

This Fair Processing Notice applies people a wide variety of people, from those who licensed the office from us to those who are working in them, including:

- The directors, shareholders or those with persons with significant control (PSC) in a company or other entity.
- Those who have signed the license for companies, charities, government departments, trusts, funds etc.
- Partners in limited liability partnerships
- Employees or contractors for any of the above
- Sole traders/ self-employed and any employees or contractors
- Partners in unincorporated partnerships and any employees or contractors

Our contact details

Our office is at 150 Minories, London EC3N | 0800 917 4444 | info@beoffices.com

Our Data Protection Officer is Kristy Gouldsmith and she can be contacted at DPO@beoffices.com

1. The data we collect about you

In your capacity as our client or prospective client, or an employee/contractor/worker of such, we may collect personal data from you. Personal data means any information about an individual from which that person can be identified.

Our primary goal in collecting personal data from you is to help us:

- verify your identity
- comply with our legal obligations
- deliver our services
- improve, develop and market new services
- investigate or settle enquiries or disputes
- comply with any applicable law, court order, other judicial process, or the requirements of a regulator; and
- enforce our agreements with you.

We use different methods to collect data from and about you, including through:

Direct interactions	You may give us your personal data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you: • apply for further information about our services using our contact form or otherwise • subscribe to our information emails • request marketing to be sent to you • or give us some feedback.
Automated technologies or interactions	As you interact with our website, we will collect data about your device, your browsing actions and patterns when you consent to our use of cookies.
Third parties or publicly available sources	We may receive personal data about you from various third parties and public sources including those set out below: Land Registry Companies House The Insolvency Service Electoral Roll Publicly available sources Other professionals, including surveyors, accountants, solicitors or barristers.

Individual clients

If you are a sole trader or a partner in an unincorporated partnership, we will collect the following data: below:

- Name and job title
- Address, email, and phone number
- Gender and date of birth

- Contact information including the company you work for and email address, where provided
- Payment information
- Relevant information, such as proof of address or identity, as required by anti-money laundering (AML). We need to check that you are using our services legally. To do this, we use providers that perform various checks for us in relation to AML, fraud and other 'know your client' related checks.

The following searches may be made:

- Electoral roll
- Postcode address files
- Consent databases
- Telephone directories
- Mortality registers
- Politically Exposed Persons (PEP) Intelligence databases
- Sanctions databases
- Birth Index Register
- Age range
- Bank account validation and verification.

We need this data in order to provide you with our services; without it, we are unable to provide our services to you. We will continue to process personal data to satisfy our client due diligence obligations throughout the time that you are our client.

Corporate clients

When we are engaged by corporate entities, those providing instructions are not data subjects. However, as part of such instructions, personal data may be provided to us (e.g. personal data relating to officers or personnel of our corporate client).

We will ask you to provide us with personal data of the owners, directors, partners and persons with significant control of the business and we may require you to provide us with additional personal data as you use our services.

We will collect, store and process the following personal data of the above-named individuals:

- Full name
- Email address
- Date of birth
- Home address
- Proof of address
- Proof of identity
- Other client due diligence information as required to on-board the company and meet our legal requirements, such as AML, fraud prevention, conflict checks and PEP checks.

We need to check that you are using our services legally. To do this, we use providers that perform various checks for us in relation to AML, fraud and other 'know your client' related checks.

The following searches may be made:

- Electoral roll
- Postcode address files
- Consent databases
- Telephone directories
- Mortality registers
- PEP Intelligence databases
- Sanctions databases
- Birth Index Register
- Age range
- Bank account validation and verification

We need this data in order to provide you with our services; without it, we are unable to provide our services to you. We will continue to process personal data to satisfy our client due diligence obligations throughout the time that you are our client.

For all sole traders or partners in unincorporated partnerships we will also collect billing information, including bank account information and payment information.

If you fail to provide personal data

Where we need to collect personal data by law, or under the terms of a contract that we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you. In this case, we may have to cancel the contract that you have with us but we will notify you if this is the case at the time.

Employees/contractors/ workers – collectively 'workers'

We process data regarding the people that are actually working in the licensed office:

CCTV – the building has CCTV and this will capture your image.

Access passes – the access pass will have the name and photo of the worker. Each worker will provide their own photo. The access passes are bar coded and do not contain any biometric data of the worker.

Contacts for your business – name, job title, phone and mobile number.

Fire wardens – name and mobile number.

2. How we use your personal data and legal basis for doing so

We may use your information for the following purposes:

Action	Reason	Legal basis
Responding to enquiries	Our website allows you to request information about our services using an electronic enquiry form. Contact information is required in each case, together with details of other personal data that is relevant to your service enquiry. This information is used to enable us to respond to your requests.	We are using your data with your consent to respond to your enquiry.
Fulfilment of services – sole traders and partners in unincorporated partnerships	It is necessary for us to process your information to perform our obligations in accordance with any contract that we may have with you.	We have a contract with you.
Fulfilment of services – corporate entities	We need to process the data of 'workers' for crime prevention, health and security via CCTV and access passes. We also need the personal data of your fire wardens. We need the personal data of your business contacts.	Legitimate interest
Resolving complaints or disputes	We need to be able to resolve any complaints or disputes with you.	Legitimate interest.

Legal compliance	We use your personal data to comply with our legal obligations, including anti-money laundering, conflicts and our regulatory and statutory obligations.	It is our legal obligation to use your personal data to comply with any legal obligations imposed upon us.
Marketing communications	We use your personal data to send you information about our services which may be of interest to you. We may also conduct surveys to improve our services. You may also consent to receiving our marketing.	It is in our legitimate interest to use your personal data for marketing purposes and you can unsubscribe at any time. Consent and you can unsubscribe at any time.

Our business requirements – legitimate interests

Action	Reason for processing – legitimate interest
Managing our business and marketing strategies (including recording and reporting on our business development activities).	We need to have business development and marketing strategies.
Purchasing, maintaining and claiming against our insurance policies.	We need to protect our business.
Continuously reviewing and improving our services and developing new ones.	We use your feedback to improve our services.
Obtaining legal advice, establishing, defending and enforcing our legal rights and obligations in connection with any legal proceedings or prospective proceedings.	We need to understand our obligations and establish and defend our legal rights.
Monitoring and producing statistical information regarding the use of our platforms, and analysing and improving their functionality.	We need to ensure that our website and other platforms are working properly.
Maintaining the security of our systems, platforms, premises and communications, including detecting and preventing threats.	We need to ensure that our premises and our platforms are secure.
Managing the proposed sale, restructuring, transfer or merging of any or all part(s) of our business, including responding to queries from the prospective buyer or merging organisation.	We need to be able to manage or sell parts of our business, if we choose to do so.

We have a legitimate interest in using your personal data for the above purposes. We have balanced your rights and freedoms against our business needs. Please inform us if you object to our processing.

3. Who we share your personal data with

We may share personal data with a variety of the following categories of third parties as necessary:

Entity	Legal basis for sharing
Our professional advisers such as lawyers and accountants.	Legitimate interest.
Government or regulatory authorities or law enforcement.	Legal obligation.
Professional indemnity or other relevant insurers.	Legitimate interest.
Regulators/tax authorities/corporate registries.	Legal obligation.
Third parties to whom we outsource certain services such as, without limitation, document processing and translation services, confidential waste disposal, IT systems or software providers, IT support service providers, document and information storage providers.	Legitimate interest.
Third party service providers to assist us with client insight analytics, such as Google Analytics.	Consent.

Please note this list is non-exhaustive and there may be other examples where we need to share personal data with other parties in order to provide our services as effectively as we can.

We conduct an appropriate level of due diligence and put in place contractual documentation in relation to any sub-contractor to ensure that they process personal data appropriately and according to our legal and regulatory obligations.

4. International transfers

We do not transfer your personal data outside of the UK or the EU.

5. Data security

We are committed to keeping the personal data provided to us secure and we have implemented appropriate information security policies, rules and technical measures to protect the personal data that we have under our control from unauthorised access, improper use or disclosure, unauthorised modification and unlawful destruction or accidental loss.

All of our directors, employees, consultants, workers and data processors (i.e. those who process your personal data on our behalf, for the purposes listed above), who have access to, and are associated with the processing of personal data, are obliged to respect the confidentiality of such personal data.

6. Retention of personal data

By law, we have to keep basic information about our clients and their employees etc.

Data	Retention Period
Anti-money laundering and client due diligence data	Five years from the last significant transaction.
Financial information	7 years
CCTV footage	28 days from the date of the image unless it is required for health and safety or crime detection/prevention purposes; at the request of any law enforcement authority; or for our own civil law purposes.
Access passes	These are returned by the worker once they have left your business.
Contact details	These are retained for six months and then deleted.

1. How to access your information and your other rights

You have the following rights in relation to the personal data that we hold about you:

- **Your right of access:** if you ask us, we will confirm whether we are processing your personal data and, if necessary, provide you with a copy of that personal data (along with certain other details). If you require additional copies, we may need to charge a reasonable fee.
- **Your right to rectification:** if the personal data that we hold about you is inaccurate or incomplete, you are entitled to request to have it rectified. If you are entitled to rectification and if we have shared your personal data with others, we will let them know about the rectification where possible. If you ask us, where possible and lawful to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.

Your right to erasure: you can ask us to delete or remove your personal data in some circumstances, such as where we no longer need it or if you withdraw your consent (where applicable). If you are entitled to erasure and if we have shared your personal data with others, we will let them know about the erasure where possible. If you ask us, where it is possible and lawful for us to do so, we will also tell you who we have shared your personal data with so that you can contact them directly.

- **Your right to restrict processing:** you can ask us to 'block' or suppress the processing of your personal data in certain circumstances, such as where you contest the accuracy of that personal data or you raise an objection with us. If you are entitled to restriction and if we have shared your personal data with others, we will let them know about the restriction where it is possible for us to do so. If you ask us, where it is possible and lawful for us to do so, we will also inform you who we have shared your personal data with so that you can contact them directly.
- **Your right to data portability:** you have the right, in certain circumstances, to obtain personal data that you have provided us with (in a structured, commonly used and machine readable format) and to reuse it elsewhere or to ask us to transfer this to a third party of your choice.
- **Your right to object:** you can ask us to stop processing your personal data, and we will do so, if we are:
 - relying on our own or someone else's legitimate interests to process your personal data, except if we can demonstrate compelling legal grounds for the processing; or
 - processing your personal data for direct marketing purposes.
- **Your right to withdraw consent:** if we rely on your consent (or explicit consent) as our

legal basis for processing your personal data, you have the right to withdraw that consent at any time.

- **Your right to lodge a complaint with the Information Commissioner's Office:** if you have a concern about any aspect of our privacy practices, including the way we have handled your personal data, you can report it to the ICO. We would, however, appreciate the chance to deal with your concerns before you approach the ICO, so please contact us in the first instance.

Please note that some of these rights may be limited where we have an overriding interest or legal obligation to continue to process the data, or where data may be exempt from disclosure due.

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

Helpline number: 0303 123 1113

What personal data do we collect about you; how do we use that personal data; and what is our legal basis? When you are a client, we collect and process your personal data in order to fulfil our

contract for services with you, to fulfil our legal obligations and with your consent. We need a legal basis in order to process your personal data. Most of our processing is because we either have a contract for services with you or we have a legal obligation to process the data. On occasion, we will seek your consent to process your personal data but you are free to refuse. We collect your name, address, date of birth and phone. Our legal basis to do so is because we have a contract with you and need this information for that contract. We need your bank account details for our contract with you. In order to comply with our legal obligations to prevent money laundering, we process your:

- passport (name, DOB, facial biometrics, passport number, nationality, gender, place of birth, signature)
- Biometric Residents Permit (name, date and place of birth/ biometrics - fingerprints and a photo of face/ immigration status / access to public funds)
- identity card issued by the Electoral Office for Northern Ireland (name, DOB, photo)
- valid photo card driving license (name, DOB, signature)
- HM Forces Identify Card (name, photo, number)
- firearms certificate or shotgun license (name, address)
- recent evidence of entitlement to a state- or local authority-funded benefit, including housing benefit, council tax benefit, tax credits, state pension, educational or other grant (name, address, DOB, NI number)
- instrument of a court appointment, such as a liquidator or grant of probate (name, address)
- current council tax demand letter or statement (name, address)
- HMRC-issued tax notification (name, address, DOB, NI number)
- end of year tax deduction certificates (name, address, DOB, NI)
- current bank statements or credit/debit card statements (name, address)
- current utility bill (name, address)
- disabled drivers blue badge (name, address)
- current student card (name, photo)
- national identify card (name, photo)

We will send you marketing information and newsletters when you consent for us to do so. We will also send you this type of information because you are a client of ours. You have the right to unsubscribe to marketing at any time. If you do choose to unsubscribe, we will keep your name and email address on a suppression list so that we don't email you again by accident. How long do we hold your personal data? We will hold your personal data that was collected for anti-money laundering purposes for five years, after which it will be destroyed. We will hold the personal data that was collected for the purposes of providing you with the service while you are a client and for seven years, after which it will be destroyed. When we use your personal data for marketing, we will do so only while we have your consent. If you withdraw your consent, we will hold your name and email on a suppression list for five years. Do we use any automated decision making? We do not use any automated decision making. Who do we share your personal data with? We share your personal data with the following recipients:

- our software providers
- cloud service providers
- payment providers
- companies that check your anti-money laundering documents
- SOCA

Do we transfer your personal data outside of the EU or EEA? We do not transfer your personal data outside of the EU. Your rights You have rights in respect of our processing of your personal data which are:

- To access to your personal data and information about our processing of it. You also have the right to request a copy of your personal data (but we will need to remove information about other people).
- To rectify incorrect personal data that we are processing.
- To request that we erase your personal data if: o we no longer need it; o if we are processing your personal data by consent and you withdraw that consent; o if we no longer have a legitimate ground to process your personal data; or o we are processing your personal data unlawfully
- To object to our processing if it is by legitimate interest.
- To restrict our processing if it was by legitimate interest.
- To request that your personal data be transferred from us to another company if we were processing your data under a contract or with your consent and the processing is carried out automated means.

If you want to exercise any of these rights, please contact us. If you have any questions or concerns, please email DPO@beoffices.com as most matters can be resolved informally in the first instance. You also have the right to lodge a complaint about our processing the UK's Information Commissioner's Office.