37SIGNALS DATA PROCESSING ADDENDUM
(*Last updated December 23, 2022*)

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 and its Schedules 1 and 2 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.

"CCPA" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 *et seq.* and associated regulations.

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

"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; the 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.

"GDPR" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“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.

“UK Addendum” means the UK Information Commissioner’s International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, entered into by and between Customer and 37signals and attached hereto as Schedule 3 for the international transfer of Personal Data from the UK to third countries that, according to the UK government, does not ensure an adequate level of data protection.

“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, and referring to either or both of the following as the context requires:

- **“Controller to Processor Clauses,”** meaning Module Two of the Standard Contractual Clauses, attached as Schedule 4.
- **“Processor to Processor Clauses,”** meaning Module Three of the Standard Contractual Clauses, attached as Schedule 5.

“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.

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 on behalf of Customer and in accordance with Customer's documented instructions. 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 2 (Details of the Processing).

2.3.3 Without prejudice to section 2.3.1, 37signals shall:

i. Not "sell" or "share" Personal Data 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.

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.

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.

5.4 **Liability.** 37signals shall be liable for the acts and omissions of its Subprocessors to the same extent 37signals would be liable if performing the services of each Subprocessor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

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. EUROPEAN SPECIFIC PROVISIONS

11.1 **GDPR.** 37signals will Process Personal Data in accordance with Data Protection Laws and Regulations including the GDPR requirements directly applicable to 37signals's Processing of Personal Data.

11.2 **Data Protection Impact Assessment.** Upon Customer's request, 37signals shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation under the GDPR or other Data Protection Laws and Regulations to carry out a data protection impact assessment related to Customer's use of the Services, to the extent Customer does not otherwise have access to the relevant information, and to the extent such information is available to 37signals. In addition, 37signals shall provide reasonable assistance to Customer in Customer's cooperation or prior consultation with the Supervisory Authority in performing its tasks relating to Section 11.2 of this DPA, to the extent required under the GDPR or other Data Protection Laws and Regulations.

11.3 **Transfer mechanisms for data transfers.** Subject to the additional terms in Schedule 1, 37signals makes available the 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.

List of Schedules

Schedule 1: Transfer Mechanisms for European Data Transfers
Schedule 2: Details of the Processing
Schedule 3: UK International Data Transfer Addendum
Schedule 4: Controller to Processor Clauses
Schedule 5: Processor to Processor Clauses

SCHEDULE 1
ADDITIONAL TERMS APPLICABLE TO TRANSFER MECHANISMS FOR EUROPEAN DATA TRANSFERS

1. **Customers covered.** The UK Addendum and/or Standard Contractual Clauses (as applicable) and the additional terms specified in this Schedule 1 apply to (a) the Customer as identified in the DPA and its End Users and (b) all Customer Affiliates, including, but not limited to, End Users of Customer established within the European Economic Area, Switzerland and the United Kingdom, that have entered into the DPA and/or the Agreement. For the purpose of the UK Addendum and/or the Standard Contractual Clauses (as applicable) and this Schedule 1, the aforementioned entities shall be deemed "data exporters."

2. **Appointment of new Subprocessors and List of current Subprocessors.** Customer acknowledges and expressly agrees that (a) 37signals's Affiliates may be retained as Subprocessors; and (b) 37signals and 37signals's Affiliates respectively may engage third-party Subprocessors in connection with the provision of the Services. The list of current Subprocessors for each 37signals product can be found at the following webpages:

- 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.

3. **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 UK Standard Contractual Clauses or Controller to Processor Clauses, or Processor to Processor Clauses may have all commercial information or clauses unrelated to the applicable UK 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.

4. **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.

5. **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.

6. **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 2
DETAILS OF THE PROCESSING

1. **Nature and Purpose of Processing.** 37signals will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the DPA, and as further instructed by Customer in its use of the Services.

2. **Duration of Processing.** Subject to Section 8 of the DPA, 37signals will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing.

3. **Categories of Data Subjects.** Customer may submit Personal Data to the Services, the categories, extent and detail of which are determined and controlled by Customer in its sole discretion.

4. **Types of Personal Data.** Customer may submit Personal Data to the Services, the type, extent and detail of which are determined and controlled by Customer in its sole discretion.

SCHEDULE 3
UK INTERNATIONAL DATA TRANSFER ADDENDUM

Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	The effective date of the Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: As identified in the Agreement. Trading name (if different): If any, as identified in the Agreement. Main address (if a company registered address): As provided in the Agreement. Official registration number (if any) (company number or similar identifier): N/A	Full legal name: 37signals LLC Trading name (if different): N/A Main address (if a company registered address): 2045 W Grand Ave, Suite B, PMB 53289, Chicago, Illinois 60612, USA Official registration number (if any) (company number or similar identifier): N/A
Key Contact	Full Name (optional): Job Title: Contact details including email: *See contact details in the Agreement.*	Full Name (optional): Elaine Richards Job Title: COO Contact details including email: elaine@37signals.com
Signature (if required for the purposes of Section 2)	By signing the Agreement, the Exporter is deemed to have signed this Addendum, if required	By signing the Agreement, the Importer is deemed to have signed this Addendum, if required.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: The effective date of the Agreement. Reference (if any): Schedule 4 or 5 of the DPA, as applicable. Other identifier (if any): N/A Or □ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information that must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the parties), and which, for this Addendum, is set out in:

Annex 1A: List of Parties: The Appendix to Schedule 4 or 5 of the DPA, as applicable.

Annex 1B: Description of Transfer: The Appendix to Schedule 4 or 5 of the DPA, as applicable.

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: The Appendix to Schedule 4 or 5 of the DPA, as applicable.

Annex III: List of Sub processors (Modules 2 and 3 only): Inapplicable because the parties choose Option 2 for Clause 9 of the EU SCCs; but for a list of 37signals's subprocessors, see Schedule 1of the DPA.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved	Which Parties may end this Addendum as set out in Section 0 below: ☒ Importer

Addendum changes	☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows Data Subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 17.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.

Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws apply.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 9 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
    b. Sections 0 to 10 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed to alternative amendments which meet the requirements of Section 0, the provisions of Section 14 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

15. The following amendments are made to the Addendum EU SCCs (for the purpose of Section 0):

    a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

    b. In Clause 2, delete the words:

       "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

       "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

       "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

       "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

    g. References to Regulation (EU) 2018/1725 are removed;

    h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

    i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

    j. Clause 13(a) and Part C of Annex I are not used;

    k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

    l. In Clause 16(e), subsection (i) is replaced with:

       "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

    m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or

    b. reflects changes to UK Data Protection Laws;

    The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 17, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes" will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in (i) its direct costs of performing its obligations under the Addendum; and/or (ii) its risk under the Addendum, and in either case it has first taken reasonable steps to reduce those costs or risks so that they are not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

SCHEDULE 4
CONTROLLER TO PROCESSOR CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer") have agreed to these standard contractual clauses (hereinafter: "Clauses").

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

  (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

  (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1(b) and Clause 8.3(b);

  (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

  (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

  (v) Clause 13;

  (vi) Clause 15.1(c), (d) and (e);

  (vii) Clause 16(e);

  (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Not used

<u>SECTION II – OBLIGATIONS OF THE PARTIES</u>

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter **“Sensitive Data”**), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non- material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) 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.

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.

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 behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

<u>SECTION IV – FINAL PROVISIONS</u>

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.
In these cases, it shall inform the competent supervisory authority of such non- compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Denmark.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

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

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.

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.

SCHEDULE 5
PROCESSOR TO PROCESSOR CLAUSES

SECTION I

Clause 1

Purpose and scope

(e) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[5] for the transfer of personal data to a third country.

(f) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

have agreed to these standard contractual clauses (hereinafter: "Clauses").

(g) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(h) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(c) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(d) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

[5] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision […].

Clause 3

Third-party beneficiaries

(c) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1(b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(d) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(d) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(e) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(f) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Not used

<u>SECTION II – OBLIGATIONS OF THE PARTIES</u>

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter.[6]

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal

[6] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 **Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 **Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter **"Sensitive Data"**), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 **Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[7] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

[7] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

Use of sub-processors

(a) The data importer has the controller's general authorisation for the engagement of sub- processor(s) from an agreed list. The [8]data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub- processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub- processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

Clause 11

Redress

(g) The data importer shall inform data subjects in a transparent and easily accessible format, through

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(h) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(i) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(j) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(k) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(l) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(h) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(i) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(j) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non- material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(k) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(l) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(m) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(n) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(c) 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.

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.

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 behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(d) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(g) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(h) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;[9]

[9] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant,

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(i) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(j) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(k) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(l) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.3 Notification

(f) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

(g) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(h) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.]

(i) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(j) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.4 Review of legality and data minimisation

(d) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(e) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(f) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(f) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(g) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(h) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(i) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(j) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

(e) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(f) The Parties agree that those shall be the courts of Denmark.

(g) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(h) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

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): 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 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.

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.