

# Personal Data Fair Processing Notice

---

This notice explains what information I collect, when I collect it and how we use this. During the course of our activities, we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

## **Who am I?**

Steven Tweedie at Grad House Limited, Room 3.10, Warwick Mill Business Village, Carlisle, Cumbria, CA4 8RR, take the issue of security and data protection very seriously and strictly adhere to guidelines published in the General Data Protection Regulation (EU) 2016/679 which is applicable from the 25th May 2018, together with any domestic laws subsequently enacted.

I am notified as a Data Controller with the Office of the Information Commissioner under registration number **ZA464198** and I am the data controller of any personal data that you provide to us.

Our Data Protection Officer is Steven Tweedie, Mobile 07967 133 485 [steven@contentonline.co.uk](mailto:steven@contentonline.co.uk)

Any questions relating to this notice and our privacy practices should be sent to [info@gradhouse.co](mailto:info@gradhouse.co) or by writing to Grad House Ltd, Room 3.10 Warwick Mill Business Village, Carlisle, Cumbria, CA4 8RR.

## **How we collect information from you and what information I collect**

I collect information about you:

- From your application for accommodation
- From any references we may collect to assess your suitability as a tenant
- From any credit reference agencies, we may use these to assess your financial suitability as a tenant

I collect the following information about you:

- Tenant name, e-mail address, telephone number, Date of Birth, address (including any previous addresses), marital status, National Insurance Number, nationality, next of kin, name of university or college where you are studying (if applicable), the name of friends that you are staying with (if applicable);
- Guarantor name, e-mail address, telephone number, Date of Birth, address (including any previous addresses), marital status, National Insurance Number, nationality, next of kin (if applicable);
- Property address; term, rent, deposit, utility and service responsibilities;
- The employment status of tenants and/or guarantors, address, contact details (including email, phone and fax numbers) of the employer/accountant, payroll numbers, length of employment, salary information (including any regular overtime or commission), and any other income received;
- Bank account details of the tenant, including account number and sort code, and any hire purchase/loan agreements/credit cards or store cards that you have; and
- Any welfare benefits that you may be eligible for, or are currently on.

## **Why I need this information about you and how it will be used**

I we need your information and will use your information:

- to undertake and perform our obligations and duties to you in accordance with the terms of our contract with you;
- to enable us to supply you with the services and information which you have requested;
- to help you to manage your tenancy;
- to carry out due diligence on any prospective tenant and/or guarantor, including whether there is any money judgements against them, or any history of bankruptcy or insolvency;
- to analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer;

- to contact you in order to send you details of any changes to our suppliers which may affect you; and
- for all other purposes consistent with the proper performance of our operations and business.

### **Sharing of Your Information**

The information you provide to me will be treated by me as confidential and will be processed only by any third party, acting on my behalf, within the UK/EEA.

I may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- If I/we enter into a joint venture with or merge with a business entity, your information may be disclosed to our new business partners or owners;
- To carry out due diligence on you as a prospective tenant/ guarantor, including but not limited to the carrying out of affordability checks, due diligence checks and the obtaining of references from relevant parties, whose data you have provided;
- If you request so, your information shall be disclosed in order to determine if there are any money judgements against you, as the prospective tenant/guarantor, or to determine if they have a history of bankruptcy or insolvency;
- If you are unable to make payments under your tenancy, your information may be disclosed to any relevant party assisting in the recovery of this debt or the tracing of you as a tenant; and
- In the creation, renewal or termination of the tenancy, your information will be disclosed to the relevant local authority, tenancy deposit scheme administrator, service/utility provider, freeholder, factor, facilities manager or any other relevant person or organisation in connection with this.

Unless required to do so by law, I/we will not otherwise share, sell or distribute any of the information you provide to me/ us without your consent.

### **Transfers outside the UK and Europe**

Your information will only be stored within the UK and EEA.

## Security

When you give us information we take steps to make sure that your personal information is kept secure and safe. Here are the places where your data is held along with some details on the security and encryption used to ensure your data is safe:

Product / Method	Description, i.e. what we use it for	Encryption used	Encryption type verified by supplier on	Additional Security measures used	Verified Internally by
E-MAIL SERVER - MICROSOFT EXCHANGE	This is our primary means of communication internally and externally. E-mails are sent for us to customers and received by us from customers, suppliers and partners.	With Office 365, your data is encrypted at rest and in transit, using several strong encryption protocols, and technologies that include Transport Layer Security/Secure Sockets Layer (TLS/SSL), Internet Protocol Security (IPSec), and Advanced Encryption Standard (AES).	3rd October 2018	Each individual within the organisation may only access data stored on their log in. Only 1 central admin has access to the full system.	ST
DROPBOX	This is our primary means of document storage within the business. Each employee has a log in to a central account. Space is dedicated to storage of key business documentation and can be accessed via the cloud log in.	Dropbox files and Dropbox Paper docs at rest are encrypted using 256-bit Advanced Encryption Standard (AES). To protect data in transit between Dropbox apps (currently desktop, mobile, API, or web) and our servers, Dropbox uses Secure Sockets Layer (SSL)/Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. Similarly, data in transit between a Paper client (mobile, API, or web) and the hosted services is encrypted via SSL/TLS.	3rd October 2018	We have set up several different levels of access. Only key personal get access to all data. Access is limited to a "need to have" basis.	ST
PARDOT	This is our primary email marketing automation software. Each employee has a secure login.	The Pardot Services use industry-accepted encryption products to protect Customer Data and communications during transmissions between a customer's network and the Pardot Services, including 128-bit SSL certificates signed by a Root Certificate Authority and / or 2048-bit RSA public keys at a minimum.	3rd October 2018	Passwords are changed at regular intervals. Passwords are deleted immediately that an employee leaves.	CP
SALESFORCE	Salesforce is where we store all our customer data. Every employee has a secure login and has limited access dependent on their Salesforce access privileges. For example an employee can only see customers they deal with. The Managing Director can see all records. The Finance Director and Marketing Manager can see only the records shared with them by the Managing Director.	The platform encryption process uses symmetric key encryption and a 256-bit Advanced Encryption Standard (AES) algorithm using CBC mode, PKCS5 padding, and a randomized, 128-bit initialization vector (IV) to encrypt field-level data and files stored on the Salesforce platform. Both data encryption and decryption occur on the application servers	3rd October 2018	Passwords are changed at regular intervals. Passwords are deleted immediately that an employee leaves.	CP
APPLE CONTACTS	This is our primary means of storing contact details for our customers, suppliers, employees and other business contacts.	File Vault in macOS and data protection in iOS. They also refuse to add a backdoor into any of their products. ?	3rd October 2018	The contacts list is accessed by employees via their laptop computer or mobile phones. Laptops are accessed by passwords known only to the user and mobile phones by a unique 6 digit code or facial recognition.	CC
MOBILE PHONES	This is our primary means of communication within the company. The phones are used for storage of customer, supplier, employees and other business contacts via iClouds and locally on each device.	File Vault in macOS and data protection in iOS. They also refuse to add a backdoor into any of their products. ?	3rd October 2018	Access to mobile phones is through entry of a unique 6 digit code or facial recognition.	CC
XERO ACCOUNTING CLOUD SOFTWARE	Xero is our cloud accounting package. Used by all members of staff for the following functions: Quotes, Invoices, Credit Notes, Financial Statements etc.	We encrypt all data that goes between you and Xero using industry-standard TLS (Transport Layer Security), protecting your personal and financial data. Your data is also encrypted at rest when it is stored on our servers, and encrypted when we transfer it between data centres for backup and replication.	3rd October 2018	2 factor authentication PLUS We have set up several different levels of access. Only key personal get access to all data. Access is limited to a "need to have" basis.	ST
SURVEY MONKEY	We use this tool to collect customer information when we run surveys or competitions, usually via the website.	SSL (Secure Sockets Layer) is a protocol developed for transmitting private documents or information via the Internet. SSL creates a secure connection between the client and a server, encrypting sensitive information being transmitted through the web page. SSL encryption is automatically turned on for all surveys and works on all the browsers Survey Monkey support.	3rd October 2018	The password and log in details are changed regularly and are only known by two members of the Marketing team.	JH
EVENTBRITE	We use the Eventbrite platform to book customers onto our events. Customer data is entered and submitted by the customer. Eventbrite data is linked to Pardot and the data collected is stored there.	All credit card information is encrypted with strong industry-standard cryptographic protocols such as AES and TLS while in transit through our systems. Eventbrite's website and APIs are accessible via a 256-bit SSL certificate issued by Digicert. Credit card information is never stored after transaction authorisation. Access to encryption keys is held by the smallest number of Eventbrite employees possible.	3rd October 2018	The password and log in details are changed regularly and are only known by two members of the Marketing team.	CP
COMPUTER HARD DISCS	Almost all business documents are stored within Dropbox. A small number are stored locally on individual users laptops and are password protected by the user when appropriate.		3rd October 2018	Laptops are accessed by passwords known only to the user. Company offices are in a secured location accessed by authorised personnel only. Laptops are kept in locked drawers or other secure locations overnight. When being transported laptops are never left unattended.	CC
SKYPE	Skype is used on a daily basis to help with speedy communication between staff working from home to communicate with the head office or with each other. Some of our suppliers and customers also use Skype.	Skype use TLS (transport-level security) to encrypt messages between Skype client and the chat service in our cloud, or AES (Advanced Encryption Standard) when sent directly between two Skype clients. Skype uses the AES (Advanced Encryption Standard*), also known as Rijndael, which is used by the US Government to protect sensitive information, and Skype has for some time always used the strong 256-bit encryption.	3rd October 2018	Passwords are changed at regular intervals. Passwords are deleted immediately that an employee leaves.	JH
HARDCOPY FILES KEPT IN OFFICE / HOME OFFICE	All business including our need to keep or carry some data in paper format. It is our policy to minimise this for both data protection reasons and also to minimise our environmental impact. Inevitably however some personal data is stored in print format. This would include such documents as: Quotes, Invoices, License Agreements, Policy Documents, Contracts, CV's , Payroll Data, Tax Records.	None	N/A	All print matter that is no longer required is either shredded on site by our cross shredding machine known as "Sally The Shredder". If we do not have time to feed it to Sally we send it to our off site data shredding company, Carlisle Business Supplies. The material is sealed into Opaque bags and collected by secure vehicle for off site shredding. Our Office Administrator is responsible for the maintenance of our internal shredding and the contract with the offsite shredding company.	ST

## **How long we will keep your information**

I review my data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract I have with you.

My full retention schedule is available at our office and I can provide a copy by request to me at [info@gradhouse.co](mailto:info@gradhouse.co)

## **Your Rights**

You have the right at any time to:

- ask for a copy of the information about you held by me/ us in my records;
- require me/ us to correct any inaccuracies in your information;
- make a request to me/ us to delete what personal data of yours I/ we hold; and
- object to receiving any marketing communications from me/ us.

If you would like to exercise any of your rights above please contact me on [info@gradhouse.co](mailto:info@gradhouse.co)

Should you wish to complain about the use of your information, I would ask that you contact me to resolve this matter in the first instance. You also have the right to complain to the Information Commissioner's Office in relation to my/ our use of your information. The Information Commissioner's contact details are noted below:

### **England:**

Information Commissioner's Office  
Wycliffe House, Water Lane  
Wilmslow, Cheshire, SK9 5AF  
Telephone: 0303 123 1113  
Email: [casework@ico.org.uk](mailto:casework@ico.org.uk)

### **Wales**

Information Commissioner's Office  
2nd floor, Churchill House  
Churchill way, Cardiff, CF10 2HH  
Telephone: 029 2067 8400  
Email: [wales@ico.org.uk](mailto:wales@ico.org.uk)

### **Scotland:**

The Information Commissioner's Office  
45 Melville Street, Edinburgh, EH3 7HL  
Telephone: 0131 244 9001  
Email: [Scotland@ico.org.uk](mailto:Scotland@ico.org.uk)

### **Northern Ireland:**

Information Commissioner's Office  
3rd Floor, 14 Cromac Place  
Belfast, BT7 2JB  
Telephone: 028 9027 8757  
Email: [ni@ico.org.uk](mailto:ni@ico.org.uk)

The accuracy of your information is important to me - please help me keep my records updated by informing me of any changes to your email address and other contact details.