Mr Gary J Getty BA(Hons) MCIH MARLA
for Getty Lettings Ltd

PRIVACY POLICY

Contents

1. Introduction

Getty Lettings Ltd and Mr Gary John Getty (we or I) are committed to ensuring the secure and safe management of data held by us/me in relation to customers, and other individuals. I, any staff or any other third-party that I contract with in fulfilment of my landlord obligations, 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.

I need to gather and use certain information about individuals. These can include customers (tenants) and other individuals that I have a contractual relationship with. I 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 my duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

2. Data

2.1 I hold a variety of data relating to individuals, including customers (also referred to as "data subjects") which is known as personal data. The personal data held and processed by me is detailed within the "fair processing notice" (FPN) at Appendix 2 hereto.

2.1.1 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 me.

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

3. Processing of personal data

3.1 I am permitted to process personal data on behalf of data subjects provided I am doing so on one of the following grounds:

- processing with the consent of the data subject (see clause 3.3 hereof);
- processing is necessary for the performance of a contract between the data subject and I, or for entering into a contract with the data subject;
- processing is necessary for my 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.

3.2 Fair processing notice

3.2.1 I have produced a fair processing notice (FPN) which I am required to provide to all customers whose personal data is held by me. 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.

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

3.3 Consent

Consent as a ground of processing will require to be used from time to time by me when processing personal data. It should be used by me where no other alternative ground for processing is available. In the event that I require to obtain consent to process a data subject's personal data, I 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 me must be for a specific and defined purpose (i.e. general consent cannot be sought).

Where consent is obtained and relied upon, the individual providing consent has the right to withdraw that consent at any time following it being provided.

3.4 Processing of special category personal data or sensitive personal data

In the event that I process special category personal data or sensitive personal data, I 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 or social protection law;
- 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;
- processing relates to personal data manifestly made public by the individual;
- processing is necessary for the purposes of preventative or occupational medicine, for the assessment of working capacity of employees, medical diagnosis, the prevention of health or social care or treatment;
- processing is necessary for public interest in the area of health;
- processing is necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes;
- processing is carried out in the course of legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim and on the condition that it relates to members or former members who have regular contact with the entity; and

- processing is necessary for reasons of substantial public interest under law.

3.5 I will comply with all requirements for processing your personal data, as set out in the FPN.

4. Data sharing

4.1 I share my 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 I can monitor compliance by these third parties with data protection laws, I will require the third-party organisations to enter in to an agreement with me to govern the processing of data, security measures to be implemented and responsibility for breaches.

4.2 Data sharing

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

4.2.2 Where I share in the processing of personal data with a third-party organisation, I shall require the third-party organisation to enter in to a “data sharing agreement” with me in accordance with the terms of the model data sharing agreement set out in Appendix 3 to this policy where the circumstances of sharing require such an agreement to be in place.

4.3 Data processors

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

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

4.3.2 If a data processor wishes to sub-contact their processing, my 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.

4.3.3 Where I contract with a third party to process personal data held by me, I shall require the third party to enter in to a data processing agreement with me in accordance with the terms of the model data processing agreement set out in Appendix 4 to this policy. Should they not enter into this, I will provide them with the data protection statement of requirements for data processors. This will outline what I require from them as a data processor, acting on my behalf.

5. Data storage and security

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

5.1 Paper storage

If personal data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. When the personal data is no longer required it must be disposed of by me so as to ensure its destruction. If the personal data requires to be retained on a physical file then I will ensure that it is affixed to the file which is then stored in accordance with my storage provisions.

5.2 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 and information encrypted on that media device. Personal data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

6. Breaches

6.1 A data breach can occur at any point when handling personal data and I 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 subject of the breach require to be reported externally in accordance with Clause 6.3 hereof.

6.2 Internal reporting

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

- as soon as the breach or potential breach has occurred, I must consider (i) the breach and its nature; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- I must seek to contain the breach by whatever means available;
- I must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with clause 6;
- notify third parties in accordance with the terms of any applicable data sharing agreements.

6.3 Reporting to the ICO

I am required to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the ICO within 72 hours of

becoming aware of the breach occurring. I must also consider whether it is appropriate to notify those data subjects affected by the breach.

7. Data subject rights

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

7.2 Data subjects have a variety of rights which include a right to request a restriction of processing their data, a right to be forgotten and a right to restrict or object to my processing of their data. These rights are notified to my customers in my fair processing notice.

7.3 Subject access requests

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

7.3.1 I 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.

7.3.2 Where the personal data comprises data relating to other data subjects, I 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.

7.3.3 Where I do not hold the personal data sought by the data subject, I must confirm that I 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.

7.4 The right to be forgotten

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

7.4.2 Each request received by me 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. I will then have the responsibility for accepting or refusing the data subject's request in accordance with this clause and will respond in writing to the request.

7.5 The right to restrict or object to processing

7.5.1 A data subject may request that I restrict my processing of the data subject's personal data, or object to the processing of that data.

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

7.5.2 Each request received by me 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. I will then have responsibility for accepting or refusing the data subject's request in accordance with clause 7.5 and will respond in writing to the request.

8. Data protection impact assessments (DPIAs)

8.1 These are a means of assisting us in identifying and reducing the risks that my operations have on personal privacy of data subjects.

8.2 I shall carry out a DPIA 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; and

8.2.1 In carrying out a DPIA, I shall 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 I will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

8.3 I will require to consult the ICO in the event that a DPIA identifies a high level of risk which cannot be reduced. I will be responsible for such reporting where such a high level of risk is identified.

9. Archiving, retention and destruction of data

I cannot store and retain personal data indefinitely. I must ensure that personal data is only retained for the period necessary. I shall ensure that all personal data is archived and destroyed timeously and at the point that I no longer need to retain that personal data