Ortto

Customer GDPR Addendum

This General Data Protection Regulation Addendum ("**Addendum**"), effective as of _____ (the "**Effective Date**"), amends those certain Terms of Use *(https://ortto.com/terms)* (the "**Agreement**") between _____, located at_____ ("**Customer**") and AutopilotHQ Inc., located at 1390 Market Street, Suite 200, San Francisco, CA, 94102 ("**Ortto**"), governing Customer's use of Ortto services. Customer and Ortto are each a "**Party**" and collectively are the "**Parties**".

In consideration of the mutual promises and obligations set forth herein, the sufficiency of which the Parties acknowledge, the Parties agree as follows:

1. Definitions

Capitalized terms used in this Addendum have the meaning set forth in Article 4 of the GDPR, unless defined in this Addendum or in the Agreement. References to "GDPR" shall be construed as references to "GDPR" and/or "UK GDPR", as applicable. The following terms shall have the meanings set forth below:

a) "**Customer Personal Data**" means Personal Data that is provided by Customer to Ortto and Processed by Ortto on behalf of Customer pursuant to Ortto's provision of the Services.
b) "**Data Protection Laws**" shall mean, to the extent applicable, (i) the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council ("**GDPR**") and any related or implementing domestic legislation, (ii) GDPR as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ("**UK GDPR**"), together with the Data Protection Act 2018, and any subordinate, related or implementing domestic legislation ("**UK Data Protection Law**"); each as may be amended or replaced from time to time.
c) "**Member State**" means any relevant member state of the European Union ("**EU**") or European Economic Area ("**EEA**") from time to time.
d) "**Personal Data Breach**" means a personal data breach as defined in Article 4 of the GDPR that affects Customer Personal Data.
e) "**Restricted Transfer**" means a transfer of Customer Personal Data by Customer or on its behalf to Orttoor any Ortto Affiliate (or any subsequent onward transfer), in each case, where such transfer would be prohibited by Data Protection Laws in the absence of the protection for the transferred Customer Personal Data provided by the relevant SCC.
f) "**SCC**" means, as the context requires or otherwise indicated in this Addendum, (i) Module 2 of the EU standard contractual clauses set out in the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended or replaced from time to time by a competent authority under the relevant Data Protection Laws ("**Module 2 SCC**"), and/or (ii) the standard contractual clauses (processors) set out in Decision 2010/87/EC, as amended or replaced from time to time, pursuant to Article 46 of the UK GDPR ("**UK SCC**").

g) "**Subprocessor**" means any third party (other than Ortto's employees), including any affiliate of Ortto that Ortto engages in accordance with the Agreement, that Processes Customer Personal Data on behalf of Ortto in order to provide the Services.
h) "**Transfer**", "**Transferred**" or "**Transferring**" means, whether by physical or electronic means, across national borders, both (i) the moving of Customer Personal Data from one location or person to another, and (ii) the granting of access to Customer Personal Data by one location or person to another.

2. Processing; Roles of the Parties

This Addendum sets forth the GDPR requirements applicable to Personal Data Processed by Ortto or through Ortto's (or a Subprocessor's) systems in connection with providing the services set forth in the Agreement (collectively, the "**Services**"). **Exhibit A** hereto sets out the Parties' understanding of the Customer Personal Data to be Processed by Ortto pursuant to this Addendum, as required by Article 28(3) of the GDPR. Customer will inform Orttoof any changes to Exhibit A required in order to reflect Customer's actual use of the Services. The Parties acknowledge that for purposes of this Addendum, Customer is a Controller and Ortto is a Processor.

3. Article 28 Requirements

In accordance with GDPR Article 28(3), Orttowill (and ensure that any Subprocessor acting under Ortto's authority also will):

a) Process the Customer Personal Data solely (i) as needed to provide the Services; (ii) in accordance with the specific documented instructions provided by Customer, including with regard to any Transfers, as set forth in the Agreement and this Addendum; and (iii) as required to comply with any EEA or Member State law (in which case, Ortto shall provide prior notice to Customer of such legal requirement, unless that law prohibits this disclosure on important grounds of public interest); provided, however, that Ortto will not have any obligation to monitor UK, EEA or Member State requirements.

b) Ensure that persons authorized to Process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) Take all security measures required by GDPR Article 32. Namely, taking into account the state of the art, 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, Ortto shall implement the measures set forth at https://journeys.autopilotapp.com/legal/security-policy, which include appropriate technical and organizational security measures to ensure a level of security appropriate to the risk, including, as appropriate: (i) the pseudonymisation and encryption of Customer Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (iii) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

d) Assist the Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising Data Subjects' rights as set forth in GDPR Chapter III, taking into account the nature of the Processing.

e) Assist the Customer with the obligations regarding Personal Data Breaches (GDPR Articles 33 and 34 and section 5 below), data protection impact assessments (GDPR Article 35), and prior consultation of the supervisory authority (GDPR Article 36), in all cases, taking into account the nature of Processing and the information available to Ortto.

f) At the Customer's discretion, return all the Customer Personal Data to the Customer after the end of the provision of Services relating to Processing, and delete existing copies (it being expressly understood that Customer has the ability to and may at its discretion export (return) all Customer Personal Data to Customer), unless applicable UK, EEA or Member State law requires Ortto to store the Customer Personal Data.

g) Provide the Customer with all information necessary to demonstrate compliance with the obligations laid down in the GDPR, and not more than once per year, allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer; provided, however: that (a) the Customer gives at least two weeks' written notice to Ortto; (b) such audit or inspection will be conducted during normal business hours and shall not interfere with Ortto operations; and (c) Customer shall not be entitled access to any information (including Personal Data) that is not Customer Personal Data and that is subject to a confidentiality obligation under law or contract, including without limitation any such obligation owed to another customer of Ortto. Notwithstanding the foregoing, Customer shall be entitled to exercise its rights under this Section 3(h) more than once per year during the term of the Agreement in the event of a Personal Data Breach or if required by a Supervisory Authority.

h) Immediately inform Customer if, in Ortto's opinion, an instruction infringes the GDPR or other UK, EEA or Member State data protection provisions; provided, however, that Ortto will not have any obligation to monitor UK, EEA or Member State data protection provisions.

4. Subprocessors

a) Ortto shall not share any Customer Personal Data with or engage any Subprocessor without prior specific or general written authorization of the Customer; provided, however, that Customer hereby specifically authorizes Ortto to Transfer Customer Personal Data to Subprocessors listed in **Exhibit A, Annex III** hereto for purpose of providing the Services, subject to the following conditions: (i) Ortto maintains a list of the Subprocessors to which it makes such Transfers and provides this list to the Customer upon written request; (ii) Ortto provides to the Customer at least 30 days' prior notice of the addition or replacement of any Subprocessor on this list so that the Customer may have an opportunity to object in writing to such addition(s) or replacement(s); and (iii) if the Customer makes such an objection on reasonable grounds and Ortto is unable to modify the Services to prevent the Transfer to the additional Subprocessor, the Customer shall have the right to terminate the relevant Processing. In addition, Orttowill impose on any Subprocessor the data protection obligations as set out in this Addendum. Where a Subprocessor fails to fulfill its data protection obligations, Ortto shall remain fully liable to the Customer for the performance of the Subprocessor's obligations.

b) Consistent with its obligations under the Privacy Shield Framework, Ortto shall require that any Subprocessor self-certifies to the Privacy Shield Framework or another mechanism permitted by Data Protection Laws for Transfers and Processing of Personal Data to a Third Country, or will ensure that any Subprocessor is obliged to provide adequate privacy and personal data protections for the Customer Personal Data that are no less protective than those required by the Privacy Shield Principles.

5. Transfers

a) Customer instructs Orttoto Transfer Customer Personal Data outside the UK or EEA as required to perform the Services, as set forth in this Addendum.
b) Customer and each Customer Affiliate (each as "data exporter") and Ortto("data importer"), with effect from the commencement of the relevant transfer, hereby enter into (i) the Module 2 SCC in respect of any Restricted Transfer from Customer or any Customer Affiliate to Ortto governed by GDPR; and/or (ii) the UK SCC in respect of any Restricted Transfer from Customer or any Customer Affiliate to Ortto governed by UK Data Protection Law; each of which is expressly incorporated herein.
c) The Parties agree that with respect to the Module 2 SCC:

1) Clause 7 – *Docking clause* shall apply;

2) In Clause 9 – *Use of subprocessors*, "Option 2"shall apply and the "time period" shall be 30 days;

3) In Clause 11(a) – *Redress,* the optional language shall not apply;

4) In Clause 13(a) – *Supervision,* the following shall be inserted: [[*Where the data exporter is established in an EU Member State*:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.] ***OR*** [*Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:*] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.] ***OR*** [*Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679*:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.]

5) In Clause 17 – *Governing law,* ["Option 1"] ["Option 2"] shall apply and the "Member State" shall be [*specify Member State*];

6) In Clause 18 – *Choice of forum and jurisdiction*, the Member State shall be [*insert Member State*];

7) Annex I shall be deemed populated with the relevant sections of Annex I to this Addendum;

8) Annex II shall be deemed populated with the relevant sections of Annex II to this Addendum.

d) The Parties agree that with respect to the UK SCC:

1) Appendix 1 shall be deemed populated with the relevant sections of Annex I to this Addendum and the processing operations are deemed to be those described in the Agreement; and

2) Appendix 2 shall be deemed populated with the relevant sections of Annex II to this Addendum.

e) If at any time the UK Government approves the Module 2 SCC for use under UK Data Protection Laws, the provisions of Section 5.(c) shall apply in place of Section 5.(d) in respect of Restricted Transfers subject to UK Data Protection Laws, subject to any modifications to the Module 2 SCC required by the UK Data Protection Laws (and subject to the governing law being English law and the Supervisory Authority being the Information Commissioner's Office).

f) If, at any time, a Supervisory Authority or a court with competent jurisdiction over a Party mandates that Transfers from Controllers in the EEA or the UK to Processors established outside the EEA or the UK must be subject to specific additional safeguards (including but not limited to specific technical and organizational measures), the Parties shall work together in good faith to implement such safeguards and ensure that any Transfer of Customer Personal Data is conducted with the benefit of such additional safeguards.

g) Ortto has certified its adherence to the Privacy Shield Framework. Ortto represents and warrants that (i) its Privacy Shield certification covers the Customer Personal Data that Orttoreceives or accesses in the United States, and that it will maintain its Privacy Shield certification throughout the term of the Agreement; (ii) it will process Customer Personal Data covered by Privacy Shield in accordance with Privacy Shield principles, including as relate to onward transfers; (iii) it will submit to the investigatory and other jurisdiction of the U.S. Federal Trade Commission and/or data protection authorities in the EU, to the extent that such investigatory and other jurisdiction would apply to Ortto under the Privacy Shield Framework; and (iv) as applicable, based on the nature of the processing, it agrees to assist the Customer in responding to individuals exercising their rights under the Privacy Shield. Ortto agrees to immediately notify the Customer if it determines that it can no longer meet its obligations under the Privacy Shield.

6. Personal Data Breaches

Ortto shall promptly and thoroughly investigate all allegations of unauthorized access to, use or disclosure of Customer Personal Data. In accordance with GDPR Article 33, paras. (1) and (2), Ortto will notify Customer without undue delay in the event of any Personal Data Breach.

7. Conflicting Terms

This Addendum supplements, and does not replace, any existing obligations related to the privacy and security of Customer Personal Data as already set forth in the Agreement. In the event of a conflict between the terms of this Addendum and the Agreement, Ortto shall comply with the obligations that provide the most protection for Customer Personal Data, in particular, in terms of security. In the event of any conflict or inconsistency between the terms of the Agreement or this Addendum, and the terms of an agreement governing Transfer outside the UK

or EEA entered into pursuant to Section 5 herein, the applicable clauses of the agreement governing Transfer entered into Section 5 herein shall control.

8. Survival

Notwithstanding anything to the contrary in the Agreement, the obligations pursuant to this Addendum shall survive termination of the Agreement for as long as Ortto holds or Processes Customer Personal Data on behalf of the Customer.

Accepted and agreed to as of the Effective Date by the authorized representative of each party:

CUSTOMER	**AUTOPILOTHQ, INC.**
Customer Name:	Signature:_____
Signature: _____	Print Title:_____
Date:_____	Date: _____

Exhibit A

Description of Processing and Security Measures

This Exhibit A includes certain details of the Processing of Customer Personal Data as required by the SCC and by GDPR Article 28(3).

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): Controller

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

The data importer is: AutopilotHQ, Inc.

Address: 1390 Market Street, Suite 200 San Francisco CA 94102 USA

Contact person's name, position and contact details: Matt Fitzsimons, Head of Finance, privacy@ortto.com

Activities relevant to the data transferred under these Clauses: A United States-based provider of services which provides online services to its customers that permit customers to engage with their customers using omnichannel communication methods

Signature and date: ...

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

The obligations and rights of Customer and Customer Affiliates

The obligations and rights of Customer and Customer Affiliates are set out in the Agreement and in this Addendum.

Subject matter and duration of the Processing of Customer Personal Data

Ortto's Processing of the Customer Personal Data is done in connection with the Customer's use of the Services. Customer allows Orttoto retain Personal Data related to the Services beyond the termination of Services, but Orttoagrees to delete any retained Personal Data at the request of the Customer (it being expressly understood that Customer has the ability to, and may at its discretion, export (return) all Customer Personal Data to Customer at any time).

The nature and purpose of the Transfer and Processing of Customer Personal Data; Processing operations

Ortto's Processing of the Customer Personal Data is done for the express purpose and to the extent necessary to provide the Services.

Categories of data subjects whose personal data is transferred / processed

Customers, employees and agents of Customers, and/or end users of Customers' services.

Categories of personal data transferred; Types of Customer Personal Data to be Processed

May include IP addresses, names, e-mail addresses, or other personal contact information uploaded to our Service by the Customer, or its employees and agents, or via the Customer's Sites and their use of our Services.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Determined by the Customer's use of the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data will be retained up to 30 days after the Customer ceases use of the Services.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Ortto's transfer of the Customer Personal Data to Subprocessors is done for the express purpose and to the extent necessary to provide the Services.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13 of the Module 2 SCC

[*specify Member State*]

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES

Description of the technical and organisational measures implemented by the Contracted Processors (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

See the measures set forth at https://journeys.autopilotapp.com/legal/security-policy.

Measures of pseudonymisation and encryption of personal data

- Personal data is encrypted using AES-256

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- SOC2 certification (pending)
- Continuous scanning through Vanta

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

- Monitoring for backups
- Routine testing of restore processes
- Documented restore processes

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- Routine testing of processes
- Logging of access to customer instances

Measures for user identification and authorisation

- Username and password authentication with optional two factor authentication
- Application user roles and permissions (Admin, Creator, Manager, Read Only)

Measures for the protection of data during transmission

- Use industry standard encryption for data being transmitted over public networks (i.e. HTTPS/TLS/SSL)
- Access to data requires authentication and authorization

Measures for the protection of data during storage

- Data is backed up to a remote location daily
- Access to data requires authentication and authorisation

Measures for ensuring physical security of locations at which personal data are processed

- https://aws.amazon.com/compliance/data-center/controls/
- No data is stored on-premise or backed up physically

Measures for ensuring events logging

- Alerts when logging is not running
- Automated testing

Measures for ensuring system configuration, including default configuration

- Use of infrastructure as code tools (i.e. Terraform)
- Regular scanning and alert of changes to system configuration
- Vanta infrastructure scanning

Measures for internal IT and IT security governance and management

- Use of infrastructure as code tools (i.e. Terraform)
- Code reviews
- Accountability and auditing based deployments

Measures for certification/assurance of processes and products

- Vanta scanning
- Vendor assessments

Measures for ensuring data minimisation

- Only personally identifiable information collected are name, email, business name and website
- Data ingested by integrations are customisable by the customer

Measures for ensuring data quality

- Database schemas to restrict data collected to ensure consistency
- Data is siloed to its system/source

Measures for ensuring limited data retention

- Backups are kept for 29 days

- Data is deleted the moment it has been consumed/processed

Measures for ensuring accountability

- Logging of access to customer instances
- Logging of changes to applications

Measures for allowing data portability and ensuring erasure

- Use of industry standard data storage options to allow for portability to different providers and environments
- Actions to delete data by customers through the application are actioned immediately

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

- Follow subprocessor's DPA practices

Annex III

List of Subprocessors (Clause 9(a), option 2)

			Location of Data	
Company	**HQ Address**	**Support Contact**	**Uses Amazon Web Services?**	**Server Location**
Amazon Web Services, Inc.	1200 12th Avenue South, Suite 1200, Seattle, WA 98144	https://aws.amazon.com/contact-us/	Yes	AWS US East 2 (Ohio)
MailUp, Inc.	450 Townsend St., San Francisco, CA 94107	support@beefree.io	Yes	EU-West (Ireland)
Elastic Cloud	800 West El Camino Real, Suite 350 Mountain View CA 94040	info@elastic.co	Yes	AWS US East 2 (Ohio)
Google Cloud Platform	1600 Amphitheatre Parkway Mountain View, CA 94043	https://cloud.google.com/support/	No	us-central1 (Iowa)
MongoDB	100 Forest Avenue, Palo Alto CA 94301	https://support.mongodb.com/welcome	Yes	United States
SendGrid, Inc.	1801 California Street, Denver, CO 80202	https://support.sendgrid.com/hc/en-us	No	East Coast (Virginia) & West Coast (Las Vegas)
Twilio Inc.	375 Beale St, Suite 300, San Francisco, CA 94105	support@twilio.com	No	East Coast (Virginia) & West Coast (Oregon)
HelpScout.	1019 Market St, San Francisco, CA 94103	https://www.helpscout.com/contact/	Yes	
Recurly	400 Alabama Street, Suite 202 San Francisco, CA 94110	https://support.recurly.com/hc/en-us	Yes	United States