37SIGNALS DATA PROCESSING ADDENDUM
(*Last updated April 20, 2023*)

This Data Processing Addendum together with its Schedules and Appendices (**"DPA"**) forms a part of the 37signals Terms of Service and Privacy Policy, both as updated from time to time, or other applicable agreement between 37signals LLC ("**37signals**") and the customer (**"Customer"**) identified in such agreement (**"Agreement"**) for the use of 37signals' online services (**"Services"**). All capitalized terms not defined herein shall have the meaning set forth in the Agreement. To the extent of any conflict between this DPA, any previously executed data processing addendum, and the Agreement, this DPA will govern. In the event of any conflict or inconsistency between the body of this DPA on the one hand, and the UK Addendum and/or Standard Contractual Clauses (as applicable) on the other, the UK Addendum and/or Standard Contractual Clauses (as applicable) shall prevail.

Customer enters into this DPA on behalf of itself and, to the extent required under applicable Data Protection Laws and Regulations, on behalf of Customer's Authorized Affiliates. For the purposes of this DPA only, "Customer" shall include Customer and Authorized Affiliates.

This DPA reflects the parties' agreement with regard to the Processing of Personal Data. In the course of providing the Services to Customer pursuant to the Agreement, 37signals may process Personal Data on behalf of Customer, and the Parties agree to comply with the following provisions with respect to any Personal Data.

DATA PROCESSING TERMS

1. DEFINITIONS

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Authorized Affiliate" means any of Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, (b) is permitted to use the Services pursuant to the Agreement between Customer and 37signals but has not signed its own Agreement with 37signals and is not a "Customer" as defined under the Agreement, and (c) qualifies as a Controller of Personal Data Processed by 37signals.

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data, and includes "business" as defined in the CCPA.

"Customer Data" means what is described in the 37signals Privacy Policy, available at https://basecamp.com/about/policies/privacy, as "your data", "your information" or similar terms.

"Data Protection Laws and Regulations" means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including, to the extent applicable, laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom including the General Data Protection Regulation, Regulation (EU) 2016/679 ("**GDPR**"); the Swiss Federal Act on Data Protection ("**FADP**"); the United Kingdom Data Protection Act of 2018 ("**UK GDPR**"); and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and associated regulations and amendments, including, when effective, the California Privacy Rights Act amendments ("**CCPA**") and the privacy laws of other U.S. states (collectively, "**U.S. Privacy Laws**").

"Data Subject" means the identified or identifiable person to whom Personal Data relates.

"End Users" means Customer's end users such as employees, contractors, "clients" as that term is used in Basecamp, or others that Customer invites to use a 37signals Service via Customer's account.

"Personal Data" means any information that is Customer Data and that relates to (i) an identified or identifiable natural person and/or (ii) an identified or identifiable legal entity (where such information is protected similarly as personal data under applicable Data Protection Laws and Regulations).

"Processing" (including its various forms) means any operation or set of operations which is performed upon Personal Data, whether or not by automatic 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.

"Processor" means the entity that Processes Personal Data on behalf of the Controller and includes a "service provider" as defined under the CCPA.

"Security, Privacy and Architecture Documentation" means 37signals's security overview and security whitepaper, as updated from time to time and accessible at https://basecamp.com/about/policies/security and https://basecamp.com/about/policies/security/37signals%20Security%20Overview.pdf, HEY's security overview, as updated from time to time and accessible at https://www.hey.com/security/, 37signals's Privacy Policy, as updated from time to time and accessible at https://basecamp.com/about/policies/privacy, or other documentation made reasonably available by 37signals.

"Standard Contractual Clauses" means the contractual clauses annexed to the European Commission's Implementing Decision 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, located at http://data.europa.eu/eli/dec_impl/2021/914/oj, and completed as set forth in Section 11 below.

"Subprocessor" means any Processor engaged by 37signals.

"Supervisory Authority" means an independent public authority that is established by an EEA State pursuant to the GDPR, the UK's Information Commissioner's Office and/or the Swiss Federal Data Protection and Information Commissioner.

"**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the Effective Date at https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf).

2. PROCESSING OF PERSONAL DATA

2.1 **Roles of the Parties.** The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is either a Controller or Processor of Personal Data and 37signals is a Processor.

2.2 **Customer's Processing of Personal Data.** Customer shall, in its use of the Services:

2.2.1 Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations. For the avoidance of doubt, Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws and Regulations;

2.2.2 have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquires Personal Data;

2.2.3 have provided adequate notices to, and obtained valid consents from, any Data Subjects relating to the Processing (including the disclosure) of Personal Data by Customer and, as applicable, to cross-border transfers of such Personal Data; and

2.2.4 shall not, by act or omission, cause 37signals to violate any Data Protection Laws and Regulations, or notices provided to or consents obtained from Data Subjects as result of Processing the Personal Data.

2.3 **37signals's Processing of Personal Data.**

2.3.1 37signals shall treat Personal Data as confidential information and shall only Process Personal Data: (1) to fulfill its obligations to Customer under the Agreement, including this DPA; (2) on behalf of Customer and in accordance with Customer's documented instructions; and (3) in compliance with Data Protection Laws and Regulations. This DPA and the Agreement are Customer's complete and final documented instructions to 37signals for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately. For the purposes of the UK Addendum and/or Standard Contractual Clauses (as applicable), the following is deemed an instruction by the Customer to process Personal Data: (i) Processing in accordance with the Agreement; (ii) Processing initiated by Customer and/or its End Users in their use of the Services; and (iii) Processing to comply with other reasonable documented instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement and this DPA.

2.3.2 The subject matter of Processing of Personal Data by 37signals is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, and the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1.

2.3.3 Without prejudice to section 2.3.1, 37signals shall:

i. Not "sell" Personal Data or "share" Personal Data for purposes of "cross-context behavioral advertising" or "targeted advertising" as such terms are defined under U.S. Privacy Laws;

ii. Not attempt to (a) re-identify any pseudonymized, anonymized, aggregate, or de-identified Personal Data or (b) link or otherwise create a relationship between Customer Data and any other data, without Customer's express authorization;

iii. Not retain, use, or disclose Personal Data outside of the direct business relationship between Customer and 37signals;

iv. Comply with any applicable restrictions under U.S. Privacy Laws on combining Personal Data with personal data that 37signals receives from, or on behalf of, another person or persons, or that the 37signals collects from any interaction between it and a data subject; and

v. Immediately notify Customer if 37signals determines that (a) it can no longer meet its obligations under this DPA or Data Protection Laws and Regulations; (b) it has breached this DPA; or (c) in 37signals's opinion, an instruction from Customer infringes Data Protection Laws and Regulations.

2.3.4 37signals shall promptly notify Customer of any government requests for access to or information about 37signals's Processing of Personal Data on Customer's behalf unless prohibited by Data Protection Laws and Regulations. 37signals will provide Customer with reasonable cooperation and assistance in relation to any such request. If 37signals is prohibited by applicable Data Protection Laws and Regulations from disclosing the details of a government request to Customer, 37signals shall inform Customer that it can no longer comply with Customer's instructions under this DPA without providing more details and await Customer's further instructions. 37signals shall use all available legal mechanisms to challenge any demands for data access through national security process that it receives, as well as any non-disclosure provisions attached thereto.

2.3.5 37signals shall provide reasonable assistance to and cooperation with Customer for Customer's performance of a data protection impact assessment of Processing or proposed Processing of Personal Data, when required by applicable Data Protection Laws and Regulations, and at

Customer's reasonable expense.

2.3.6 37signals shall provide reasonable assistance to and cooperation with Customer for Customer's consultation with regulatory authorities in relation to the Processing or proposed Processing of Personal Data, including complying with any obligation applicable to 37signals under Data Protection Laws and Regulations to consult with a regulatory authority in relation to 37signals' Processing or proposed Processing of Personal Data.

2.3.7 37signals certifies that it understands its obligations under this DPA (including without limitation the restrictions under Section 2) and that it will comply with them.

3. DATA SUBJECT REQUESTS

37signals shall, to the extent legally permitted, promptly notify Customer if 37signals receives a request from a Data Subject to exercise the Data Subject's rights related to Personal Data under Data Protection Laws and Regulations, including the right of access, right to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability; to object to the Processing, or to assert its right not to be subject to an automated individual decision making process (**"Data Subject Request"**). Taking into account the nature of the Processing, 37signals shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, 37signals shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent 37signals is legally permitted to do so and the response is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer shall be responsible for any costs arising from 37signals's provision of such assistance.

4. 37SIGNALS PERSONNEL

4.1 **Confidentiality.** 37signals shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities, and have executed written confidentiality agreements. 37signals shall ensure that such confidentiality obligations survive the termination of the personnel engagement.

4.2 **Reliability.** 37signals shall take commercially reasonable steps to ensure the reliability of any 37signals personnel engaged in the Processing of Personal Data.

4.3 **Limitation of Access.** 37signals shall ensure that 37signals's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.

4.4 **Questions.** For questions about this DPA or any other privacy matters, please send an email to privacy@37signals.com.

5. SUBPROCESSORS

5.1 **Appointment of Subprocessors.** Customer acknowledges and agrees that 37signals may engage third-party Subprocessors in connection with the provision of the Services. 37signals has entered into a written agreement with each Subprocessor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data, to the extent such is applicable to the nature of the Services provided by such Subprocessor.

5.2 **List of Current Subprocessors and Notification of New Subprocessors.** 37signals shall make available to Customer the current list of Subprocessors for the 37signals Services on 37signals's website. 37signals shall provide notification to the Customer of a new Subprocessor(s) before authorizing any new Subprocessor(s) to Process Personal Data in connection with the provision of the applicable

Services. Customers must subscribe to the 37signals Subprocessor Github page for notification of Subprocessor changes.

5.3 **Objection Right for New Subprocessors.** Customer may object to 37signals's use of a new Subprocessor by notifying 37signals promptly in writing within ten (10) business days after receipt of 37signals's notice of a new Subprocessor in accordance with Section 5.2. In the event Customer objects to a new Subprocessor, 37signals may, at its option, 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 new Subprocessor without unreasonably burdening the Customer. If 37signals is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate with written notice to 37signals the applicable Agreement solely with respect to Services that cannot be provided by 37signals without use of the new Subprocessor. As of the effective date of termination, 37signals will refund Customer any prepaid fees such terminated Services covering the remainder of the term and will not penalize Customer for such termination.

6. SECURITY

6.1 **Controls for the Protection of Personal Data.** 37signals shall maintain appropriate technical and organizational measures to protect the security (including protection against unauthorized or unlawful Processing; accidental or unlawful destruction, loss or alteration or damage; or unauthorized disclosure of, or access to, Personal Data), confidentiality, and integrity of Personal Data, as set forth in the Security, Privacy and Architecture Documentation. 37signals will not materially decrease the overall security of the Services during a subscription term.

6.2 **Third-Party Certifications and Audits.** Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, 37signals shall make available to Customer a copy of 37signals's then most recent third-party audits or certifications, as applicable; provided, however, that this provision shall not apply if Customer or Customer's independent, third-party auditor is a competitor of 37signals.

6.3 **Unauthorized Processing of Personal Data.** Customer retains the right to take reasonable and appropriate steps to stop and remediate unauthorized Processing of Personal Data, including any Processing of Personal Data not authorized in this DPA.

7. PERSONAL DATA INCIDENT MANAGEMENT AND NOTIFICATION

37signals maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Documentation and the Agreement. 37signals shall notify Customer without undue delay, and in compliance with Data Protection Laws and Regulations, after becoming aware of the accidental or unlawful destruction, loss, alteration, or unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed by 37signals or its Subprocessors (a "**Personal Data Incident**"). 37signals shall make reasonable efforts to identify the cause of such Personal Data Incident and take those steps as 37signals deems necessary and reasonable in order to remediate the cause of such a Personal Data Incident to the extent the remediation is within 37signals's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's End Users.

8. RETURN AND DELETION OF PERSONAL DATA

Upon termination of the Agreement, 37signals shall return Personal Data to Customer and, to the extent allowed by applicable law, delete Personal Data in accordance with the procedures and timeframes specified in the Security, Privacy and Architecture Documentation.

9. AUTHORIZED AFFILIATES

9.1 **Contractual Relationship.** Each Authorized Affiliate agrees to be bound by the terms of this DPA and, to the extent applicable, the Agreement. Further, all access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement, and any violation of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a violation by Customer. For the avoidance of doubt, an Authorized Affiliate is not and does not become a party to the Agreement by Customer entering into this DPA, and is only a party to the DPA.

9.2 **Communication.** Customer shall remain responsible for coordinating all communication with 37signals under this DPA and be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

9.3 **Rights of Authorized Affiliates.** Where an Authorized Affiliate becomes a party to the DPA with 37signals, it shall, to the extent required under applicable Data Protection Laws and Regulations, be entitled to exercise the rights and seek remedies under this DPA, subject to the following:

9.3.1 Except where applicable Data Protection Laws and Regulations require that the Authorized Affiliate exercise a right or seek any remedy under this DPA against 37signals directly by itself, the parties agree that (a) only Customer shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and that (b) Customer shall exercise any such rights under this DPA in a combined manner for all of its Authorized Affiliates together (as set forth, for example, in Section 9.3.2, below), not separately for each Authorized Affiliate individually.

9.3.2 The parties agree that Customer shall, when carrying out an on-site audit of the procedures relevant to protecting Personal Data, take all reasonable measures to limit any impact on 37signals and its Subprocessors by combining, to the extent reasonably possible, several audit requests carried out on behalf of different Authorized Affiliates in one single audit.

10. LIMITATION OF LIABILITY

To the extent permitted under applicable Data Protection Laws and Regulations, each party's and all of its Affiliates' liability arising out of or related to this DPA and all DPAs between Authorized Affiliates and 37signals, whether in contract, tort or under any other theory of liability, is subject to the limitations of liability set forth in the Agreement, and such limitations apply to the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together. For the avoidance of doubt, 37signals's and its Affiliates' total liability for all claims from the Customer and all of its Authorized Affiliates arising out of or related to the Agreement and each DPA shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

11. INTERNATIONAL DATA TRANSFERS

11.1 Subject to the additional terms in Schedule 1, 37signals makes available the Standard Contractual Clauses and the UK Addendum, which shall apply to any transfers of Personal Data under this DPA from the European Economic Area and/or their member states and Switzerland, and the United Kingdom, respectively, to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are made in connection with the Processing of Personal Data under the DPA and are subject to such Data Protection Laws and Regulations.

11.2 To the extent legally required, by signing the Agreement, Customer and 37signals are deemed to have signed the Standard Contractual Clauses, which form part of this DPA and (except as described in Section 11.4 and 11.5 below) will be deemed completed as follows:

11.2.1 Module 2 of the Standard Contractual Clauses applies to transfers of Personal Data from Customer (as a controller) to 37signals (as a processor) and Module 3 of the Standard Contractual Clauses applies to transfers of Personal Data from Customer (as a processor) to 37signals (as a processor);

11.2.2 Clause 7 (the optional docking clause) is included;

11.2.3 Under Clause 9 (Use of sub-processors), the Parties select Option 2 (General written authorization);

11.2.4 Under Clause 11 (Redress), the optional language requiring that Data Subjects be permitted to lodge a complaint with an independent dispute resolution body shall not be deemed to be included;

11.2.5 Under Clause 17 (Governing law), the Parties choose Option 1 (the law of an EU Member State that allows for third-Party beneficiary rights). The Parties select the laws of Ireland;

11.2.6 Under Clause 18 (Choice of forum and jurisdiction), the Parties select the courts of Ireland;

11.2.7 Annex I(A) and I(B) (List of Parties) is completed as set forth in Schedule 1;

11.2.8 Under Annex I(C) (Competent supervisory authority), the Parties shall follow the rules for identifying such authority under Clause 13 and, to the extent legally permissible, select the Irish Data Protection Commission;

11.2.9 Annex II (Technical and organizational measures) is completed with Schedule 1 of this DPA; and

11.2.10 Annex III (List of subprocessors) is not applicable as the Parties have chosen General Authorization under Clause 9.

11.3 With respect to Personal Data transferred from the United Kingdom for which United Kingdom law (and not the law in any European Economic Area jurisdiction or Switzerland) governs the international nature of the transfer, the UK Addendum forms part of this DPA and takes precedence over the rest of this DPA as set forth in the UK Addendum. Undefined capitalized terms used in this provision shall mean the definitions in the UK Addendum. For purposes of the UK Addendum, they shall be deemed completed as follows: (a) the Parties' details shall be the Parties and their affiliates to the extent any of them is involved in such transfer; (b) the Key Contacts shall be the contacts set forth in Schedule 1; (c) the Approved Standard Contractual Clauses referenced in Table 2 shall be the Standard Contractual Clauses as executed by the Parties; (d) either Party may end this DPA as set out in Section 19 of the UK Addendum; and (e) by entering into the Agreement, the Parties are deemed to be signing the UK Addendum.

11.4 For transfers of Personal Data that are subject to the FADP, the Standard Contractual Clauses form part of this DPA as set forth in Section 7(b) of this DPA, but with the following differences to the extent required by the FADP: (1) references to the GDPR in the Standard Contractual Clauses are to be understood as references to the FADP insofar as the data transfers are subject exclusively to the FADP and not to the GDPR; (2) references to personal data in the Standard Contractual Clauses also refer to data about identifiable legal entities until the entry into force of revisions to the FADP that eliminate this broader scope; (3) the term "member state" in Standard Contractual Clauses shall not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Standard Contractual Clauses; and (4) the relevant supervisory authority is the Swiss Federal Data Protection and Information Commissioner (for transfers subject to the FADP and not the GDPR), or both such Commissioner and the supervisory authority identified in the Standard Contractual Clauses (where the FADP and GDPR apply, respectively)

11.5 Copies of Subprocessor Agreements. The parties agree that copies of the Subprocessor agreements that must be provided by 37signals to Customer pursuant to the applicable Standard Contractual Clauses or Controller to Processor Clauses, or Processor to Processor Clauses may have all commercial information or clauses unrelated to the applicable Standard Contractual Clauses, Controller to Processor Clauses, or Processor to Processor Clauses removed by 37signals beforehand; and, that such copies will be provided by 37signals, in a manner to be determined in its discretion, only upon request by Customer.

11.6 Processor to Processor Clauses. For purposes of the Processor to Processor Clauses, Customer agrees

that it is unlikely that 37signals will know the identity of Customer's Controller(s) because 37signals does not have a direct relationship with such Controller(s). Therefore, Customer will fulfill any and all of 37signals's obligations to Customer's Controller(s) under the Processor to Processor Clauses.

11.7 Audits and Certifications. The parties agree that the audits described in the UK Addendum and/or Standard Contractual Clauses (as applicable) shall be carried out in accordance with Section 6.2 of the DPA.

11.8 Certification of Deletion. The parties agree that the certification of deletion of Personal Data that is described in the UK Addendum and/or Standard Contractual Clauses (as applicable) shall be provided by 37signals to Customer only upon Customer's request.

SCHEDULE 1

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: The entity identified as Customer in the DPA or such other agreement between 37signals and Customer

Address: The Address for the Customer associated with the 37signals account

Contact person's name, position and contact details: The contact details associated with the 37signals Account

Activities relevant to the data transferred under these Clauses: The activities specified in the DPA

Signature and date: By using 37signals's services to transfer data to Third Countries, the exporter will be deemed to have signed Annex 1

Role (controller/processor): Controller, or in some instances Processor

Data importer(s):

Name: 37signals LLC

Address: 2045 W Grand Ave, Suite B, PMB 53289, Chicago, Illinois 60612, USA

Contact person's name, position and contact details: Elaine Richards, COO, elaine@37signals.com

Activities relevant to the data transferred under these Clauses: 37signals is a cloud- based software-as-a-service provider of collaboration and communication software which processes personal data upon the instruction of the data exporter in accordance with the terms of the agreement between the data exporter and 37signals.

Signature and date: By processing the data exporter's data on data exporter's instructions, the data importer will be deemed to have signed this Annex I

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data exporter and/or data subjects (as directed by data exporter), may submit personal data to the Services concerning the following categories of data subjects:

- Prospects, customers business partners and vendors (who are natural persons) of data exporter;
- Employees or contact persons of data exporter's prospects, customers, business partners and vendors;
- Employees, agents, advisors, independent contractors, members and/or freelancers of data exporter; and/or
- Other categories of data subjects as expressly determined by the data exporter.

Categories of personal data transferred

Data exporter and/or data subjects (as directed by data exporter) may submit personal data to the Services, the type, extent and detail of which is determined and controlled by the data exporter and/or the data subject in its sole discretion.

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.

Data exporter and/or data subjects (as directed by data exporter) may submit Sensitive Data to the Services, the type, extent and detail of which is determined and controlled by the data exporter and/or the data subject in its sole discretion. 37signals takes the security and privacy of data very seriously. The restrictions and safeguards that apply to all Personal Data, including any Sensitive Data, can be found in 37signals's Privacy Policy, as updated from time to time and accessible at https://basecamp.com/about/policies/privacy; security policies, as updated from time to time and accessible at https://basecamp.com/about/policies/security and https://basecamp.com/about/policies/security/37signals%20Security%20Overview.pdf, and HEY's security overview, as updated from time to time and accessible at https://www.hey.com/security/.

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

Data exporter and/or data subjects (as directed by data exporter) may submit personal data to the Services either once, or on a continuous basis (for example by making changes to personal data) as determined and controlled by the data exporter and/or the data subject in its sole discretion.

Nature of the processing

37signals processes personal data only as necessary to perform the Services and only performs the type(s) of processing as instructed by the data exporter and/or data subject and only pursuant to the Agreement, the DPA and these Clauses.

Purpose(s) of the data transfer and further processing

The purposes of the processing are determined solely by the data exporter and/or data subject in its sole discretion.

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

Subject to any other terms allowing or requiring longer retention, and subject to 37signals's normal data retention policies, 37signals only processes personal data for the duration of the Agreement, unless the data is deleted prior thereto by the data exporter and/or data subject.

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

37signals transfers Personal Data to Sub-processors as set forth in 37signals's Privacy Policy, available at https://basecamp.com/about/policies/privacy.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority will be determined in accordance with the GDPR and where possible, will be the Irish Data Protection Commissioner.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

The various measures we take 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, can be found in 37signals's Privacy Policy, as updated from time to time and accessible at https://basecamp.com/about/policies/privacy; security policies, as updated from time to time and accessible at https://basecamp.com/about/policies/security and https://basecamp.com/about/policies/security/37signals%20Security%20Overview.pdf, and HEY's security overview, as updated from time to time and accessible at https://www.hey.com/security/.

37signals establishes data processing agreements with all of its sub-processors that handle personal data, which require those sub-processors to adhere to the same, if not more stringent requirements, as 37signals. You can find out more about each sub-processor for each 37signals service here:

- For Basecamp, at https://basecamp.com/about/policies/privacy/basecamp-subprocessors;
- For HEY, at https://basecamp.com/about/policies/privacy/hey-subprocessors;
- For Highrise, at https://basecamp.com/about/policies/privacy/highrise-subprocessors;
- For Campfire, at https://basecamp.com/about/policies/privacy/campfire-subprocessors; and
- For Backpack, at https://basecamp.com/about/policies/privacy/backpack-subprocessors.