Appataxi Ltd
Data Protection Policy
10th October 2018

1. Introduction

This Policy sets out the obligations of Appataxi Ltd, a company registered in the United Kingdom under number 09272538, whose registered office is at Karoha, The Street, Acol, Birchington, Kent CT7 0JA ("the Company") regarding data protection and the rights of customers, business contacts ("data subjects") in respect of their personal data under EU Regulation 2016/679 General Data Protection Regulation ("GDPR").

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 such as 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.

This Policy sets the Company's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. All personal data must be:

2.1 Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

2.2 Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

2.3 Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

2.4 Accurate and, where necessary, kept up to date.

2.5 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.

2.6 Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.

3. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects:

3.1 The right to be informed.

3.1.1 Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

3.1.2 Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose;

a) if the personal data is used to communicate with the data subject, when the first communication is made; or

b) if the personal data is to be transferred to another party, before that transfer is made; or

c) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

3.2 The right of access.

3.2.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.

3.2.2 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.

3.2.3 The Company does not charge a fee for the handling of normal SARs but reserves the right to charge reasonable fees for additional copies of information that have already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

3.3 The right to rectification.

3.3.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.

3.3.2 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.

3.4 The right to erasure (also known as the 'right to be forgotten').

3.4.1 Data subjects have the right to request that the Company erases the personal data it holds about them in the following circumstances:

a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) The data subject objects to the Company holding and processing their personal data (and where there is no overriding legitimate interest to allow the Company to continue doing so);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation.

3.4.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erase 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.

3.4.3 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).

3.5 The right to restrict processing.

3.5.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company 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.

3.5.2 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).

3.6 The right to data portability.

3.6.1 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format(s):

a) Excel or similar.

3.6.2 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

3.6.3 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.

3.7 The right to object.

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

3.7.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing immediately, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights, and freedoms or that the processing is necessary for the conduct of legal claims.

3.7.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall case such processing immediately.

3.8 Rights with respect to automated decision-making and profiling.

3.8.1 The Company does not use personal data in automated decision-making processes.

3.8.2 The Company does not use personal data for profiling purposes.

4. **Lawful, Fair, and Transparent Data Processing**

The GDPR seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject.

4.1 The GDPR states that processing of personal data shall be lawful if at least one of the following applies:

4.1.1 The data subject has given consent to the processing of their personal data for one or more specific purposes;

4.1.2 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;

4.1.3 The processing is necessary for compliance with a legal obligation to which the data controller is subject;

4.1.4 The processing is necessary to protect the vital interests of the data subject or of another natural person;

4.1.5 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

4.1.6 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.

5. **Specified, Explicit, and Legitimate Purposes and Retention Periods of Personal Data**

5.1 The Company collects and processes the personal data set out in the table below. This includes:

5.1.1 Personal data collected directly from data subjects.

5.1.2 The Company only collects, processes, and holds personal data for the specific purposes set out in the table below.

5.2 The Company only keeps personal data for the periods set out in the table below and when no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

Type of Data	**Purpose of Data**	**Retention Period**
Name, address and contact details	To carry out business objectives	40 years

6. **Accuracy of Data and Keeping Data Up-to-Date**

6.1 The Company shall ensure that all personal data collected, processed, and held by it 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.

6.2 The accuracy of personal data shall be checked when it is collected. 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.

7. Accountability and Record-Keeping

7.1 The Company's Data Protection Contact is Tony Baker, appataxi.cab@gmail.com.

7.2 The Data Protection Contact shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Company's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

7.3 The Company shall keep written internal records of all personal data collection, holding, and processing.

8. Data Security - Transferring Personal Data and Communications

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

8.1 All emails containing personal data must be encrypted;

8.2 All emails containing personal data must be marked "confidential";

8.3 Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances; and

8.4 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential". Where possible, all removable electronic media shall be encrypted and password protected.

9. Data Security - Storage

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

9.1 All electronic copies of personal data should be stored securely using passwords;

9.2 All hardcopies 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;

9.3 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise; and

9.4 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 behalf of the Company 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 the Company that all suitable technical and organisational measures have been taken).

10. **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.

11. **Data Security - Use of Personal Data**

11.1 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time; and

11.2 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Tony Baker 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.

12. **Data Security - IT Security**

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

12.1 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;

12.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, 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;

12.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date; and

12.4 No software may be installed on any Company-owned computer or device without the prior approval of the Tony Baker.

13. **Organisational Measures**

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

13.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

13.2 Only employees, agents, sub-contractors, or other parties working on behalf of the Company 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 the Company;

13.3 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed; and

13.4 All agents, contractors, or other parties working on behalf of the Company 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 of the Company arising out of this Policy and the GDPR.

14. Transferring Personal Data to a Country Outside the EEA

14.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

14.2 Any transfer of data shall be 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;

14.3 Any transfer of data shall be to a country (or international organisation) which provides appropriate safeguards that complies with a supervisory authority (e.g. the Information Commissioner's Office); and

14.4 Any transfer shall be made with the informed consent of the relevant data subject(s).

15. Data Breach Notification

15.1 All personal data breaches must be reported immediately to the Company's Data Protection Officer/Contact who will follow the guidelines provided by the supervisory authority (e.g. the Information Commissioner's Office).

16. Implementation of Policy

This Policy shall be deemed effective as of 10th October 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: Tony Baker

Position: Director

Date: 10th October 2018

Due for Review by: 9th October 2019

Signature: