GDPR DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**Addendum**") forms part of the agreement, as updated from time to time, between Drift and Customer governing Customer's use of Drift's service, whether under Drift's Terms of Service available at https://www.drift.com/terms-of-service/, or, if executed, separate Terms of Service or Master Subscription Agreement ("**Agreement**"). The effective date of this Addendum is the later of (i) the date of the final signature hereto; or (ii) May 25, 2018.

This Addendum regulates only the Processing of Personal Data subject to EU Data Protection Law for the Purposes (as defined in Annex 2) by the Parties in the context of the Service. The terms used in this Addendum have the meaning set forth in this Addendum. Except as modified below, the Agreement remains in full force and effect. Annexes 1, 2, and 3 form an integral part of this Addendum.

The Parties agree that the terms and conditions set out below are added as an Addendum to the Agreement.

1. Definitions. The following terms have the meanings set out below for this Addendum:

1.1. "Controller" means the entity which alone or jointly with others determines the purposes and the means of the Processing of Personal Data.

1.2. "Data Subject" means a natural person whose Personal Data are processed in the context of this Addendum.

1.3. "EU Data Protection Law" means the EU General Data Protection Regulation 2016/679 (as amended and replaced from time to time) and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC, and as amended and replaced from time to time) and its national implementing legislation.

1.4. "Personal Data" means any information relating to an identified or identifiable natural person. 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.

1.5. "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.6. "Privacy Shield" means the EU-U.S. Privacy Shield framework created by the U.S. Department of Commerce ("DoC") and the European Commission, and the Swiss-U.S. Privacy Shield framework created by the DoC and the Swiss government.

1.7. "Processor" means the entity that processes Personal Data on behalf of a Controller.

1.8. "Processing of Personal Data" (or "Processing/Process") means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.9. "Service" has the meaning in the Agreement.

1.10. "Standard Contractual Clauses" means the standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection set out in the European Commission's decision (C(2010)593) of 5 February 2010, as attached hereto as Annex 4.

1.11. "Sub-Processor" means the entity engaged by the Processor or any further sub-contractor to Process Personal Data on behalf of and under the instructions of the Controller.

1.12. "Third Countries" means all countries outside of the scope of the data protection laws of the European Economic Area ("EEA"), excluding countries approved as providing adequate protection for Personal Data by the European Commission from time to time.

2. Roles of the Parties. For the purpose of this Addendum, Customer is a Controller and Drift is a Processor for the Processing of Personal Data for the Purposes (as defined in Annex 2) in the context of the Service.

3. Obligations of Drift. When Processing Personal Data for the Purposes in connection with the Service, Drift:

3.1. Will only Processes Personal Data on behalf of Customer in accordance with the Customer's lawful written instructions and not for any other purposes than those specified in Annex 2 or as otherwise agreed by both Parties in writing.

3.2. Will promptly inform Customer if, in its opinion, Customer's instructions infringe EU Data Protection Law, or if Drift is unable to comply with Customer's instructions.

3.3. Will, taking into account the nature of the Processing and the information available to Drift, assist Customer in ensuring compliance with Customer's obligations under EU Data Protection Law, including data security, data breach notifications, data protection impact assessments, and prior consultations with supervisory authorities.

3.4. Will, taking into account the nature of the Processing, take appropriate technical and organizational measures to assist Customer in fulfilling Customer's obligation to respond to Data Subjects' requests to exercise their rights as provided under EU Data Protection Law. If Drift receives a request directly from a Data Subject, law enforcement agency or regulator. Drift shall, unless prohibited from doing so by applicable law (including binding terms of the request itself), notify Customer about such request and only take further action as instructed by Customer. To the extent legally permitted, Customer shall be responsible for all reasonable costs arising from Drift's provision of such assistance or compliance with such requests.

3.5. Will notify Customer when local laws prevent Drift from complying with the instructions received from Customer via this Addendum or is required to process Personal Data by law to which Drift is subject, except if such disclosure is prohibited by applicable law.

3.6. Will, at the choice and direction of the Customer after the end of the provision of the Services, delete or return all Personal Data processed under this Addendum to the Customer after the end of the provision of the Services, and delete existing copies unless EU or member state law requires storage of the Personal Data.

3.7. Will implement (and regularly test and review) internal Personal Data Breach identification, response and notification procedures in accordance with good industry practice. In the event of a Personal Data Breach relating to or affecting the Personal Data:

3.7.1. Drift shall, at its own expense, notify such Personal Data Breach to Customer without undue delay after Drift becoming aware of such Personal Data Breach; and

3.7.2. Drift shall, at its own expense: (i) co-operate with Customer's reasonable requests; and (ii) provide all information reasonably requested by Customer, in each case, as required to enable Customer to comply with EU Data Protection Law and co-operate with the directions or guidance of any Supervisory Authority.

4. **Data Transfers**. Drift shall not transfer any Personal Data to a Third Country unless the following conditions are fulfilled.

4.1. Drift complies with reasonable instructions notified to it in advance by Customer with respect to the processing of the Personal Data.

4.2. If the transfer is to Drift:

4.2.1. In the US, Drift shall maintain its certification under Privacy Shield to process such Personal Data;

4.2.2. Drift shall comply with the data importer obligations in the Standard Contractual Clauses which are hereby incorporated into and form part of this Addendum and Customer shall comply with the data exporter obligations.

4.3. If the transfer is to a Sub-Processor in a Third Country, Drift shall:

4.3.1. if the transfer is to the US, ensure that the receiving party is certified to process such Personal Data under Privacy Shield; or

4.3.2. ensure that the Sub-Processor shall comply with the data importer obligations in the Standard Contractual Clauses. For the purpose of this Section 4.3.2, Customer hereby grants Drift a mandate to execute the Standard Contractual Clauses with any relevant Sub-Processor it appoints on behalf of the Customer.

5. **Sub-Processing.**

5.1. Customer acknowledges and agrees that Drift may engage third-party Sub-Processors in connection with the performance of the Service. The Sub-Processors approved by Customer as at the date of the Agreement or this Addendum are listed in Annex 3 hereto. Drift has entered into a written agreement with each Sub-Processor containing data protection obligations not less protective than those in this Addendum with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

5.2. Customer shall, within ten days of the effective date of this Addendum, sign up via https://goo.gl/forms/bV4t9DgcSGBHmwPH2 in order to receive notifications of new Sub-Processors("**Sub-Processor Notification Process**"). Drift shall provide notification via the Sub-Processor Notification Process, of a new Sub-Processor before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

5.3. Customer may object to Drift’s use of a new Sub-processor by notifying Drift promptly in writing to legal@drift.com within ten (10) business days after receipt of Drift’s notice in accordance with the mechanism set out in Section 5.2. In the event Customer objects to a new Sub-processor, as permitted in the preceding sentence, Drift will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer’s configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-processor without unreasonably burdening the Customer. If Drift is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to the Services that cannot be provided by Drift without the use of the objected-to new Sub-Processor by providing written notice to Drift. Drift will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Service, without imposing a penalty for such termination on Customer.

5.4. Where a Sub-Processor fails to fulfill its data protection obligations, Drift shall remain fully liable to Customer for the performance of the Sub-Processor’s obligations.

5.5. With reference to Section 5(h) of the Standard Contractual Clauses, Customer acknowledges and expressly agrees that Drift may engage new Sub-processors as described in Sections 5.1 to 5.3 of this Addendum.

6. Security of the Processing; Confidentiality.

6.1. Drift will implement and maintain a comprehensive written information security program with appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including the security measures listed in Annex 1 and as appropriate: (a) the pseudonymization and encryption of Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

6.2. Drift must take steps to ensure that any person acting under its authority who has access to Personal Data is subject to a duly enforceable contractual or statutory confidentiality obligation and will not process the Personal Data except on instructions from Customer.

7. Data Protection Audit.

7.1. Customer, acting by itself or through its appointed representative (acting pursuant to an NDA approved by Drift), shall have the right during the term of the Agreement and for as long thereafter as Drift processes Personal Data regarding which Customer is a Controller, to assess compliance by Drift with the applicable requirements of the EU Data Protection Law and/or this Addendum, and to review the technical and organizational measures taken by Drift against the unauthorized or unlawful processing of Personal Data and against the unauthorized access to, accidental loss or destruction of, or damage to, Personal Data, on at least thirty (30) days’ advance notice to Drift. Before the commencement of any audit, Customer and Drift shall mutually agree upon the scope, timing, and duration of the audit, and Customer shall take all reasonable measures to limit any adverse impact thereof on Drift.

7.2. To the extent permitted by applicable law, Customer shall bear the costs and expenses incurred in respect of the parties’ compliance with their obligations under this clause, unless the audit identifies that the Drift is not in compliance with the applicable requirements of the EU Data Protection Law and/or this Addendum, in which case Drift shall reimburse Customer for all reasonable costs and expenses incurred by Customer and Drift in connection with the audit.

8. Limitation of Liability.

8.1. IN NO EVENT SHALL EITHER PARTY BE LIABLE CONCERNING THE SUBJECT MATTER OF THIS ADDENDUM, REGARDLESS OF THE FORM OF ANY CLAIM OR ACTION (WHETHER IN CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE), FOR DAMAGES, IN THE AGGREGATE, IN EXCESS OF THE LIABILITY CAP SET FORTH IN THE AGREEMENT. ALL OTHER TERMS IN THE AGREEMENT RELATING TO THE RECOVERY OF LOSSES SHALL APPLY MUTADIS MUTANDI TO THE RECOVERY OF LOSSES UNDER THIS ADDENDUM.

9. Modification of this Addendum. This Addendum may only be modified by a written amendment signed by each of the Parties.

10. Termination. The Parties agree that this Addendum expires upon the termination or expiry of the Service.

11. Governing Law. This Addendum is governed by, and shall be construed in accordance with, the laws governing the Agreement.

12. Invalidity and Severability; Conflict. If any provision of this Addendum is found by any court or administrative body of competent jurisdiction to be invalid or unenforceable, the invalidity or unenforceability of such provision shall not affect any other provision of this Addendum and all provisions not affected by such invalidity or unenforceability will remain in full force and effect. In the event of any inconsistency between this Addendum and any Standard Contractual Clauses entered into by the parties, the Standard Contractual Clauses shall prevail.

Bikeschule Sauerland Anja Dransfeld und Maik Wiesegart GbR, Allehof 1, 58809 Neuenrade, Germany (“Customer”)	**Drift.com, Inc. (“Drift”)**
Signature: M. Wiesegart	Signature:
Name: Maik Wiesegart	Name: William Collins
Title: Owner	Title: VP of Operations

ANNEX 1 – Data Security Measures

Drift will, as a minimum, implement the following types of security measures:

1. When Processing Personal Data on behalf of Customer in connection with the Services, Drift has implemented and will maintain appropriate technical and organizational security measures for the Processing of such data, including the measures specified in this Section to the extent applicable to Drift's Processing of Personal Data. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of processing. Additional information concerning such measures may be specified in the Agreement.

2. Physical Access Control. Drift employs measures designed to prevent unauthorized persons from gaining access to data processing systems in which Personal Data is processed, such as the use of security personnel, secured buildings and data center premises.

3. System Access Control. The following may, among other controls, be applied depending upon the particular Services ordered: authentication via passwords and the logging of access on several levels. For Services: (i) log-ins to Services Environments by Drift employees (ii) logical access to data centers is restricted and protected by firewall/VLAN.

4. Transmission Control. All messages and files sent through Drift are encrypted. Except as otherwise specified for the Services, transfers of data outside the Service environment are also encrypted.

5. Input Control. The Personal Data source is under the control of the Customer and is managed by secured file transfer (i.e., via web services or entered into the application) from the Customer. Note that some Services permit Customers to use unencrypted file transfer protocols. In such cases, Customer is solely responsible for its decision to use such unencrypted field transfer protocols.

6. Data Backup. Back-ups are taken on a regular basis; back- ups are secured using a combination of technical and physical controls, depending on the particular Service.

7. Data Segregation. Personal Data from different Drift customers' environments is logically segregated on Drift's systems.

ANNEX 2 – Description of the Processing Activities

This Annex 2 describes the Processing by Drift under the Addendum.

Subject-matter of the Processing

The performance of the Service pursuant to the Agreement.

Nature and Purpose of the Processing

Processing Personal Data on behalf of and in accordance with Customer's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by Data Subjects as required under EU Data Protection Law; and (iii) Processing to comply with other documented, reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement.

Types of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title, work department, and manager/supervisor name
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- Photographs
- Biographical and directory information, including linked social media profile or posts
- IDs and login credentials for use of the Services
- Identifiers related to work or personal devices used to access data exporter's IT systems
- Log information generated through the use of data exporter's IT systems
- Actions performed by the employee while accessing or using the Services
- IP address
- localization data

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer's representatives including employees, contractors, collaborators, and advisors of data exporter (who are natural persons).
- Customer's end-user customers, prospects, and partners, including employees, contractors, collaborators, and advisors of such end-user customers, prospects, and partners (who are natural persons).

Duration of the Processing

Until directed by Customer to end Processing.

ANNEX 3 – Approved Subprocessors

Name	Nature of Processing	Location
Message Systems, Inc. (DBA Sparkpost) 9130 Guilford Road Columbia, MD 21046	Provision of email delivery services.	USA
Amazon Web Services P.O. Box 81226 Seattle, WA 98108-1226	Cloud infrastructure.	USA
Segment Segment.io, Inc. 100 California Street, Suite 700 San Francisco, CA 94111	Customer Data facilitation.	USA
Sendgrid, Inc. 1801 California Street, Suite 500 Denver, Colorado 80202 U.S.A.	Provision of email delivery services.	USA
Salesforce.com The Landmark @ One Market Street San Francisco, CA 94105m USA	Customer Relationship Management platform.	USA
Pandadoc 153 Kearny St; 5th Floor San Francisco, CA 94108	Document management.	USA

Annex 4

DATA PROCESSING AGREEMENT
(EU Standard Contractual Clauses)

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organization: [ ]

Address: [ ]
Tel.: [ ] fax: [N/A] e-mail: [ ]
Other information needed to identify the organisation:
………
(the data **exporter)**

And

Name of the data importing organisation: Drift.com, Inc.

Address: 3 Copley Place, 7th Floor, Boston, MA 02116

Tel.: 855-266-1567 fax: + N/A; e-mail: legal@drift.com

Other information needed to identify the organisation: Not applicable
(the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions
For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law**'** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data

subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
Name (written out in full): [ ]
Position: [ ]
Address: [ ]

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): William Collins
Position: VP of Operations

Address: Drift.com, Inc., 3 Copley Place, 7th Floor, Boston, MA 02116

Other information necessary in order for the contract to be binding (if any):

Signature……………………………………….

(stamp of organisation)

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

Data Exporter is the legal entity that has executed the Standard Contractual Clauses as a Data Exporter.

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

Data Importer is a provider of enterprise cloud computing solutions that processes personal data upon the instruction of the data exporter.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Data Exporter's representatives including employees, contractors, collaborators, and advisors of data exporter (who are natural persons).
- Data Exporter's end-user customers, prospects, and partners, including employees, contractors, collaborators, and advisors of such end-user customers, prospects, and partners (who are natural persons).

Categories of data

The personal data transferred concern the following categories of data (please specify):

Data exporter may submit Personal Data to the Services, the extent of which is determined and controlled by the data exporter in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title, work department, and manager/supervisor name
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- Photographs
- Biographical and directory information, including linked social media profile or posts
- IDs and login credentials for use of the Services
- Identifiers related to work or personal devices used to access data exporter's IT systems
- Log information generated through the use of data exporter's IT systems
- Actions performed by the employee while accessing or using the Services
- IP address
- localization data

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify): None.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

The objective of Processing of Personal Data by data importer is the performance of the Services pursuant to the Agreement.

DATA EXPORTER:

Name: [ ]

Authorised Signature ………………………………………

DATA IMPORTER: Drift.com, Inc.

Name: William Collins

Authorised Signature:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

1. When Processing Personal Data on behalf of Customer in connection with the Services, Drift has implemented and will maintain appropriate technical and organizational security measures for the Processing of such data, including the measures specified in this Section to the extent applicable to Drift’s Processing of Personal Data. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of processing. Additional information concerning such measures may be specified in the Agreement.

2. Physical Access Control. Drift employs measures designed to prevent unauthorized persons from gaining access to data processing systems in which Personal Data is processed, such as the use of security personnel, secured buildings and data center premises.

3. System Access Control. The following may, among other controls, be applied depending upon the particular Services ordered: authentication via passwords and the logging of access on several levels. For Services: (i) log-ins to Services Environments by Drift employees (ii) logical access to data centers is restricted and protected by firewall/VLAN.

4. Transmission Control. All messages and files sent through Drift are encrypted. Except as otherwise specified for the Services, transfers of data outside the Service environment are also encrypted.

5. Input Control. The Personal Data source is under the control of the Customer and is managed by secured file transfer (i.e., via web services or entered into the application) from the Customer. Note that some Services permit Customers to use unencrypted file transfer protocols. In such cases, Customer is solely responsible for its decision to use such unencrypted field transfer protocols.

6. Data Backup. Back-ups are taken on a regular basis; back- ups are secured using a combination of technical and physical controls, depending on the particular Service.

7. Data Segregation. Personal Data from different Drift customers’ environments is logically segregated on Drift’s systems.

DATA EXPORTER:

Name: [ ]

Authorised Signature ……………………………………….

DATA IMPORTER: Drift.com, Inc.

Name: William Collins

Authorised Signature: ………………………………………………..