

Data Protection Notice

Compliance with the EU General Data Protection Regulation (“GDPR”)

Ashby Capital LLP (“**Ashby Capital**”, “**we**”, “**us**”) takes the security and privacy of personal data seriously. This Data Protection Notice (the “**Notice**”) sets out our approach to compliance with the GDPR and covers:

1. who is covered by this Notice;
2. what personal data we collect;
3. how we obtain your personal data;
4. how we use your personal data;
5. using personal data for marketing purposes;
6. on what legal basis we use your personal data;
7. with whom we share your personal data;
8. transfers of your personal data outside the EEA;
9. protecting your personal data;
10. how long we will keep your personal data;
11. your rights with respect to your personal data;
12. changes to this Notice; and
13. how to contact us.

1. Who is covered by this Notice

This Notice also applies to officers and employees of our investors, advisers, suppliers, service providers, consultants or commercial counterparties, and other organisations who contact us on behalf of those organisations, and those of advisers, agents and other service providers of our investors, with whom we interact in performing our role to manage and administer the Portfolio.

It also applies when you interact with us, such as by:

- corresponding with us;
- visiting our website for job opportunities; or
- generally enquiring about the Portfolio or browsing our website.

2. Personal data that we collect

This information includes:

- **Personal details:** such as name (including name prefix or title), gender, age and date of birth, nationality, business and home telephone details, residential address, business and personal email-address, position and place of work;
- **Government issued identifiers:** such as passport, identification card, driving licence, taxpayer identification number, national insurance number; and
- **Financial and tax information:** such as bank account details and individual self-certification form for tax reporting purpose.

3. How we obtain your personal data

We combine information that we have about you from various sources, including the information that you have provided to us.

We may receive personal data about you from sources, including:

- property managers;
- suppliers and third party service providers;
- banks and financial intermediaries; and
- publicly available sources.

Receiving Personal Data

We receive personal data throughout the course of performing our services via electronic means, mail, telephone, or as a result of notes taken during meetings.

4. How we use your personal data

We may collect and process personal data, for the following purposes:

- To carry out, develop and improve our business, market our Portfolio and conduct surveys or research;
- to carry out our contractual responsibilities with you; for compliance with legal and regulatory requests and related disclosures, including:
 - complying with Know-Your-Customer (KYC), Anti-Money Laundering and Combating the Financing of Terrorism laws (AML/CFT);
 - complying with requests from, and requirements of, local or foreign regulatory or law enforcement authorities; and
 - tax identification and reporting.
- to exercise or defend legal claims or protect rights of another natural or legal person; and
- we also combine information that we have about you from various sources, including the information that you have provided to us.

5. Use of personal data for marketing purposes

Personal data will only be used for marketing purposes where we have the consent of the person(s) to whom the data relates, or where there is a legitimate business reason for us to do so (for example, promoting, marketing and advertising our services). In situations where the latter is applicable, individuals will always be given the opportunity to opt-out of receiving further communications. We will not initiate unsolicited contact with any individuals.

6. The legal basis we use

We use personal data on the following bases:

- to comply with legal and regulatory obligations of Ashby Capital imposed by the laws of the EU and Member States. Please refer to section 4 “How do we use your personal data?” for more details; and
- for our legitimate business interests, including:
 - to operate and improve our business and minimise any disruption to the services that we may offer to our investors, the Portfolio or the tenants of our properties; and
 - to manage risks and prevent fraud.

In cases in which we wish to use your information for our legitimate business purposes, we carefully consider the position and do not proceed if we think your interests or fundamental rights and freedoms relating to your personal information would be prejudiced.

7. With whom we share your personal data

Only employees of Ashby Capital LLP and approved third parties will have access to the personal data we hold.

We share certain of your personal data with:

- the following trusted third parties:
 - any agents, consultants or third party service providers that we work with to provide services to our investors or the Portfolio. Examples include advisers, auditors and delegates; (the “**Service Providers**”);
 - entities with which we maintain commercial arrangements. Examples include banks, insurers and other financial intermediaries as well as their respective agents and contractors;
 - competent tax authorities, e.g. Her Majesty’s Revenue and Customs (HMRC); or
 - any other third parties such as public administrations, local or foreign law enforcement agencies, public and judicial authorities and other organisations to which Ashby Capital or Service Providers is under an obligation to make disclosure under any applicable legal or regulatory requirement; and
- our professional advisers.

8. Transfers to third countries

Once we have received personal data, we may store it in hard copy paper form and/or electronically. We do not normally transfer such information to anyone outside the European Economic Area. However, we may do so when particular circumstances so require. In such case, we will take steps to ensure that the information is protected by appropriate organisational and security measures by entering into European Commission Model Clauses with the recipients implementing standard data protection clauses. More information about European Commission Model Clauses can be found at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en

9. Protecting your personal data

Vetting and due diligence procedures for employees and providers

Pre-employment vetting, including criminal background checks, is conducted on all employees and references are obtained from previous employers.

Due diligence on third parties and suppliers

We undertake due diligence on a risk based approach when engaging with potential suppliers or other third parties. In accordance with Article 28 of the GDPR, we have reviewed our internal supplier management policies. We have had discussions with our key suppliers (those who process personal data on our behalf) to seek clarification of the steps being taken to ensure they are GDPR compliant and to ensure that our agreements with those suppliers provide adequate protection for data they process on our behalf, and we have updated relevant contract terms.

Training

In accordance with our GDPR implementation process, training will be rolled out to all employees during 2018.

Remote working

Where appropriate, Ashby Capital employees are able to work remotely. The same technological measures are in place to protect remote workers from viruses and social engineering. Remote access to our network is controlled via secure authentication, including password protection for company issued devices as well as our cloud platform.

Personal Data back ups

Our key business service systems, within which personal data is held, are backed up regularly.

Physical security measures

Secure entry systems are in place in our office. There is a manned reception presence at our office during normal working hours and the office is locked and burglar-alarmed outside these hours.

Technological security measures

Our servers are password protected and we operate a "need to know" access control policy where appropriate. Our network is secured by managed firewalls and anti-virus software. Internal and external vulnerabilities, including those on remote devices, are identified and remediated on a regular basis.

10. Retention and destruction of physical data

We will retain your personal data for the shortest of the following:

- up to four years from the date that we collected it; and
- until we receive your request to delete your personal data,

unless it is necessary for us to retain that personal data under applicable law or regulation (including for litigation purposes).

Where you have contacted us with a question or request, we will keep your personal data for as long as necessary to allow us to respond your question or request.

Physical records are stored securely on site. Data held in files will be subject to file retention and destruction policies in line with following criteria: (i) the length of time we have an ongoing relationship with you; and (ii) whether there is a legal obligation to which we are subject. Such files will be reviewed at appropriate intervals and destroyed accordingly. A confidential information destruction bin is available in the office and we use a certified secure destruction provider.

11. Your Rights

The GDPR provides you with certain rights. You may be entitled to:

- ask Ashby Capital about the processing of your personal data, and request a copy of your personal data;

- request the correction and/or (in some cases such as where we process your personal data based on your consent and you have decided to withdraw the consent) deletion of your personal data;
- request the restriction of the processing of your personal data;
- in some cases (such as where we process your personal data based on our legitimate interest and we cannot demonstrate a compelling ground for the processing; or where the processing is for direct marketing purpose), object to the processing of your personal data;
- withdraw your consent to the processing of your personal data where Ashby Capital is processing personal data based on your consent; and
- request receipt or transmission to another organisation, in a machine-readable form, of the personal data that you have provided to Ashby Capital.

Where you are given the option to share your personal data with us, you can always choose not to do so.

If we have requested your consent to processing and you later choose to withdraw it, we will respect that choice in accordance with our legal obligations.

Choosing not to share your personal data with us or withdrawing your consent to our use of it could mean that we are unable to perform the actions necessary to achieve the purposes of processing described (see section 4 “How we use your personal data”) or that you are unable to make use of the services and products offered by us. After you have chosen to withdraw your consent we may be able to continue to process your personal data to the extent required or otherwise permitted by law, in particular in connection with e.g., our obligations under the AML regulatory requirements.

You can exercise these rights at any time by sending a request by email to Simon Osborne, Legal Counsel (sosborne@ashbycapital.com), and providing further information (including appropriate proof of identity) as requested by us.

12. Changes to this Notice

We may amend this Notice from time to time. We will notify you of any substantive or material change in this Notice by sending e-mails or by publishing announcements on our website.

In order to ensure that you can receive our notification promptly, we suggest that you notify us promptly of any update to your e-mail address and other contact details that you provided to us.

13. Contact Us

For any questions or concerns regarding our data processing activities, personal data that we hold, or any additional queries, please contact: Simon Osborne, Legal Counsel (sosborne@ashbycapital.com)

We hope that we will be able to respond to questions about personal data and our processing in a suitable way. In the event that we are unable to do this, you additionally have the right to complain to the relevant data protection authority, which in the UK is the Information Commissioner. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website also has further information on your rights and our obligations.

June 2018