

## Privacy Notice

This Privacy Notice is for all clients and prospective clients of WBR Group Limited and all its subsidiaries. This details how we will collect and process the personal data that we hold about you and your rights under UK Data Protection legislation and regulation in respect of the data held.

WBR Group processes your data in accordance with the terms of the Data Protection Act 2018, the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 and the relevant provisions relating to the General Data Protection Regulation contained within the European Union (Withdrawal) Act 2018 (UK GDPR). This Privacy Notice explains, in detail, the types of personal data we may collect about you when you interact with us. It also explains how we will store and handle that data and keep it safe. Unless otherwise indicated, references in this Privacy Notice to the GDPR refer to the UK GDPR.

We know that there's a lot of information here, but we want you to be fully informed about your rights, and how we use your data. We hope the following sections will answer any questions you have but if not, please do get in touch with us.

The WBR Group companies and trading entities will be referred to as “we” or “our” in this notice.

WBR Group Limited will be the Data Controller as defined under UK Data Protection legislation and regulations.

Our contact details are:

Data Protection Officer  
WBR Group Limited  
5A Dominus Way  
Meridian Business Park  
Leicester LE19 1RP

Tel: 0333 320 9230  
Website: [wbrgroup.co.uk](http://wbrgroup.co.uk)

For further information on how your information is used, how we maintain the security of our information, and to exercise your rights to access information we hold on you, please contact us. Similarly, if you believe that the information we hold is wrong or out of date, please let us know and we will update it.

### What is personal data?

Personal data is any data that can be used to identify you.

### What personal data do we collect, how and when?

We will collect personal data from you at the outset of your relationship with us, from your application or from information you share as part of the initial meetings. We may also collect information from other third parties such as your financial adviser or accountant and any providers that are transferring money or assets to your scheme on your instruction. We will also collect personal data from you and other third parties instructed on your behalf throughout the course of your relationship with us as part of normal day to day activities. This could include during face to face or online meetings, by letter, email, telephone, online forms or platforms, social media, or third-party links.

You voluntarily give us your personal information for instance when:

- you contact us via our website
- provide a comment on our website
- write a review
- sign up to any newsletters
- interact with us on social media platforms, and/or
- use our services.

This personal data could include:

- Contact information such as name and address, country of residence, telephone numbers and email addresses;
- Information and correspondence from your contact with us, voice recordings from telephone calls, letters and emails;
- Socio-demographic information; date of birth (age), marital status, employment details, profession, gender, nationality and citizenship;
- Details of other people such as joint applicants, next of kin, power of attorney, children, or beneficiaries;
- Transactional information; account transactions, access to our online client portals;
- Financial details such as bankruptcy, tax status, earnings, unique tax reference number, sources of wealth, sources of funds;
- For clients of WBR Law Limited, legal case or transaction information;
- Legal; national identifiers, wills, national insurance number, copy documents relating to your identity, including photographic identification, such as birth certificate, passport, driving licence, proof of address documents, marriage certificates, information from fraud agencies, credit reference agencies, electoral roll and other publicly available information;
- Images of you collected by photography or CCTV should you visit our offices or attend our events – please see CCTV below for more information;
- Payment information that relates to a contractual relationship including bank details;
- Information collected automatically via cookies when you visit one of our websites or use one of our online platforms. See separate Website Privacy Notice our website for additional information; and
- Special category data if necessary, such as information relating to your health, such as medical conditions and disabilities, criminal data, information you provide if you are vulnerable, or where we suspect you may be vulnerable, biometric data supplied as part of our identity verification process, such as facial recognition data, fingerprints, and signature.

## CCTV

We may install CCTV systems in our offices and on the outside of our building and personal data in form of images or CCTV footage may be recorded.

We would operate CCTV in accordance with the ICO CCTV Code of Practice and are processing CCTV data in order to pursue our legitimate interests of:

- promoting a safe working environment and monitoring health and safety at our premises
- monitoring the safety and security of our premises
- deterring and assisting in the prevention, investigation and detection of crime and/or serious breaches of policies and procedures, and
- assisting with the identification and prosecution of offenders, including use of images as evidence in criminal proceedings.

CCTV would never used for any automated decision taking.

In all locations where CCTV is installed, signs are displayed notifying individuals that CCTV is in operation. Images captured by CCTV will not be kept for longer than is necessary and ordinarily, will not be retained for more than 30 days. However, on occasions, there may be a need to keep images for longer such as where a crime is being investigated.

We will only disclose images and audio to other authorised bodies such as the police or other law enforcement agencies for the purposes set out above.

## Telephone call recording

We record most incoming and outgoing telephone calls. Your personal data may be collected as a result.

We record conversations for the following reasons:

- to allow us to be able to properly assess the needs of our clients (including potential clients) and third parties in order that we can provide them with a better service and resolve their queries;
- to ensure we comply with regulatory requirements;
- to identify training and development needs;
- to identify and evaluate any expressions of dissatisfaction and/or complaints;
- to enable us to review call quality;
- to be able to collate internal management information regarding call handling;
- to protect the wellbeing and safety of our staff by identifying any threatening behaviour which can then be evidenced and acted upon where necessary.

Call recordings are destroyed in accordance with the retention information in this notice. If the recording is available, you can submit a request for a copy of your call by making a data subject access request to our DPO.

## Why do we need to collect personal data?

We are only entitled to hold and process your data where the law allows us to. The current law on data protection (Article 6 GDPR) sets out a number of different reasons for which a firm may collect and process your personal data.

We process your personal data for the following purposes:

- To provide the services set out in our agreement with you (contractual obligations), including but not limited to managing our relationship with you, communicating with you, providing you with advice or guidance in connection with our services to you, make and arrange payments;
- To carry out your instructions and manage your accounts and investments (contractual obligations);
- To meet our legal and regulatory obligations, as might reasonably be expected as part of running our business and which does not materially impact your rights, freedom or interests (legitimate interests);
- To send you updates, newsletters, and marketing communications (with your consent);
- To train our staff, measure the quality of the service we give to clients, improve our services and customer experience (legitimate interests); and
- To prevent fraud or other criminal activity and ensure the security of your data and accounts (legal compliance).

We will only process your personal data where we have a legal basis for doing so. This includes:

- Where you have provided positive consent to us;
- Where processing is necessary for the performance of a contract between you and us or to take steps to enter into a contact; or
- Where processing is necessary for compliance with a legal or regulatory obligation.

There may also be occasions, for example with fraud prevention, where we rely upon a legitimate interest basis upon which the data may be processed. A decision to process data on the basis of legitimate interest will be made on a case by case basis, only where necessary, and in line with the guidance set out in UK Data Protection legislation. We will not process data on a legitimate interest basis where you would not normally expect the data to be processed, or if it may cause you harm. In these circumstances, your legitimate interests will override ours.

There may also be specific circumstances where we process data where we rely upon a substantial public interest basis – see special category data below.

The primary legal basis that we intend to use for the processing of your data is for the performance of our services agreement contract with you.

The information that we collect about you is essential for us to be able to carry out the services that you require from us effectively. We may also use your information to verify your identity, improve our services or prevent and detect crime, fraud, or corruption. Without collecting your personal data, we would also be unable to fulfil our legal and regulatory obligations.

Where we process information on the basis of your consent, you have the right to contact us at any time to withdraw that consent.

### Special category data

Where special category data is processed, we will either obtain your explicit consent to collect and process this information, or where that is not relevant or obtaining consent is either not possible or unreasonable, we will rely on a substantial public interest basis, either support for individuals with a particular disability or medical condition, safeguarding of economic well-being of certain individuals, or suspicion of terrorist financing or money laundering. We will only collect and use special category data where we are required to do so by law, regulatory requirement, professional governing bodies, or it is required to enable us to fulfil our contract with you or your employer.

### Regulatory

We also use data to communicate with our regulators or legislators and to obey laws, regulations and codes of conduct that apply to us.

For example, we will process your data to enable us to identify and/or verify your identity and conduct fraud, credit and anti-money laundering checks in accordance with anti-money laundering and counter terrorism financing legislation and regulation.

### Consent

We may use your data to notify you of our other services but only where we have your consent to do so.

### Who will we share data with?

We may share your personal data to others, including trusted third parties which provide services we need to use in connection with the services we carry out for you, and other entities within the WBR Group.

These third parties include:

- claimants, beneficiaries, assignees and payees;
- pension schemes and providers with which the person whose personal information we are processing has an association;
- HM Revenue and Customs;
- your professional advisers, such as Financial Advisers, Legal Advisers, Accountants;
- investment providers you or your advisers have indicated you wish to use;
- other organisations you ask us to share information with;
- our regulators, auditors, legal advisors, consultants, and relevant ombudsmen;

- pension trustees where you are using our SSAS services;
- healthcare, social and welfare organisations;
- central and local government where required to do so by applicable law and regulation;
- service providers and suppliers we have engaged to support us in the delivery of our service to you, such as banks, IT providers, consultants, credit reference agency, identity verification service providers;
- any personal representatives you appoint;
- current, past, or prospective employers;
- market research companies solely for the purpose of improving our services;
- the company that securely hosts our off-site cloud storage servers; and
- any other third party permitted by law and in the following circumstances:
  - To protect the security of our business;
  - To comply with court orders;
  - If we sell, merge, restructure, or otherwise reorganise our business.

We may need to disclose sensitive personal data about you to third parties, such as information relating to your health where required to do so to give effect to an instruction from you or your Financial Adviser in respect of your account.

Where we share data with a credit reference agency or identity verification service provider, the service will check your details against various databases to confirm your identity and address. A non-credit footprint will be left on your credit history. This means you will be able to see a check has been carried out, but other credit reference agencies will not.

We apply a strict policy to those recipients or data processors to keep your data safe and protect your privacy. In particular:

- we provide only the information they need to perform their specific services;
- they may only use your data for the exact purposes we specify in our contract with them;
- we work closely with them to ensure that your privacy is respected and protected at all times;
- if we stop using their services, any of your data held by them will either be deleted or rendered anonymous.

If we wish to pass your personal data on to a third party for any purpose other than those stated in this notice, we will only do so once we have obtained your consent unless we are legally required to do so.

## Processing and sharing your data outside the UK

Your data is stored and processed within the UK. Any cloud IT and similar data storage facilities we used are based in the UK.

Your personal data will not be transferred outside of the UK unless the destination country has an adequate level of protection equivalent to that in the UK, or appropriate safeguards in contractual agreements that the third party will give your information the same level of protection it has in the UK.

Where adequate safeguards cannot be put in place, your information will only be transferred outside the UK where:

- You have given explicit consent to do so after having been informed of the potential risks;
- The transfer is required for the performance of a contract with us, for example, you decide you to invest in an investment that is managed or based outside the UK.

## Securing your data

We take protecting your data very seriously. Data you give us may be subject to Legal Professional Privilege and may be extremely sensitive and confidential.

We have implemented appropriate technical and organisational measures to protect your personal data from unauthorised access, disclosure, alteration, and destruction. We protect our IT system from Cyber Attack. Access to your personal data is password-protected, and sensitive data is secured by encryption. We regularly monitor our system for possible vulnerabilities and attacks, and we carry out penetration testing to identify ways to further strengthen security.

We have clear data protection and information security policies and procedures in place (along with regulatory and other legal obligations to keep your data safe) and these are regularly assessed as part of our compliance processes.

## How long do we keep your data for?

We will retain your personal information for as long as is necessary to carry out our contracted service to you and to perform our regulatory, statutory and legal obligations. In some instances, legislation and regulations set the length of time information must be kept. In other situations, we will use our discretion to ensure that we do not keep information longer than we need to.

Generally, we will retain your information for a period of six to seven years following the termination of the contractual relationship with us. There may be exceptions to this, such as where we need to keep records in respect of legal proceedings, a criminal investigation, where legislation requires us to keep information for longer, or where it is impractical to separate your data from that of someone else for whom we are still required to hold their information.

Where the last point applies, we will not attempt to use your data in any way, we will not give any other organisation access to your information, we will continue to have appropriate technical and organisational security in place to protect your information, and we will delete your information when we are able to do so.

For some data where we believe there is a legitimate reason for doing so, we may decide that it is proper and appropriate to keep data for longer than the stated retention periods.

Exceptions include:

- enquiries where we do not take on your case are kept for up to 24 months;
- call recordings are stored for six months.
- Data relating to our tax advisory services will be retained for 8 years from conclusion of the project;
- Data relating to our property conveyancing services will be retained for 10 years from conclusion of the transaction;
- Data relating to services provided on behalf of Phoenix Life will be returned to Phoenix Life at the end of our relationship with the client's scheme.

## Your Rights

UK Data Protection legislation and regulations set out a number of rights individuals have over their data.

- The right to be informed – you have the right to be informed about what data will be used, when and how it will be used. That is the purpose of this Privacy Notice;
- The right of access – you may request we provide you with a copy of the personal information we hold on you (commonly referred to as a 'data subject access request'). If we choose not to action your request, we will explain to you the reasons for our refusal;
- The right to rectification – if your data is inaccurate, you may request it be corrected. In specific circumstances, dependent on the purposes for our processing of your data, you may also request to have incomplete personal data completed. We may seek to verify the accuracy of the personal information before updating it;
- The right to erasure – you may request your data be erased (also known as the right to be forgotten). This only applies to data we hold at the time your request is received and does not apply to any data that may be obtained in the future. A request may be made where:
  - it is no longer required for its original purpose;
  - you have withdrawn consent (where we had relied on consent as the legal basis for processing), or
  - your information has been processed unlawfully;

unless:

- we have legal or regulatory obligations to comply with; or
- the information may be required to establish, exercise or defend a legal claim;
- The right to restrict processing – you can request restriction or suppression of your data where:
  - You have asked for data rectification, and we are verifying the changes;
  - Your information has been processed unlawfully;
  - Your information is no longer required for its original purpose, but we have retained your information to establish, exercise or defend a legal claim; or



- You have objected to your personal information being used (see below) and we are considering your objection request.

Where a restriction is in place, we shall continue to store your information (up to the point we would naturally delete your information), but not use it;

- The right to data portability – you can ask for your data to be provided in a structured, commonly used and machine readable format. This will include requests for your data to be securely moved, copied, or transferred electronically to another electronic storage facility;
- The right to object – you can object to us processing your information where it is being used for certain purposes, such as direct marketing purposes. In this instance we will note your preference and suppress direct marketing. We will also consider an objection to processing your information where we have used the legitimate interests legal basis for processing. This request may relate to all of your personal data we hold or only certain information, and may only apply to a particular purpose for processing; and
- Rights regarding automated decision making and profiling – we do not employ automated individual decision-making or profiling tools.

For further details on your rights, please visit the Information Commissioner's Office at <https://ico.org.uk/your-data-matters/>.

### If you wish to complain

If you wish to make a complaint about the way we handle your personal data, then please call, or write to us in the first instance. We will respond quickly with a summary guide of our complaints process and let you know the next steps we will take. Contact details for the complaints team are:

Email: [complaints@wbrgroup.co.uk](mailto:complaints@wbrgroup.co.uk)

Telephone: 03333 209 230

Postal Address: The Complaints Team, WBR Group, 5a Dominus Way, Leicester. LE19 1RP.

You also have the right to make a complaint, if you feel that your data has not been handled correctly or you are unhappy with our response to any requests you have made to us regarding the use of your personal data, direct to the Information Commissioner's Office:

Online chat: <https://ico.org.uk/make-a-complaint/> (opens in a new window; please note we can't be responsible for the content of external websites)

Telephone: 0303 123 1113

Postal Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow. SK9 5AF.

### Changes to this Privacy Notice

We reserve the right to revise this Privacy Notice at any time. We will keep this Privacy Notice under regular review (at least annually) and will place any updates on our website ([wbrgroup.co.uk](http://wbrgroup.co.uk)). Paper copies of the Privacy Notice are also available by contacting [marketing@wbrgroup.co.uk](mailto:marketing@wbrgroup.co.uk).

This Privacy Notice was last updated in May 2024.