detecting unlawful acts
- Complying with our regulatory requirements in relation to unlawful acts or dishonesty
- Dealing with suspicions of terrorist financing or money laundering
- Where it is necessary for us to obtain legal advice or establish, exercise or defend legal rights

It may involve investigating and gathering intelligence on suspected financial crimes, fraud and threats and sharing data between banks and with law enforcement and regulatory bodies.

We have in place administrative, technical and physical measures on our website and internally designed to guard against and minimise the risk of loss, misuse or unauthorised processing or disclosure of the personal information that we hold.

## 2. Types of Personal Information

We use many different types of personal information as detailed in the table below:-

| Type of Personal Information | Description |
|---|---|
| Contact | Your name, address, email address, telephone numbers and any other contact details. |
| Financial | Your financial position, status and history and possibly also financial information regarding your business or family members. |
| Transactional | Details about your investments, pensions, loans and any payments to and from your accounts with us. |
| Communications | Information that we learn about you from letters, emails and conversations between us. |
| Contractual | Information we learn about you in order to provide our products or services to you and details regarding the actual products and services that we provide to you. |
| Social Relationships | Your family, friends, business associates and other relationships. |
| Socio-demographic | This includes details about your age, gender, where you work or your profession, your nationality, ethnicity, education levels and where you fit into income and social-economic groupings. |
| Locational | Information that we obtain about your physical location which may come from your mobile phone, the address where you connect a computer or mobile device to the internet, or where you have bought something using your Brown Shipley Visa card. |
| National identifier | The number or code given to you by a government entity to identify who you are such as your National Insurance Number. |
| Open Data and Public Records | Information about you that is available in public records such as the Electoral Register or Companies House and other information about you that is openly available on the internet. |
| Special categories of data | The law treats some types of personal data as being special and we only collect and use these types of data if the law allows us to do so. Special categories of data that we may process include:-<br>• Racial or ethnic origin<br>• Sexual orientation (for example if you provide details of your marital status or dependents)<br>• Religious, philosophical or political beliefs (for example if you are considered a Politically Exposed Person or your beliefs can be identified from your occupation)<br>• Trade union membership (for example if this can be identified from your occupation<br>• Health data (for example for wealth planning services or insurance products or pension provision)<br>• Criminal convictions and offences (for example if you are subject to sanctions or included on fraud databases)<br>• Biometric data (for example if you choose to use fingerprint or face recognition when using the Brown Shipley & Co Limited mobile application software (the "**App**")). |
| Behavioural | Details about how you use our products and services and your attitude to risk. |
| Consents | Any permissions, consents or preferences that you indicate to us such as how you would like us to contact you. |
| Documentary Data | Details about you that are stored in documents or copies of them (for example your passport, drivers licence or birth certificate). |
| Technical | Details on the technology and devices you use. |
| Usage Data | Other data about how you use our products and services. |
| CCTV Recording | CCTV surveillance is used primarily to assist with security and safety of our staff and visitors to our offices, although in occasional situations we may use CCTV footage in investigations and/or be asked to provide to law enforcement agencies. |

In certain circumstances, the provision of information to us is required in order for us to decide whether to offer our services to you or to comply with our legal obligations e.g. in relation to certain information about your tax status or in relation to our anti-money laundering requirements. What we need from you in each circumstance will be explained to you in the relevant services application form or client profile form. If you do not provide us with the required information, we will not be able to offer certain services to you.

## 3. Our use of automated tools

As part of the provision of our services to you, we sometimes use automated tools to help us make decisions based on personal information we have, or are allowed to collect from others, about you, your business or other related parties. We use these automated tools to inform our decision making – we do not rely on them solely to make any decisions and the final decisions lie with members of our banking and advisory teams. The use of such automated tools helps us to make sure our decisions are quick, fair, efficient and correct, based on what we know. These automated tools can affect the products, services or features we may offer you now or in the future. Examples of where we use such automatic tools when we make decisions about you are detailed below:-

### Tailoring products and services

To assess your suitability for certain products when we provide wealth planning services we use internal and external profiling tools to help us ascertain your risk profile

We may also place you in groups with similar clients, known as customer segmentation. We use customer segmentation to learn about our clients' needs and guide us when designing products and services for different customer segments, and to manage our client relationships.

### Approving credit

We use a system to help us decide whether to lend money to you or your business. This system is called credit scoring and it uses past data about you to assess how you're likely to act while paying back any money you borrow. This includes data about similar accounts you may have had before. Credit scoring uses data from four sources:

- Your application form
- Credit reference agencies
- Data we may already hold about you
- Data we obtain from public sources e.g. Companies House.

The credit scoring system provides an overall assessment based on this information which we and other banks and lenders use to help make responsible lending decisions that are fair and informed.

### Detecting fraud

We use your personal information to help us to decide whether your personal or business accounts may be being used for fraud or money-laundering. We may detect suspicious activity on your account which could suggest that an account is being used in ways that fraudsters frequently work. Alternatively, we may notice that an account is being used in a way that is unusual for you or your business. Either of these could indicate a possible risk of fraud or money laundering. If we think there is a risk of fraud, we may stop activity on the accounts or refuse access to them. Fraud prevention agencies will also keep a record of the risk that you or your business may pose. This may result in other organisations refusing to provide you with products or services, or to employ you.

## 4. How we collect your personal information

We will collect personal information about you (or other related parties or your business) from you, from other companies within our Group and from others as follows:

Information you give to us:

- When you apply for our products or services or complete other forms or documentation;
- When you talk to us either in person or over the telephone;
- Correspond via emails or letters or via our website;
- During review meetings;
- If you take part in any competitions, surveys or promotions that we may run.

### Information we collect when you use our services.

This includes:

- The amount, frequency, type, location, origin and recipients of payment and transaction data.
- Profile and usage data. This includes the profile you create to identify yourself when you connect to our internet, mobile and telephone services. It also includes other data about how you use those services. We gather this data from devices you use to connect to those services, such as computers and mobile phones, using cookies and other internet tracking software. For full information please see the section on Cookies on our website, www.brownshipley.com.
- CCTV surveillance - CCTV systems are installed at all of our office premises. All internal and external CCTV cameras are clearly visible. Typically, they are positioned on the exterior of the building, reception areas and lift lobbies.
- If you provide us with details of other individuals, you agree to inform them of our use of their data as detailed in this privacy notice.

### Information from third parties we work with:

- Independent Financial Advisors
- Organisations that introduce you to us

- Credit reference agencies such as Experian, Equifax and Transunion International UK Limited (formally Callcredit). The following link provides further details about Transunion and the information it holds www.transunion.co.uk/legal-information/general-privacy-notice
- Fraud prevention agencies
- Government and law enforcement agencies
- Land agents
- Public information sources such as Companies House
- Medical practitioners
- Agents working on our behalf
- Companies that you work for or hold shares in

## 5. Who we might share your personal information with

We will only use and share your information where it is necessary for us to lawfully carry out our business activities or where we have your permission. Your personal data may be disclosed to other members of our Group, our agents, brokers and connected parties, and other financial institutions whose products we may provide or propose for you, such as insurance cover.

We may also share your personal information with:

- Other companies that we introduce you to.
- Where required for your product or service.
- HM Revenue & Customs, amongst other regulatory bodies and authorities.
- With third parties providing services to us, such as market analysis and benchmarking, correspondent banking and sub-contractors acting on our behalf, such as the companies that print our account statements.
- With other banks to help trace funds where you are a victim of suspected financial crime and you have agreed for us to do so, or where we suspect funds have entered your account as a result of financial crime.
- UK Financial Services Compensation Scheme
- Credit reference agencies
- Fraud prevention agencies
- Parties linked directly to you by contract, such as a spouse with a joint account
- Agents and advisers who we use to help run your accounts and services, collect what you owe and explore new ways of doing business
- Companies, organisations or people where you have agreed with us to share your data.
- In anonymised form as part of statistics or other aggregated data shared with third parties or
- Where permitted by law, it is necessary for our legitimate interests or those of a third party, and it is not consistent with the purposes listed above.

We may need to share your personal information with other organisations to provide you with the product or service you have chosen:

- If you have a Visa card with us, we will share transaction details with companies which help us to provide this service such as Visa.
- If you use payment services, we will share your data with our payment service providers such as SWIFT, Faster Payments, CHAPS or BACS.
- If you have a secured loan or mortgage with us, we may share information with other lenders who also hold a charge on the property or professional advisers who may assist us with creating the loan or security documentation.
- If you have chosen to work with third parties in relation to payment initiation and account data services, you are allowing that third party to access information relating to your account. We are not responsible for any such third party's use of your account information, which will be governed by their agreement with you and any privacy notice they provide to you.

We may also share your personal information if there are any corporate changes to the Group in the future:

- Where we or KBL may choose to sell, transfer, or merge parts of our business, or our assets.
- During any such process, we may share your data with other parties. We'll only do this if they expressly agree to a formally binding contract to keep your data safe, private and confidential.

Some of the information you provide to us may be transferred to, stored and processed by third party organisations which process data for us and on our behalf. These third parties may be based (or store or process information) in the UK or elsewhere including outside of the EEA. As with many financial institutions, these third parties may include third party IT platforms (including cloud based platforms), suppliers of administrative and support services and suppliers of other specialist products. Where we transfer information to third parties to enable them to process it on our behalf, we ensure that the providers meet

or exceed the relevant legal or regulatory requirements for transferring data to them and keeping it secure.

We may also be obliged to disclose data under certain laws or by order of court or other competent regulatory body or may be permitted to disclose it under applicable data protection laws. For example, we work with law enforcement agencies to support their duty to detect, investigate, prevent and prosecute crime.

## 6. Sending data outside of the European Economic Area ("EEA")

We will only send your data outside of the EEA if:

- It is required in order to follow your instructions and provide our services to you.
- You request us to.
- We have to comply with a legal duty.
- We are establishing, exercising or defending our legal rights.
- We are otherwise permitted to do so under applicable data protection laws.
- The European Commission has decided that the country or organisations we are sharing your information with will protect your information adequately.

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

- Put in place a contract with the recipient that means they must protect the personal information to the same standards as is required in the EEA
- Transfer it to a non-EEA country with privacy laws that give the same protection as the EEA
- Transfer it to organisations that are part of Privacy Shield (or any successor or replacement scheme). This is a framework that sets privacy standards for data sent between the United States of America and European Union countries to ensure that those standards are similar to what are used within the EEA.
- Transfer it to organisations or countries that have other approved certification schemes or codes in place
- Rely on another appropriate ground under applicable data protection laws

If you want to know more about these types of transfers, you can contact us using the contact details set out at section 9 opposite.

## 7. How long will we keep your information?

We will keep your personal data for as long as you are a client of Brown Shipley, and in most cases, we will retain your data for a period of 15 years from the time when you cease to be a client. However, if you are a client of one of our pension products, we will keep your data indefinitely. We keep your data to maintain records according to any rules that apply to us for specific products and to respond to any future questions or complaints. We may keep your data for longer than the usual 15 years after you have ceased to be a client if we cannot or are not required to delete it for legal, regulatory or technical reasons.

Telephone calls that we record are retained for a period of seven years. CCTV recordings are generally retained for six months.

Information that we may provide to other organisations such as law enforcement, fraud prevention or credit reference agencies will operate different retention periods over which we have limited, if any, control.

## 8. Marketing

We may from time to time use your personal information to tell you about relevant products and services e.g. we may mail you a magazine about Brown Shipley and its products and services; this is usually sent on a quarterly basis. We also occasionally invite clients to social events. We hope that you find our magazine and invitations of interest but if you would prefer not to receive marketing material please let us know at any time using one of the methods set out in Section 9. You will also be given the opportunity when we initially establish a relationship with you to tell us whether or not you'd like to receive certain marketing communications and in what formats.

## 9. Your rights

Under the GDPR and DPA you have a number of important rights free of charge although they will not apply in all circumstances. In summary, those include rights to:

- Access your personal information and certain other supplementary information
- Require us to correct any mistakes in your information which we hold.
- Withdraw your consent or explicit consent given to enable us to process your personal data
- Require the erasure of personal information concerning you in certain situations.
- Receive the personal information concerning you which you have provided to us, in a structured, commonly used and machine-readable format and have the

right to transmit those data to a third party in certain situations. (This right is separate to your right to ask us to allow third parties to access certain of your payment transactions data.)

- Object at any time to processing of personal information concerning you for direct marketing
- Object to decisions being taken by automated means which produce legal effects concerning you or similarly significantly affect you
- Object in certain other situations to our continued processing of your personal information
- Otherwise restrict our processing of your personal information in certain circumstances

Please note that if you object to us processing your personal information, request us to restrict processing your personal information or request us to delete your personal information, we may have to suspend the operation of your account and/or the products or services we provide to you.

For further information on each of those rights, including the circumstances in which they apply, see the Guidance from the UK Information Commissioner's Office (ICO) on individuals' rights under the General Data Protection Regulation.

If you would like to exercise any of those rights, please:

- Email, call or write to us using the details below:

  Data Protection Officer
  Brown Shipley & Co. Limited
  3 Hardman Street Manchester M3 3HF
  Email address: DPO@brownshipley.co.uk
  Telephone number: 0161 214 6500
- Let us have enough information to identify you (e.g. account number, user name, registration details)
- Let us have proof of your identity and address (a copy of your driving licence or passport and a recent utility or credit card bill), and
- Let us know the information to which your request relates, including any account or reference numbers, if you have them.

We will respond to your requests within the applicable statutory time period.

## 10. Information Commissioner's Office

You can contact the Information Commissioner's Office via https://ico.org.uk/ or on 0303 123 1113 or at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF for information, advice or if you wish to exercise your right to make a complaint.

## 11. Changes to this policy

We may make changes to this notice from time to time as our business and internal practices and/or applicable laws change. If we intend to make any changes that are inconsistent with the original purpose(s) for which your personal data was collected or obtained, we will notify you in advance wherever possible with reference to our terms and conditions issued to you, or otherwise as is permitted by applicable law. However, please note that in some cases, if you do not agree to such changes it may not be possible for us to continue to operate your account and/or provide certain products and services to you.

28 May 2019