Data Protection Policy

In respect of Jasmine Technologies Ltd, trading as Street Stream

Effective 25 May 2018

1. Introduction

1. This Policy sets out the obligations of Jasmine Technologies Limited, a company registered in England under number 08838303, whose registered office is at 11 Claylands Place, London, SW8 1NL (“we”, “us”, “our”) regarding data protection and the rights of its data subjects being its customers, staff, contractors and business contacts, those on its marketing database in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).
2. This Policy incorporates our Data Retention Policy, IT Security Policy and Employee Data Protection Policy.
3. We place high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals we deal with. We are committed not only to GDPR, but also to the spirit of protecting personal data of our data subjects.
4. The GDPR defines “personal data” as any information relating to an “identified or identifiable natural person” (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier examples include (but are not limited to) a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
5. This Policy sets our obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles in this policy must be followed at all times by us, our employees, agents, contractors, or other parties working on behalf of us.
6. We are registered with the Information Commissioner as a data controller under the register held by the Information Commissioner.

2. Personal Data Collected, Held, and Processed

Type of Data	Purpose
Name	For delivery job facilitation
Email address	For delivery job facilitation & contact from Street Stream operations support
Contact phone number	For delivery job facilitation
Company name	For delivery job facilitation
Descriptive job data (pick-up, drop-off addresses; pick-up and drop-off contacts;	For delivery job facilitation; and for invoice records
Courier proof of identity	To confirm identity of courier during verification process and retain for security reasons
Courier proof of address	To confirm identity of courier during verification process and retain for security reasons
Courier driving licence	To confirm identity of courier during verification process and retain for safety reasons
Courier profile photo	Courier profile on website to aid customer recognition

3. The Data Protection Principles

This Policy aims to ensure our compliance with the GDPR.

The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

1. Processed lawfully, fairly, and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.
5. Kept in a form which permits identification of data subjects, for no longer than is necessary for the purposes for which the personal data is processed.
6. Processed in a manner that ensures appropriate security of the personal data, including without limitation protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

4. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

1. The right to be informed (Part 12).
2. The right of access (Part 13);
3. The right to rectification (Part 14);
4. The right to erasure (also known as the ‘right to be forgotten’) (Part 15);
5. The right to restrict processing (Part 16);
6. The right to data portability (Part 17);
7. The right to object (Part 18); and
8. Rights with respect to automated decision-making and profiling (Parts 19 and 20).

5. Lawful, Fair, and Transparent Data Processing

1. The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. The GDPR states that processing of personal data shall be lawful if at least one of the following applies:
    a. The data subject has given consent to the processing of their personal data for one or more specific purposes;
    b. The processing is necessary for the performance of a contract, to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract with them;
    c. The processing is necessary for compliance with a legal obligation to which the data controller is subject;
    d. The processing is necessary to protect the vital interests of the data subject or of another natural person;
    e. The processing is necessary for the performance of a task, carried out in the public interest or in the exercise of official authority vested in the data controller; or
    f. The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2. If the personal data in question is “special category data” (also known as “sensitive personal data”) (for example, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation), at least one of the following conditions must be met:
    a. The data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless EU or EU Member State law prohibits them from doing so);
    b. The processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by EU or EU Member State law or a collective agreement pursuant to EU Member State law, which provides for appropriate safeguards for the fundamental rights and interests of the data subject);
    c. The processing is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent;

d. The data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
e. The processing relates to personal data which is clearly made public by the data subject;
f. The processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
g. The processing is necessary for substantial public interest reasons, on the basis of EU or EU Member State law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
h. The processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of EU or EU Member State law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the GDPR;
i. The processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or EU Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
j. The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the GDPR based on EU or EU Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6. Specified, Explicit, and Legitimate Purposes

1. We collect and process the personal data set out in Part 2 of this Policy. This includes:
    a. Personal data collected directly from data subjects;
    b. and Personal data obtained from third parties.
2. We only collect, process, and hold personal data for the specific purposes set out in Part 2 of this Policy (or for other purposes expressly permitted by the GDPR).

3. Data subjects are kept informed at all times of the purpose or purposes for which we use their personal data. Please refer to Part 13 for more information on keeping data subjects informed.

7. Adequate, Relevant, and Limited Data Processing

We will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Part 6, above, and as set out in Part 2, below.

8. Accuracy of Data and Keeping Data Up-to-Date

1. We shall ensure that all personal data collected, processed, and held by us is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 15, below.
2. The accuracy of personal data shall be checked when it is collected and at regular intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate

9. Data Retention

1. We shall not keep personal data for any longer than is necessary, in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
2. When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
3. For full details of our approach to data retention, including retention periods for specific personal data types held by us, please refer to our Data Retention Policy (below).

10. Secure Processing

We shall ensure that all personal data collected, held, and processed by us is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 22 to 27 of this Policy.

11. Accountability and Record-Keeping

1. Our Data Protection Officer is James Middleton (james@streetstream.net) The Data Protection Officer shall be responsible for overseeing the implementation of this Policy

and for monitoring compliance with this Policy, our other data protection-related policies, and with the GDPR and other applicable data protection legislation.

2. We shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
    a. Our name and details, our Data Protection Officer, and any applicable third-party data processors;
    b. The purposes for which we collect, hold, and process personal data;
    c. Details of the categories of personal data collected, held, and processed by us, and the categories of data subject to which that personal data relates;
    d. Details of any transfers of personal data to non-EEA countries including all mechanisms and security safeguards;
    e. Details of how long personal data will be retained by us (please refer to our Data Retention Policy (below)); and
    f. Detailed descriptions of all technical and organisational measures taken by us to ensure the security of personal data.

12. Data Protection Impact Assessments

1. We shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data, which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.
2. Data Protection Impact Assessments shall be overseen by the Data Protection Officer and shall address the following:
    a. The type(s) of personal data that will be collected, held, and processed;
    b. The purpose(s) for which personal data is to be used;
    c. Our objectives;
    d. How personal data is to be used;
    e. The parties (internal and/or external) who are to be consulted;
    f. The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
    g. Risks posed to data subjects;
    h. Risks posed both within and to us; and
    i. Proposed measures to minimise and handle identified risks.

13. Keeping Data Subjects Informed

1. We shall provide the information set out in Part 2 below to every data subject:
    a. Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b. Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose when the first communication is made (if the personal data is used to communicate with the data subject); or before that transfer is made where the personal data is to be transferred to another party; or as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

2. The following information shall be provided:
    a. Our details including, but not limited to, the identity of our Data Protection Officer; The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 2 of this Policy) and the legal basis justifying that collection and processing;
    b. Where applicable, the legitimate interests upon which we are justified in collecting and processing of the personal data;
    c. Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
    d. Where the personal data is to be transferred to one or more third parties, details of those parties;
    e. Where the personal data is to be transferred to a third party that is located outside of the European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see Part 28 of this Policy for further details);
    f. Details of data retention;
    g. Details of the data subject's rights under the GDPR;
    h. Details of the data subject's right to withdraw their consent to our processing of their personal data at any time;
    i. Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);
    j. Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
    k. Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

14. Data Subject Access

1. Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which we hold about them, what we are doing with that personal data, and why.

2. Data subjects wishing to make a SAR may do so in writing, using our Subject Access Request Form, or other written communication. SARs should be addressed to our Data Protection Officer at Jasmine Technologies Ltd, 11 Claylands Place, London, SW8 1NL.
3. Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months, if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
4. All SARs received shall be handled by our Data Protection Officer.
5. We do not charge a fee for the handling of normal SARs. We reserve the right to charge reasonable fee, for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

15. Rectification of Personal Data

1. Data subjects have the right to require, that we rectify any of their personal data that is inaccurate or incomplete.
2. We shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing us of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
3. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

16. Erasure of Personal Data

1. Data subjects have the right to request that we erase the personal data we hold about them in the following circumstances:
    a. It is no longer necessary for us to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;The data subject wishes to withdraw their consent to us holding and processing their personal data;
    b. The data subject objects to us holding and processing their personal data, (and there is no overriding legitimate interest to allow we to continue doing so) (see Part 18 of this Policy for further details concerning the right to object);
    c. The personal data has been processed unlawfully;The personal data needs to be erased, in order for us to comply with a particular legal obligation;
    d. The personal data is being held and processed for the purpose of providing information society services to a child.

2. Unless we have reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one

month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

3. In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

17. Restriction of Personal Data Processing

1. Data subjects may request that we cease processing the personal data we hold about them. If a data subject makes such a request, we shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.
2. In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

18. Data Portability

1. We process personal data using automated means.
2. Where data subjects have given their consent to us to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between us and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).
3. To facilitate the right of data portability, we shall make available all applicable personal data to data subjects in the following formats: csv files; emails.
4. Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.
5. All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

19. Objections to Personal Data Processing

1. Data subjects have the right to object to us processing their personal data based on legitimate interests and direct marketing (including profiling).

2. Where a data subject objects to us processing their personal data based on its legitimate interests, we shall cease such processing immediately, unless it can be demonstrated that our legitimate grounds for such processing overrides the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
3. Where a data subject objects to us processing their personal data for direct marketing purposes, we shall cease such processing immediately.

20. Automated Decision-Making

1. We use personal data in automated decision-making processes.
2. Where such decisions have a legal effect (or similarly significant effect) on data subjects, those data subjects have the right to challenge to such decisions under the GDPR, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from us.
3. The right described in Part 2 does not apply in the following circumstances:
    a. The decision is necessary for the entry into, or performance of, a contract between us and the data subject;
    b. The decision is authorised by law; or
    c. The data subject has given their explicit consent.

21. Profiling

1. We use personal data for profiling purposes.
2. When personal data is used for profiling purposes, the following shall apply:
3. Clear information explaining the profiling shall be provided to data subjects, including the significance and likely consequences of the profiling;
4. Appropriate mathematical or statistical procedures shall be used;
5. Technical and organisational measures shall be implemented to minimise the risk of errors. If errors occur, such measures must enable them to be easily corrected; and
6. All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling.

22. Data Security: Transferring Personal Data & Communications

We shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

1. All emails containing personal data must be marked “confidential”;
2. Personal data may be transmitted over secure networks only - transmission over unsecured networks is not permitted in any circumstances;
3. Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;
4. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself should be deleted. All temporary files associated therewith should also be deleted;
5. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;
6. Where personal data is to be transferred in hard copy form it should be passed directly to the recipient or sent using first class or recorded post; and
7. All personal data to be transferred physically, whether in hard copy form or on removable electronic media shall be transferred in a suitable container marked “confidential”.

23. Data Security - Storage

We shall ensure that the following measures are taken with respect to the storage of personal data:

1. All electronic copies of personal data should be stored securely using passwords and data encryption;
2. All hard copies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
3. No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to us or otherwise without the formal written approval of The Data Reporting Officer and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary; and
4. No personal data should be transferred to any device personally belonging to an employee. Personal data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to us that all suitable technical and organisational measures have been taken).

24. Data Security - Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to our Data Retention Policy (below).

25. Data Security - Use of Personal Data

We shall ensure that the following measures are taken with respect to the use of personal data:

1. No personal data may be shared informally and if an employee, agent, subcontractor, or other party working on our behalf requires access to any personal data that they do not already have access to, such access should be formally requested from the Data Protection Officer;
2. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on our behalf not, without the authorisation of the Data Protection Officer;
3. Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, subcontractors, or other parties at any time;
4. If personal data is being viewed on a computer screen and the computer in question is not to be left unattended, for any period of time, the user must lock the computer and screen before leaving it; and
5. Where personal data held by us is used for marketing purposes, it shall be the responsibility of the Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

26. Data Security - IT Security

We shall ensure that the following measures are taken with respect to IT and information security:

a. All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols;
b. Under no circumstances, should any passwords be written down or shared between any employees, agents, contractors, or other parties working on our behalf, irrespective of

seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

c. All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. Our IT staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so; and
d. No software may be installed on any Company-owned computer or device without the prior approval of The Data Protection Officer

27. Organisational Measures

We shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a. All employees, agents, contractors, or other parties working on our behalf shall be made fully aware of both their individual responsibilities and our responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;
b. Only employees, agents, subcontractors, or other parties working on our behalf that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by us;
c. All employees, agents, contractors, or other parties working on our behalf handling personal data will be appropriately trained to do so;
d. All employees, agents, contractors, or other parties working on our behalf handling personal data will be appropriately supervised;
e. All employees, agents, contractors, or other parties working on our behalf handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
f. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
g. All personal data, held by us shall be reviewed periodically, as set out in our Data Retention Policy (see below);
h. The performance of those employees, agents, contractors, or other parties working on our behalf handling personal data shall be regularly evaluated and reviewed;
i. All employees, agents, contractors, or other parties working on our behalf handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract;
j. All agents, contractors, or other parties working on our behalf handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees arising out of this Policy and the GDPR; and
k. Where any agent, contractor or other party working on our behalf handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless us

against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

28. Notification to the Information Commissioner's Office

a. As a data controller, we are required to notify the Information Commissioner's Office that we are processing personal data. We are registered in the register of data controllers, registration number: ZA378157
b. Data controllers must renew their notification with the Information Commissioner's Office on an annual basis. Failure to notify constitutes a criminal offence.
c. Any changes to the register must be notified to the Information Commissioner's Office within 28 days of taking place.
d. The Data Protection Officer shall be responsible for notifying and updating the Information Commissioner's Office.

29. Transferring Personal Data to a Country Outside the EEA

a. We may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.
b. The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:
    i. The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;
    ii. The transfer is to a country (or international organisation) which provides appropriate safeguards, in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in the GDPR); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;
    iii. The transfer is made with the informed consent of the relevant data subject(s);

iv. The transfer is necessary for the performance of a contract between us and the data subject (or for pre-contractual steps taken at the request of the data subject);
v. The transfer is necessary for important public interest reasons;
vi. The transfer is necessary for the conduct of legal claims;
vii. The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or
viii. The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

30. Data Breach Notification

a. All personal data breaches must be reported immediately to the Data Protection Officer.
b. If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Officer must ensure, that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
c. In the event that a personal data breach is likely to result in a high risk, (that is, a higher risk than that described under Part b) to the rights and freedoms of data subjects, the Data Protection Officer must ensure that all affected data subjects are informed of the breach directly and without undue delay.
d. Data breach notifications shall include the following information:
    i. The categories and approximate number of data subjects concerned;
    ii. The categories and approximate number of personal data records concerned;
    iii. The name and contact details of our data protection officer (or other contact point where more information can be obtained);
    iv. The likely consequences of the breach;
    v. Details of the measures taken, or proposed to be taken, by us to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

31. How to complain

We hope that our Data Protection Officer can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at https://ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

32. Implementation of Policy

This Policy shall be deemed effective as of 25 May 2018. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:
Name: James Middleton
Position: Director
Date: 25 May 2018
Due for Review by: 25 May 2019
Signature:

Data Retention Policy

In respect of Jasmine Technologies Ltd, trading as Street Stream

Effective 25 May 2018

1. Introduction

a. This Policy sets out the obligations of Jasmine Technologies Limited, a company registered in England under number 08838303, whose registered office is at 11 Claylands Place, London, SW8 1NL ("we", "us", "our")regarding the retention of personal data collected, held, and processed by us in accordance with EU Regulation 2016/679 General Data Protection Regulation ("GDPR").
b. This Data Retention Policy incorporates our Data Protection Policy dated 25 May 2018.
c. The GDPR also addresses "special category" personal data (also known as "sensitive" personal data). Such data includes, but is not necessarily limited to, data concerning the data subject's race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.
d. Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects, for no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in the public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).
e. In addition, the GDPR includes the right to erasure or "the right to be forgotten". Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:
    i. Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
    ii. When the data subject withdraws their consent;
    iii. When the data subject objects to the processing of their personal data and we have no overriding legitimate interest;
    iv. When the personal data is processed unlawfully (i.e. in breach of the GDPR)
    v. When the personal data has to be erased to comply with a legal obligation; or
    vi. Where the personal data is processed for the provision of information society services to a child.
f. This Policy sets out the type(s) of personal data held by us, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.
g. For further information on other aspects of data protection and compliance with the GDPR, please refer to our Data Protection Policy (above).

2. Aims and Objectives

a. The primary aim of this Policy, is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that we comply fully with our obligations and the rights of data subjects under the GDPR.
b. In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that excessive amounts of data are not retained by us, this Policy also aims to improve the speed and efficiency of managing data.

3. Scope

a. This Policy applies to all personal data held by us and by third-party data processors processing personal data on our behalf.
b. Personal data, as held by us is stored in the following ways and in the following locations:
    i. Third-party servers, operated by Amazon Web Servers;
    ii. Laptop computers and other mobile devices provided by us to our employees;
    iii. Computers and mobile devices owned by employees, agents, contractors and subcontractors;

4. Data Subject Rights and Data Integrity

a. All personal data held by us is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in our Data Protection Policy (as above).
b. Data subjects are kept fully informed of their rights, of what personal data we hold about them, how that personal data is used, and how long we will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).
c. Data subjects are given control over their personal data, held by us including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict our use of their personal data, the right to data portability, and further rights relating to automated decision-making and profiling, as set out in our Data Protection Policy.

5. Technical & Organisational Data Security Measures

a. The following technical measures are in place to protect the security of personal data. Please refer to our Data Protection Policy for further details:
    i. All emails containing personal data must be encrypted;
    ii. All emails containing personal data must be marked “confidential”;
    iii. Personal data may only be transmitted over secure networks;
    iv. Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;
    v. Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
    vi. Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
    vii. Where personal data is to be transferred in hard copy form, it should be passed directly to the recipient or sent using first class post or registered post;
    viii. All personal data transferred physically should be transferred in a suitable container marked “confidential”;
    ix. No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from the Data Protection Officer;
    x. All hard copies of personal data, along with any electronic copies stored on physical media should be stored securely;
    xi. No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of we or not, without authorisation;
    xii. Personal data must be handled with care at all times and should not be left unattended or on view;
    xiii. Computers used to view personal data must always be locked before being left unattended;
    xiv. No personal data should be stored on any mobile device, whether such device belongs to us or otherwise without the approval of the Data Protection Officer and then strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary;
    xv. No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on our behalf where the party in question has agreed to comply fully with our Data Protection Policy and the GDPR;

xvi. All personal data stored electronically should be backed up with backups stored onsite / offsite. All backups should be encrypted;
xvii. All electronic copies of personal data should be stored securely using passwords and encryption;
xviii. All passwords used to protect personal data should be changed regularly and should must be secure;
xix. Under no circumstances, should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
xx. All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
xxi. No software may be installed on any Company-owned computer or device without approval; and
xxii. Where personal data held by us is used for marketing purposes, it shall be the responsibility of the Data Protection Officer to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS.

b. The following organisational measures are in place to protect the security of personal data. Please refer to our Data Protection Policy for further details:
    i. All employees and other parties working on our behalf shall be made fully aware of both their individual responsibilities and our responsibilities under the GDPR and under our Data Protection Policy;
    ii. Only employees and other parties working on our behalf that need access to, and use of, personal data in order to perform their work shall have access to personal data held by us;
    iii. All employees and other parties working on our behalf handling personal data will be appropriately trained to do so;
    iv. All employees and other parties working on our behalf handling personal data will be appropriately supervised;
    v. All employees and other parties working on our behalf handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
    vi. Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
    vii. The performance of those employees and other parties working on our behalf handling personal data shall be regularly evaluated and reviewed;
    viii. All employees and other parties working on our behalf handling personal data, will be bound by contract to comply with the GDPR and our Data Protection Policy;
    ix. All agents, contractors, or other parties working on our behalf handling personal data, must ensure that any and all relevant employees are held to the same

conditions as those relevant employees arising out of the GDPR and our Data Protection Policy

x. Where any agent, contractor or other party working on our behalf handling personal data fails in their obligations, under the GDPR and/or our Data Protection Policy, that party shall indemnify and hold us harmless against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

6. Data Disposal

a. Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:
   i. Personal data stored electronically (including any and all backups thereof) shall be deleted securely by automatically or by the Data Protection Officer.
   ii. Special category personal data stored electronically (including any and all backups thereof) shall be deleted securely by the Data Protection Officer;
   iii. Personal data stored in hard copy form shall be shredded;
   iv. Special category personal data stored in hard copy form shall be shredded.

7. Data Retention

a. As stated above, and as required by law, we shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.
b. Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.
c. When establishing and/or reviewing retention periods, the following shall be taken into account:
   i. Our objectives and requirements;
   ii. The type of personal data in question;
   iii. The purpose(s) for which the data in question is collected, held, and processed;
   iv. Our legal basis for collecting, holding, and processing that data;
   v. The category or categories of data subject to whom the data relates;
d. If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.
e. Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made by us to do so (whether in response to a request by a data subject or otherwise).

f. In limited circumstances, it may also be necessary to retain personal data for longer periods, where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Type	**Purpose**	**Retention Period**	**Comments**
Name	For delivery job facilitation	Indefinite or until deemed inactive (4 years)	Can be deleted on request.
Email address	For delivery job facilitation & contact from Street Stream operations support	Indefinite or until deemed inactive (4 years)	Can be deleted on request
Contact phone number	For delivery job facilitation	Indefinite or until deemed inactive (4 year)	Can be deleted on request
Company name	For delivery job facilitation	Indefinite or until deemed inactive (4 year)	Can be deleted on request
Descriptive job data (pick-up, drop-off addresses; pick-up and drop-off contacts;	For delivery job facilitation; and for invoice records	Automatically anonymised - all readily identifiable personal data will be removed after 4 years.	Can be deleted on request
Courier proof of identity	To confirm identity of courier during verification process and retain for security reasons	Indefinite	Will be deleted if courier account is deleted. Inactive or unverified courier accounts will be deleted after 3 months or on request
Courier proof of address	To confirm identity of courier during verification process and retain for security reasons	Updated once a year	Will be deleted if courier account is deleted. Inactive or unverified courier accounts will be deleted after 3

			months or on request
Courier driving licence	To confirm identity of courier during verification process and retain for safety reasons	Updated once a year	Will be deleted if courier account is deleted. Inactive or unverified courier accounts will be deleted after 3 months or on request
Courier motor vehicle insurance	To confirm identity of courier during verification process and retain for safety reasons	Updated once a year	Will be deleted if courier account is deleted. Inactive or unverified courier accounts will automatically be deleted after 3 months or on request
Courier profile photo	To aid customer recognition of courier	Courier can update at any time	Will be deleted if courier account is deleted. Inactive or unverified courier accounts will automatically be deleted after 3 months or on request

8. Roles and Responsibilities

a. The Data Protection Officer shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, our other Data Protection-related policies (including, but not limited to, our Data Protection Policy), and with the GDPR and other applicable data protection legislation.
b. Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Protection Officer.

9. Implementation of Policy

This Policy shall be deemed effective as of 25 May 2018 No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:
Name: James Middleton
Position: Director
Date: 25 May 2018
Due for Review by 25 May 2019
Signature: James Middleton