PRIVACY POLICY

Houston Home Lettings Ltd T/A Houstons

Contents

1. Introduction

Houstons (“we” or “us”) is committed to ensuring the secure and safe management of data held by us in relation to customers, staff and other individuals. Our staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals’ data in accordance with the procedures outlined in this policy and documentation referred to herein.

We need to gather and use certain information about individuals. These can include customers (tenants, landlord clients etc.), employees and other individuals that we have a contractual relationship with. We manage a significant amount of data, from a variety of sources. This data contains “personal data” and “sensitive personal data” (known as “special categories of personal data” under the GDPR).

This policy sets out our duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

2. Legislation

It is a legal requirement that we process data correctly; we must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

(a) the General Data Protection Regulation (EU) 2016/679 (the GDPR);

(b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and

(c) any legislation that, in respect of the United Kingdom (UK), replaces, or enacts into UK domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the UK leaving the European Union.

3. Data

3.1 We hold a variety of data relating to individuals, including customers and employees (also referred to as "data subjects") which is known as personal data. The personal data held and processed by us is detailed within the "fair processing notice" (FPN) at Appendix 2 hereto and the data protection addendum of the terms and conditions of employment which has been provided to all employees.

3.1.1 Personal data is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by us.

3.1.2 We also hold personal data that is sensitive in nature (i.e. reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, or relates to health or sexual orientation). This is special category personal data or sensitive personal data.

4. Processing of personal data

4.1 We are permitted to process personal data on behalf of data subjects provided it is doing so on one of the following grounds:

- processing with the consent of the data subject (see clause 4.4 hereof);
- processing is necessary for the performance of a contract between us and the data subject or for entering into a contract with the data subject;
- processing is necessary for our compliance with a legal obligation;
- processing is necessary to protect the vital interests of the data subject or another person; or
- processing is necessary for the purposes of legitimate interests.

4.2 Fair processing notice

4.2.1 We have produced a fair processing notice (FPN) which we are required to provide to all customers whose personal data is held by us. That FPN must be provided to the customer from the outset of processing their personal data and they should be advised of the terms of the FPN when it is provided to them.

4.2.2 The FPN at Appendix 2 sets out the personal data processed by us and the basis for that processing. This document is provided to all our customers at the outset of processing their data.

4.3 Employees

4.3.1 Employee personal data and, where applicable, special category personal data or sensitive personal data, is held and processed by us. Details of the data held and processing of that data is contained within the employee FPN which is provided to employees at the same time as their contract of employment.

4.3.2 A copy of any employee's personal data held by us is available upon written request by that employee fromLaura Houston from the start of there employment..

4.4 Consent

Consent as a ground of processing will require to be used from time to time by us when processing personal data. It should be used by us where no other alternative ground for processing is available. In the event that we require to obtain consent to process a data subject's personal data, we shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by us must be for a specific and defined purpose (i.e. general consent cannot be sought).

4.5 Processing of special category personal data or sensitive personal data

In the event that we process special category personal data or sensitive personal data, we must do so in accordance with one of the following grounds of processing:

- the data subject has given explicit consent to the processing of this data for a specified purpose;
- processing is necessary for carrying out obligations or exercising rights related to employment or social security;

- processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- processing is necessary for the establishment, exercise or defence of legal claims, or whenever courts are acting in their judicial capacity; and
- processing is necessary for reasons of substantial public interest.

5. Data sharing

5.1 We share our data with various third-parties for numerous reasons in order that day to day activities are carried out in accordance with our relevant policies and procedures. In order that we can monitor compliance by these third-parties with data protection laws, we will require the third-party organisations to enter in to an agreement with us to govern the processing of data, security measures to be implemented and responsibility for breaches.

5.2 Data sharing

5.2.1 Personal data is from time to time shared amongst us and third-parties who require to process personal data that we process as well. Both us and the third-party will be processing that data in their individual capacities as data controllers.

5.2.2 Where we share in the processing of personal data with a third-party organisation (e.g. for processing of the employees' pension), we shall require the third-party organisation to enter in to a data sharing agreement with us in accordance with the terms of the model data sharing agreement set out in Appendix 3 to this policy.

5.3 Data processors

A data processor is a third-party entity that processes personal data on behalf of us and are frequently engaged if certain parts of our work is outsourced (e.g. payroll, maintenance and repair works).

5.3.1 A data processor must comply with data protection laws. Our data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify us if a data breach is suffered.

5.3.2 If a data processor wishes to sub-contact their processing, our prior written consent must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

5.3.3 Where we contract with a third-party to process personal data held by us, it shall require the third-party to enter in to a data protection addendum with us in accordance with the terms of the model data protection addendum set out in Appendix 4 to this policy.

6. Data storage and security

All personal data held by us must be stored securely, whether electronically or in paper format.

6.1 Paper storage

if personal data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no personal data is left where unauthorised personnel can access it. When the personal data is no longer required it must be disposed of by the employee so as to ensure its destruction. If the personal data requires to be retained on a physical file then the employee should ensure that it is properly secured within the file (e.g.

stapled, or the documents are put on a Treasury Tag within the file) which is then stored in accordance with our storage provisions.

6.2 **Electronic storage**

personal data stored electronically must also be protected from unauthorised use and access. Personal data should be password protected when being sent internally or externally to our data processors or those with whom we have entered in to a data sharing agreement. If personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be stored securely at all times when not being used. Personal data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7. Breaches

7.1 A data breach can occur at any point when handling personal data and we have reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of the breach require to be reported externally in accordance with clause 7.3 hereof.

7.2 Internal reporting

We take the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the data protection officer (DPO) must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- we must seek to contain the breach by whatever means available;

- the DPO must consider whether the breach is one which requires to be reported to the Information Commissioner's Office (ICO) and data subjects affected and do so in accordance with this clause 7;
- notify third parties in accordance with the terms of any applicable data sharing agreements

7.3 Reporting to the ICO

The DPO is required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of the breach to the ICO within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

8. Data protection officer

8.1. A DPO is an individual who has an over-arching responsibility and oversight over compliance by us with data protection laws. We have elected to appoint a DPO whose details are noted on our website and contained within the fair processing notice at Appendix 3 hereto.

8.2 The DPO will be responsible for:

8.2.1 Monitoring our compliance with data protection laws and this policy;

8.2.2 co-operating with and serving as our contact for discussions with the ICO;

8.2.3 reporting breaches or suspected breaches to the ICO and data subjects in accordance with part 7 hereof.

9. Data subject rights

9.1 Certain rights are provided to data subjects under the GDPR. Data subjects are entitled to view the personal data held about them by us, whether in written or electronic form.

9.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to our processing of their data. These rights are notified to our customers in our FPN.

9.3 **Subject access requests**

Data subjects are permitted to view their data held by us upon making a request to do so (a subject access request). Upon receipt of a request by a data subject, we must respond to the subject access request within one month of the date of receipt of the request. We:

9.3.1 must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law;

9.3.2 where the personal data comprises data relating to other Data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the subject access request; or

9.3.3 where we do not hold the personal data sought by the data subject, must confirm that we do not hold any personal data sought by the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

9.4 **The right to be forgotten**

9.4.1 A data subject can exercise their right to be forgotten by submitting a request in writing to us seeking that we erase the data subject's personal data in its entirety.

9.4.2 Each request received by us will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with this clause and will respond in writing to the request.

9.5 **The right to restrict or object to processing**

9.5.1 A data subject may request that we restrict our processing of the data subject's personal data, or object to the processing of that data.

9.5.1.1 In the event that any direct marketing is undertaken from time to time by us, a data subject has an absolute right to object to processing of this nature by us, and if we receive a written request to cease processing for this purpose, then we must do so immediately.

9.5.2 Each request received by us will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.5 and will respond in writing to the request.

10. Privacy impact assessments

10.1 Privacy impact assessments (PIAs) are a means of assisting us in identifying and reducing the risks that our operations have on personal privacy of data subjects.

10.2 We shall:

10.2.1 Carry out a PIA before undertaking a project or processing activity which poses a high risk to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing personal data.

10.2.2 In carrying out a PIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that we will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.

10.3 We will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

11. Archiving, retention and destruction of data

We cannot store and retain personal data indefinitely. We must ensure that personal data is only retained for the period necessary. we shall ensure that all personal data is archived and destroyed timeously and at the point that we no longer need to retain that personal data in accordance with the periods specified within the table at Appendix 5 hereto

Appendix 2

Houstons

GDPR Fair Processing Notice

(How we use your personal information)

This notice explains what information we collect, when we 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.

Houstons Office 8 68-74 Queen Elizabeth Avenue, Glasgow, G52 4NQ SC384141 ("**we**" or "**us**") take the issue of security and data protection very seriously and strictly adhere to guidelines published in the Data Protection Act of 1998 and the General Data Protection Regulation (EU) 2016/679 which is applicable from the 25 May 2018, together with any domestic laws subsequently enacted.

We are notified as a data controller with the Information Commissioner's Office (ICO) under registration number **Z3147682** and we are the data controller of any personal data that you provide to us.

Our point of contact is Laura Houston, laura@houstons.uk.com, 01413282272, address as above.

Any questions relating to this notice and our privacy practices should be sent to Laura Houston.

How we collect information from you and what information we collect

We collect information about you:

- when you apply for housing with us, become a tenant, request services/repairs, enter in to a tenancy agreement with ourselves howsoever arising or otherwise provide us with your personal details;
- from your use of our online services, whether to report any tenancy related issues, make a complaint or otherwise;
- request a call back/viewing on a property via our website or property portals.

- from your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information).

We collect the following information about you:

- Name;
- Address;
- Telephone number;
- email address;
- National Insurance number;
- Next of kin

We receive the following information from third parties:

- benefits information, including awards of Housing Benefit/Universal Credit
- payments made by you to us;
- complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland;
- reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour.

Why we need this information about you and how it will be used

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 enable us to respond to your repair request, housing application and complaints made;
- 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 services or supplies which may affect you;

- for all other purposes consistent with the proper performance of our operations and business; and

- to contact you for your views on our products and services.

Sharing of your information

The information you provide to us will be treated by us as confidential [and will be processed only by our employees within the UK/European Economic Area (EEA) We 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 we enter into a joint venture with or merge with another business entity, your information may be disclosed to our new business partners or owners;
- if we instruct repair or maintenance works, your information may be disclosed to any contractor;
- if we are investigating a complaint, information may be disclosed to Police Scotland, local authority departments, Scottish Fire & Rescue Service and others involved in any complaint, whether investigating the complaint or otherwise;
- if we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and local authority);
- if we are investigating payments made or otherwise, your information may be disclosed to payment processors, local authority and the Department for Work & Pensions;
- if we are conducting a survey of our products and/or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results;
- if we are asked by HMRC in regard to taxation, your information may be accordingly disclosed;
-

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

Transfers outside the UK and Europe

1. Data is from time to time transferred overseas to areas outwith the EEA for the purposes of passing on your information to the landlord of the property you occupy where they are situated outwith the EEA.

2. Where information is transferred outside the UK or EEA we have ensured that where necessary the appropriate agreements and arrangements between the UK and the territories we are transferring the data to are in place, and that those territories have an agreement in place regarding their compliance with the General Data Protection Regulation.

Security

When you give us information we take steps to make sure that your personal information is kept secure and safe.

All hard copies of your data is stored securely in locked filing cabinets which can be accesses only by our employees. Electronic data is stored securely, with appropriate technical and security measures in place, as well as restrictions on access.

How long we will keep your information

We review our 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 we have with you.

Our full retention schedule is available within our privacy policy at www.houstons.uk.com.

Your rights

You have the right at any time to:

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

If you would like to exercise any of your rights above please contact us at **info@houstons.uk.com**

Should you wish to complain about the use of your information, we would ask that you contact us to resolve this matter in the first instance. You also have the right to complain to

the Information Commissioner's Office (ICO) in relation to our use of your information. The ICO's contact details are noted below:

The Information Commissioner's Office – Scotland
45 Melville Street, Edinburgh, EH3 7HL
Telephone: 0131 244 9001
email:scotland@ico.org.uk

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

Appendix 3

DATA PROCESSING AGREEMENT

between

Houston's, Office 8 68-74 Queen Elizabeth Avenue, Glasgow, G52 4NQ (the "Controller");

and

name of contractor (the "Processor")

(each a "**Party**" and together the "**Parties**")

WHEREAS

(a) The Controller and the Processor have entered in to an agreement/ contract to carry out maintenance works in various properties managed by the controller (hereinafter the "Principal Agreement"/"Principal Contract");

(b) This Data Processing Agreement forms part of the Principal Agreement/Principal Contract (*delete as appropriate); and

(c) In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Agreement to the Principal Agreement. Except where the context requires otherwise, references in this Agreement to the Principal Agreement are to the Principal Agreement as amended by, and including, this Agreement.

1. Definitions

1.1 The terms used in this Agreement shall have the meanings set forth in this Agreement. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement/Contract shall remain in full force and effect. In this Agreement, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 **"Applicable Laws"** means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Controller Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Controller Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Controller pursuant to or in connection with the Principal Agreement/Contract;

1.1.3 "**Contracted Processor**" means Processor or a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Restricted Transfer**" means:

1.1.8.1 a transfer of Controller Personal Data from the Controller to a Contracted Processor; or

1.1.8.2 an onward transfer of Controller Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of the Processor for the Controller pursuant to the Principal Agreement/ Contract;

1.1.10 "**Subprocessor**" means any person (including any third party and any group company, but excluding an employee of the Processor or any of its sub-contractors) appointed by or on behalf of the Processor which is engaged in the Processing of Personal Data on behalf of the Controller in connection with the Principal Agreement/Contract; and

1.2 The terms, "**Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly**.**

2. Processing of Controller Personal Data

2.1 The Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Controller Personal Data; and

2.1.2 not Process Controller Personal Data other than on the Controller's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the relevant Processing of that Personal Data.

2.2 The Controller

2.2.1 Instructs the Processor (and authorises the Processor to instruct each Subprocessor) to:

2.2.1.1 Process Controller Personal Data; and

2.2.1.2 in particular, transfer Controller Personal Data to any country or territory,

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement/Contract; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1.

2.3 The Schedule to this Agreement sets out certain information regarding the Contracted Processors' Processing of the Controller Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). The Controller may make reasonable amendments to the Schedule by written notice to Processor from time to time as the Controller reasonably considers necessary to meet those requirements. Nothing in the Schedule (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Agreement.

3. Processor and Personnel

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Controller Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Controller Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the latest software, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the Controller Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Subprocessing**

5.1 The Controller authorises the Processor to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 The Processor may continue to use those Subprocessors already engaged by the Processor as at the date of this Agreement, subject to the Processor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 The Processor shall give the Controller prior written notice of its intention to appoint a Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. The Processor shall not appoint (nor disclose any Controller Personal Data to) the proposed Subprocessor except with the prior written consent of the Controller.

5.4 With respect to each Subprocessor, the Processor shall:

5.4.1 before the Subprocessor first Processes Controller Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level

of protection for Controller Personal Data required by the Principal Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) the Processor, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Controller Personal Data as those set out in this Agreement and meet the requirements of article 28(3) of the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) the Processor or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Controller Personal Data; and

5.4.4 provide to the Controller for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Agreement) as the Controller may request from time to time.

5.5 The Processor shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Controller Personal Data carried out by that Subprocessor, as if it were party to this Agreement in place of the Processor.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 The Processor shall:

6.2.1 promptly notify the Controller if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Controller Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Controller or as required by

Applicable Laws to which the Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach**

7.1 The Processor shall notify the Controller without undue delay upon the Processor or any Subprocessor becoming aware of a Personal Data Breach affecting the Controller Personal Data, providing the Controller with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Processor shall co-operate with the Controller and at its own expense take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Controller Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Controller Personal Data

9.1 Subject to sections 9.2 and 9.3, the Processor shall promptly and in any event within seven (7) days of the date of cessation of any Services involving the Processing of Controller Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Controller Personal Data.

9.2 Subject to section 9.3, the Controller may in its absolute discretion by written notice to the Processor within seven (7) days of the Cessation Date require the Processor to (a) return a complete copy of all Controller Personal Data to the Controller by secure file transfer in such format as is reasonably notified by the Controller to the Processor; and (b) delete and procure the deletion of all other copies of Controller Personal Data Processed by any Contracted Processor. The Processor shall comply with any such written request within seven (7) days of the Cessation Date.

9.3 Each Contracted Processor may retain Controller Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Controller Personal Data and shall ensure that such Controller Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 Processor shall provide written certification to the Controller that it has fully complied with this section 9 within fourteen (14) days of the Cessation Date.

10. Audit rights

10.1 Subject to sections 10.2 and 10.3, the Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Controller Personal Data by the Contracted Processors.

10.2 Information and audit rights of the Controller only arise under section 10.1 to the extent that the Principal Agreement/Contract does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

10.3 Where carrying out an audit of Personal Data, the Controller shall give the Processor reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1 to any individual unless they produce reasonable evidence of identity and authority; or

10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Controller undertaking an audit has given notice to the Processor that this is the case before attendance outside those hours begins

11. General Terms

governing law and jurisdiction

11.1 The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement/Contract with respect to any disputes or claims howsoever arising under this Agreement, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.2 this Agreement and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement/Contract.

Order of precedence

11.3 Nothing in this Agreement reduces the Processor's obligations under the Principal Agreement/Contract in relation to the protection of Personal Data or permits the Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement/Contract.

11.4 Subject to section 11.2, with regard to the subject matter of this Agreement, in the event of inconsistencies between the provisions of this Agreement and any other agreements between the parties, including the Principal Agreement/Contract and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Agreement, the provisions of this Agreement shall prevail.

Changes in Data Protection Laws, etc.

11.5 The Controller may:

11.5.1 by giving at least twenty eight (28) days' written notice to the Processor, from time to time make any variations to the terms of the Agreement which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

11.5.2 propose any other variations to this Agreement which the Controller reasonably considers to be necessary to address the requirements of any Data Protection Law.

Severance

11.6 Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as

possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Appendix 4

DATA PROTECTION STATEMENT OF REQUIREMENTS FOR DATA PROCESSORS

I/We, Houstons, Letting Agent ("the Data Controller") as the Data Controller require, pursuant to or in connection with the Principal Agreement/Contract, I/we have with you, [organisation name who is being contracted with] [designation – registered in terms of the Companies Acts with registered number [registered number] and having its registered office/main office at [insert address]], ("the Data Processor"), that you are compliant with the General Data Protection Regulation 2016/679, and any subsequently enacted legislation in furtherance of Data Protection. Within this document, we state what we require of you as the Data Processor in order to be compliant. Should you have any questions regarding the contents of this document, you should contact **[insert point of contact for data protection/GDPR within your operations]**.

1. Definitions

1.1. **Applicable Laws** shall mean (a) European Union or member state laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection laws; and (b) any other applicable law with respect to any Controller Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws

1.2. **Controller Personal Data** shall mean any personal data processed by the Data Processor on behalf of the Data Controller pursuant to or in connection with the Principal Agreement or Contract;

1.3. **Principal Agreement/Contract** shall mean the main contract or agreement of services or other activities existing between the Data Controller and Data Processor;

1.4. **Subprocessor** shall mean any person (including any third party, but excluding an employee of the Processor or any of its sub-contractors) appointed by or on behalf of the Processor which is engaged in the processing of personal data on behalf of the Controller in connection with the Principal Agreement/Contract.

2. Processor and Personnel

2.1. The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the Processor who may have access to the Controller Personal Data; and

2.2. The Processor must ensure that access to the Controller Personal Data is strictly limited to those individuals who need to know or need to access this data.

3. Security

3.1. The Processor must, when processing Controller Personal Data, implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk; and

3.2. In assessing the appropriate level of security, the Processor shall take into account in particular the risks that are presented by processing, in particular a Personal Data Breach.

4. Subprocessing

4.1. The Controller authorises the Processor to appoint (and permit each Subprocessor appointed to appoint) Subprocessors;

4.1.1. This is only insofar as prior written notice is given of its intention to appoint a Subprocessor, including within this, the scope of processing that shall be undertaken by the Subprocessor, and that the Controller thereafter provides prior written consent of such appointment;

4.2. The Processor may continue to use those Subprocessors already engaged by the Processor as at 25 May 2018, so long as the Processor must undertake adequate due diligence of the Subprocessor, and their systems, prior to their processing of Controller Personal Data to warrant that there is a level of protection as mandated in the Principal Agreement.

5. Data Subject Rights

5.1. The Processor must ensure that they have appropriate technical and organisational measures so as to assist in the fulfilment of the Controller's obligations to respond to requests by any Data Subject under any Applicable Law;

5.2. The Processor must notify the Controller on receipt by them, or any Subprocessor, of a request from a Data Subject under any Applicable Law; and

5.3. The Processor must ensure that no response is given to any such request by the Processor or the Subprocessor, except on documented instructions of the Controller, or as required by the Applicable Laws to which the Processor is subject, in which latter case, the Processor shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the Contracted Processor responds to the request.

6. Personal Data Breach

6.1. The Processor must notify the Controller without undue delay upon the Processor or any Subprocessor becoming aware of a Personal Data Breach affecting the Controller Personal Data, providing the Controller with sufficient information to allow them to meet any obligations under the Applicable Laws;

6.2. The Processor shall co-operate with the Controller, and at their own expense take such reasonable commercial steps as are directed by the Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach.

7. Data Protection Impact Assessment and Prior Consultation

7.1. The Processor shall provide reasonable assistance to the Controller with any Data Protection Impact Assessment and Prior consultations with Supervising Authorities.

8. Deletion or return of Controller Personal Data

8.1. The Processor must promptly and in any event, within seven (7) days of the termination or conclusion of any Services involving the processing of Controller Personal Data ("**Cessation Date**"), delete and procure the deletion of all copies of any Controller Personal Data;

8.2. The Controller may also, at its own discretion, by providing seven (7) days written notice of the Cessation Date, require the Processor, to:

8.2.1. Return a complete copy of all Controller Personal Data to the Controller by secure file transfer in such a format as is reasonably notified by the Controller to the Processor; and

8.2.2. Delete and procure the deletion of all other copies of Controller Personal Data that they, or any Subprocessor, have;

8.3. The Processor must only do what is required under Clause 8.1 and 8.2 to the extent that the Applicable Laws do not require them to retain such information. In such event, the Processor must ensure the confidentiality of all such Controller Personal Data, and that it is processed, for such periods as mandated, only insofar as said Applicable Laws require it to be processed;

8.4. The Processor must provide written certification, within 14 days of the Cessation Date, to the Controller that it has fully complied with their obligations under this Clause.

9. Audit Rights

9.1. The Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Statement, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the processing of the Controller Personal Data by the Processor;

9.2. The Controller shall give the Processor reasonable notice of any audit or inspection to be conducted, and shall make reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Processor's premises, equipment, personnel and business while the Controller's personnel are on those premises in the course of such an audit or inspection; or

9.3. The Processor need not give access to its premises for the purposes of an audit or inspection to any individual unless they produce reasonable evidence of identity and authority; or outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Controller has given notice that this will be the case.

Data retention periods

The table below sets out retention periods for personal data held and processed by me, as a letting agent. It is intended to be used as a guide only. I recognise that not all personal data can be processed and

retained for the same duration, and retention will depend on the individual circumstances relative to the data subject whose personal data is stored.

Type of record	Suggested retention time
Records relating to working time	Two years from the date they were made
Council Tax records	10 years
Accident books and records and reports of accidents	Three years after the date of the last entry
Health and safety assessments and records of consultations with safety representatives and committee	Permanently
Applicants for accommodation	Five years
Housing Benefit notifications	Duration of tenancy
Tenancy files	Duration of tenancy
Former tenants' files (key info)	Five years
Third-party documents	Duration of tenancy
Records re offenders, ex-offenders (sex offender register)	Duration of tenancy
Lease documents	Five years after lease termination
Anti-social behaviour case files	Five years/end of legal action