

This MASTER AGREEMENT ("Agreement") is made and entered into as of _____ ("Effective Date") by and between Haplo Services, LTD, a Delaware limited liability company located at Rm 4.10, 201 Borough High Street, London, SE1 1JA ("Cayuse"), and _____, a _____ located at _____ ("Customer"). Cayuse and Customer are each referred to herein as a "Party" and are collectively referred to herein as the "Parties." In consideration of the mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt, sufficiency, and adequacy of which are hereby acknowledged, the Parties hereby agree as follows:

1. ORDERING

Pursuant to this Agreement, Customer may order from Cayuse (a) licenses to access and use one or more of Cayuse's proprietary research administration and grant management software solution modules to be hosted and made available by Cayuse on a software-as-a-service basis, including related APIs (the "Subscription Service"), and/or (b) related training, implementation and/or other professional services (collectively, "Professional Services"). The specifics of each Customer order will be set forth on one or more written or electronic quotations, order form(s) and/or other documents provided by Cayuse (each, an "Order Form") that reference this Agreement and are agreed upon by both Parties. Any Customer Affiliate (as defined below) may enter into an Order Form with Cayuse under this Agreement and, solely with respect to such Order Form, such Customer Affiliate shall become a party to this Agreement and all references to Customer in this Agreement shall be deemed to refer to such Customer Affiliate. Each Order Form is a separate obligation of Customer or the Customer Affiliate, as applicable, and no other Customer Affiliate has any obligation related to, or right to access, the Subscription Service under such Order Form. For purposes of this Agreement, a "Customer Affiliate" shall mean any party that: (i) directly or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with Customer; or (ii) is part of an affiliated education system or group of educational institutions with Customer. All Order Forms are incorporated herein by reference.

2. SUBSCRIPTION SERVICE ACCESS, SUPPORT AND RESTRICTIONS

2.1 License to Subscription Service. Subject to the terms and conditions of this Agreement and the payment of all applicable Fees (as defined below), Cayuse hereby grants Customer a limited, non-transferable, non-sublicensable, non-exclusive license, during the Subscription Term (as defined below), to permit any of Customer's user(s) who are authorized by the Customer and Cayuse to use the Subscription Service ("End Users") to access and use the Subscription Service solely for Customer's internal business purposes.

2.2 Limitations on License. Customer shall not: (a) modify or make derivative works based on the Subscription Service; (b) use the Subscription Service in a manner not authorized under the documents, agreements, user manuals and any technical publications and specifications, as applicable, made generally available by Cayuse to customers relating to the operation and use of the Subscription Service ("Documentation") or in violation of any applicable law, rule or regulation, including any export/import laws; (c) distribute, transfer, grant sublicenses, or otherwise make available the Subscription Service (or any portion thereof) to other than End Users, including, but not limited to, making the Subscription Service available as an application service provider, service bureau, or rental source; (d) remove any product identification or other notices contained in the Subscription Service; or (e) reverse engineer the Subscription Service for any reason or access the Subscription Service to (i) build a competitive product or service, (ii) build a product using similar ideas, features, functions, or graphics of the Subscription Service, or (iii) copy any ideas or features. The Subscription Service is a "commercial item," as that term is defined at 48 C.F.R. 2.101 (OCT 1995), and more specifically is "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (SEPT 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (JUNE 1995), the Subscription Service is provided to U.S. Government End Users (i) only as a commercial end item and (ii) with only those rights as are granted to all other end users pursuant to the terms and conditions herein.

2.3 Support and Maintenance. Cayuse will provide support and maintenance services for the Subscription Service in accordance with the Cayuse Maintenance and Support Policy attached hereto as Appendix 1

("Support Services").

2.4 Unauthorized Access. Customer shall promptly notify Cayuse of any unauthorized use, copying or disclosure of the Subscription Service of which it becomes aware and further agrees to take such commercially reasonable measures necessary to end and prevent any such further use, copying and disclosure.

2.5 Breach of License. Cayuse, in its sole and exclusive discretion, may immediately terminate this Agreement in the event Customer or any End User violates the license grants made herein or any provision of this Section 2. Each Party acknowledges and agrees that any breach of this Section 2 by Customer or an End User shall cause immediate and irreparable injury to Cayuse, and in the event of such breach, Cayuse shall be entitled to seek and obtain injunctive relief, without bond or other security, and all other remedies available at law and in equity.

3. PROFESSIONAL SERVICES

3.1 Generally. In the event that Customer also requires related Professional Services, the parties will execute one or more statements of work (each, an "SOW"). All SOWs are incorporated herein by reference. Cayuse will provide all Professional Services and related deliverables ("Deliverables") in accordance with the specifications and schedule, if any, set forth in each SOW. If Customer notifies Cayuse in writing within thirty (30) days after the Deliverables are made available to Customer that Cayuse is not in compliance with the foregoing covenant with respect to such Deliverables, then Cayuse will, as Customer's sole and exclusive remedy and Cayuse's sole liability, use commercially reasonable efforts to cause the Deliverables to conform to such covenant at no additional cost to Customer.

3.2 Customer Personnel, Facilities and Resources. If applicable to any Professional Services, Customer will provide Cayuse with timely access to appropriate Customer personnel and will arrange for Cayuse personnel to have suitable and safe access to Customer's facilities and applicable systems. Customer will also provide suitable office space and associated resources for Cayuse personnel working on-site, including all necessary computing and office support resources, and will undertake any other responsibilities described in the applicable SOW. An SOW may also specify those tasks, activities or resources for which Customer is responsible and, if applicable, those tasks, activities and resources that will be performed jointly by Customer and Cayuse.

3.3 Approvals and Information. Customer will respond promptly to any request by Cayuse for information, approvals, decisions or authorizations that are needed by Cayuse to perform the Professional Services. Cayuse may also describe the course of action Cayuse intends to follow if it does not receive a timely response from Customer, which may include suspension of the affected Professional Services. Cayuse may follow the described course of action in the absence of a timely response from Customer. Any subsequent change requested by Customer will be subject to mutual agreement and may result in a change order to the SOW ("Change Order").

3.4 Changes to SOWs. Either party may propose changes to the Professional Services under an applicable SOW. Requests for changes will be submitted to the other party in writing for consideration of feasibility and the likely effect on the fees and the Professional Services. The parties will document any agreed upon changes in mutually executed Change Orders.

3.5 Proceeding on Oral Instructions. Cayuse may proceed with and be compensated for performing changed work for a period of up to thirty (30) calendar days if Cayuse receives an oral instruction to proceed from Customer's authorized representation and Cayuse sends a written confirmation of the oral instruction to Customer.

3.6 Customer Delays. If action or inaction by Customer, or its suppliers' failure to perform their responsibilities in a timely manner, delays or prevents Cayuse from performing the Professional Services or Custom Development, Cayuse will be entitled to a Change Order documenting an equitable adjustment in the schedule for performance and the Fees under the applicable SOW.

4. INTELLECTUAL PROPERTY

4.1 Protection of Proprietary Rights. Customer acknowledges and agrees that the Subscription Service is a commercially valuable asset of Cayuse, the development of which required the investment of substantial time, effort, and cost by Cayuse. Customer further acknowledges and agrees that the Subscription Service contains trade secrets of Cayuse and that it is Cayuse's Confidential Information (as defined below) and is proprietary to Cayuse. Accordingly, Customer hereby agrees that it and

its End Users will use the highest degree of care to maintain the confidentiality of the Subscription Service.

4.2 **Subscription Service Ownership.** As between Customer and Cayuse, Cayuse shall retain all right, title and interest in and to the Subscription Service, including all output and executables of the Subscription Service, all updates and/or upgrades thereto, and the Documentation. Except for the license granted in Section 2.1, this Agreement does not grant Customer any right, title, or interest in any intellectual property owned by or licensed to Cayuse, including Subscription Service. Customer agrees to abide by all applicable proprietary rights laws and other laws, as well as any additional copyright notices and restrictions contained in this Agreement.

4.3 **Deliverable Ownership.** Unless expressly stated otherwise in an SOW and excluding any Customer trademarks, service marks and other logos, as between Customer and Cayuse, Cayuse will retain all right, title and interest in and to all Deliverables and Customer hereby irrevocably assigns to Cayuse any and all ownership rights it may have in or to such Deliverables. Customer's rights to the Deliverables shall be the same as the rights granted to Customer under the Agreement with respect to the Subscription Services to which such Deliverable pertains.

4.4 **Data Responsibility.** Customer is solely responsible for any and all transactional data, including personally identifiable data (collectively, "Customer Data"), that may be collected or utilized by Customer through its use of the Subscription Service; provided that Customer Data may not include, and Cayuse shall have no responsibility for, any protected health information or personally identifiable data other than user name or ID, account number, user profile or preferences, mailing address, email address, IP address, landline or cellular telephone numbers. Cayuse reserves the right to take down, delete and/or block access (whether temporarily or permanently) to any Customer Data that violates any of the provisions of this Section or in respect of which Cayuse receives a complaint from any person. Customer is responsible for establishing and enforcing terms of use and privacy policies ("Customer Policies") that govern use of the Subscription Service by End Users as permitted under this Agreement and applicable law. In relation to all personal data comprised within any Customer Data, Customer warrants that such personal data shall have been obtained and supplied to Cayuse in compliance with applicable data protection and privacy legislation, including Customer having obtained all necessary consents and approvals from End Users pursuant to the Customer Policies that are necessary under such legislation to permit Cayuse to (i) provide the Subscription Service; (ii) perform its other obligations hereunder; and (iii) exercise its rights and benefits hereunder. Further, regarding all personal data comprised within any Customer Data, Cayuse will process such personal data in compliance with the Personal Data Processing Agreement attached to this Agreement as Appendix 3.

4.5 **Customer Data License; Usage Data.** Customer grants to Cayuse a limited, nonexclusive, fully paid-up, royalty-free license to copy, store, display and use the Customer Data for purposes of: (i) providing Customer and End Users access and use of Subscription Service; and (ii) enabling Cayuse to perform its other obligations hereunder. Cayuse shall fully own and retain all rights to anonymous usage data derived from Customer Data ("Usage Data") as aggregated with usage data from Cayuse's other customers for its own business purposes such as support, operational planning, product innovation and sales and marketing of Cayuse's services. For purposes of clarification, such Usage Data may not include any data that could reasonably identify Customer or any particular End User.

4.6 **Third-Party Access.** Customer consents to allow Cayuse to provide access to Customer Data to Cayuse employees and to certain third party service providers which have a legitimate need to access such data in order to provide their services to Cayuse as part of Cayuse's provision of the Subscription Service to Customer. Customer also acknowledges that, subject to the terms of this Agreement and to the extent permitted by applicable law, Customer Data may be accessed by Cayuse support personnel in foreign countries, including countries other than the jurisdiction from which the Customer Data was collected, solely for the purpose of providing Customer support, and Customer hereby authorizes such access and processing. Customer consents to allow Cayuse to provide access to Customer Data to third parties that Cayuse designates through the provision of Subscription Service under this Agreement.

4.7 **Customer Data Retention and Deletion Requests.** Upon Customer's written request, Cayuse shall delete or provide (in a format to be mutually agreed upon by the parties) any Customer Data in Cayuse's possession within a commercially reasonable time not to exceed two (2) weeks unless a shorter time is required by law. Cayuse will otherwise delete Customer Data within the time periods required by law, and at a minimum other than ordinary course backups within a commercially reasonable time following the end of the term of the Agreement.

4.8 **License to Customer Trademarks.** Customer hereby grants to Cayuse a limited, non-transferable, non-sublicensable, non-exclusive license, during the Subscription Term, to use, reproduce, display, and distribute any trademarks, service marks, or trade names that Customer may designate from time-to-time ("Customer Marks") in connection the Subscription Service to Customer and its End Users, subject to the terms of this Agreement. With prior approval, the Customer further grants Cayuse the right to display the Customer Marks on its Website and marketing materials. Cayuse shall comply with Customer's then-current policies regarding the use of Customer's Marks. Cayuse acknowledges and agrees that the Customer Marks belong to and shall continue to belong to Customer (or its licensors or other third party owners), and Cayuse shall have no rights in or to the Customer Marks other than as specifically set forth in this Agreement.

5. FEES AND PAYMENT

5.1 **Subscription Service Fees.** The pricing and fees for the Subscription Service and Professional Services are forth in the applicable Order Form or SOW (the "Fees") and will be invoiced in accordance with the provisions set forth therein. Cayuse escalates the annual Subscription Service Fee by four (4%) percent annually during the Subscription Term. Cayuse reserves the right to change the Fees for any Renewal Term (as defined below) upon thirty (30) calendar days ("Days") prior written notice to Customer.

5.2 **Payment Terms.** All amounts to be paid by Customer hereunder shall be due and payable within thirty (30) Days after Customer's receipt of the invoice therefor. All payments not made by Customer when due shall be subject to late charges of the lesser of (a) one and one-half percent (1.5%) per month of the overdue amount; or (b) the maximum amount permitted under applicable law. Any failure to pay Fees will constitute a material breach of this Agreement by Customer.

5.3 **Taxes.** Customer shall pay all sales, use and excise taxes relating to, or under, this Agreement, exclusive of taxes based on or measured by Cayuse's net income, unless Customer is exempt from the payment of such taxes and provides Cayuse with sufficient evidence of such exemption.

5.4 **Suspension.** Without limiting Cayuse's termination rights, Cayuse shall have the right to suspend the Subscription Service in the event Customer fails to pay any Fees when due.

6. CONFIDENTIALITY

6.1 **Confidentiality Obligations.** The Parties agree to hold each other's information, whether oral, written, electronic, or in any other format, and whether technical or business in nature, regarding this Agreement, Cayuse's products or business, including the Subscription Service, information regarding a Party's products, services, software, intellectual property, pricing, marketing and business plans, other information not generally known to the public and any other information received under circumstances reasonably interpreted as imposing an obligation of confidentiality ("Confidential Information"); provided that Confidential Information shall not include any of such information which: (a) was publicly available at the time of disclosure by the disclosing Party; (b) became publicly available after disclosure through no fault of the receiving Party; (c) was known to the receiving Party prior to disclosure by the disclosing Party; or (d) was rightfully acquired by the receiving Party after disclosure by the disclosing Party from a third party who was lawfully in possession of the information and was under no legal duty to the disclosing Party to maintain the confidentiality of the information in strict confidence. The Parties agree not to make each other's Confidential Information available in any form to any third party or to use each other's Confidential Information for any purpose other than as specified in this Agreement. Each Party agrees to take all reasonable steps to ensure that Confidential Information of either Party is not disclosed or distributed by its employees, agents, or consultants in violation of the provisions of this Agreement. Each Party's Confidential Information shall remain the sole and exclusive property of that Party. Each Party acknowledges that any use or disclosure of the other Party's

Confidential Information other than as specifically provided for in this Agreement may result in irreparable injury and damage to the non-using or non-disclosing party. Accordingly, each Party hereby agrees that, in the event of use or disclosure by the other Party other than as specifically provided for in this Agreement, the non-using or non-disclosing Party may be entitled to equitable relief as granted by any appropriate judicial body.

6.2 Feedback. Customer and/or its End Users may provide suggestions, comments or other feedback to Cayuse with respect to the products and services, including the Subscription Service. Feedback is voluntary and Cayuse is not required to hold it in confidence. Feedback may be used by Cayuse for any purpose without obligation of any kind. Nothing contained herein shall preclude either Party from developing any products or services or enhancing any existing products or services, including but not limited to the products that are the subject of this Agreement, provided any such developments or enhancements are not based on or derived from the other party's intellectual property or Confidential Information.

7. TERM AND TERMINATION

7.1 Term. The initial term of this Agreement shall commence on the Effective Date and shall continue in effect until terminated as set forth herein. Each Order Form will specify the initial subscription term (the "Initial Term"). Upon expiration of the Initial Term, each Order Form shall renew automatically for successive twelve (12) month renewal terms (each a "Renewal Term") unless either party provides written notice to the other party of its intent not to renew such Order Form not less than thirty (30) days prior to the expiration of the Initial Term. The Initial Term and any Renewal Terms are referred to herein collectively as the "Subscription Term."

7.2 Termination for Breach. Either Party may terminate this Agreement upon not less than thirty (30) Days prior written notice if the other Party has failed to comply with any material term, condition, or obligation of this Agreement, and such Party subsequently has failed to remedy the default within thirty (30) Days after such notice by the non-defaulting Party.

7.3 Termination for Insolvency. If Cayuse believes in good faith that Customer's ability to make payments may be impaired, or if Customer fails to pay any invoice when due and does not make such payment within ten (10) Days after receipt of notice from Cayuse of such failure, then Cayuse may, in its sole discretion, either: (a) suspend the Subscription Service until such payment is made; or (b) terminate the Subscription Service. In either event, Customer shall remain liable to pay all Fees under this Agreement.

7.4 Effect of Termination. Upon termination or expiration of this Agreement for any reason, all sums owed to Cayuse by Customer will become immediately due and payable upon the effective date of termination, and each Party shall immediately cease use of all Confidential Information belonging to the other Party and shall irretrievably delete and/or remove such items from all computer hardware and storage media, including backups. Additionally, following termination of this Agreement, Customer shall immediately cease use of the Subscription Service.

7.5 Survival. Notwithstanding any provisions contained in this Agreement to the contrary, in addition to any provisions that by their express terms survive expiration and termination of this Agreement, or by their nature may be reasonably inferred to have been intended to survive expiration and termination of this Agreement, the following provisions shall survive expiration and termination of this Agreement: 2.2 (Limitations on License), 4 (Intellectual Property), 5 (Fees and Payment), 6 (Confidentiality), 7.4 (Effect of Termination), 7.5 (Survival), 8.3 (No Other Warranties), 9 (Indemnification), 10 (Limitation of Liability) and 11 (General).

8. WARRANTIES

8.1 Mutual Warranties. Each Party represents and warrants that (a) it has the authority to enter into this Agreement and to grant the rights and licenses provided herein, and that by entering into this Agreement such Party is not in violation of any previous agreement between such Party and any third party, and (b) it will comply with all laws and regulations applicable to the obligations assumed under this Agreement.

8.2 Cayuse Warranties. Cayuse warrants that (a) all Professional Services and Support Services shall be provided in a professional, competent and workmanlike manner in accordance with the prevailing industry standards and (b) the Subscription Service, when used in accordance with the Documentation and this Agreement, will perform in

all material respects as specified in such Documentation during the applicable Subscription Term; provided that if Customer notifies Cayuse in writing that the Subscription Service does not comply with the foregoing, then Cayuse will, as Customer's sole and exclusive remedy and Cayuse's sole liability, use commercially reasonable efforts to cause the Subscription Service to comply with the foregoing at no additional cost to Customer.

8.3 No Other Warranties. EXCEPT AS SPECIFICALLY SET FORTH IN THIS SECTION 8 (WARRANTIES), CAYUSE DOES NOT MAKE ANY GUARANTEE, WARRANTY, OR REPRESENTATION, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SUBSCRIPTION SERVICE (INCLUDING ANY WARRANTY AS TO TITLE, NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE), NOR WITH RESPECT TO ANY OTHER MATTER SET FORTH IN THIS AGREEMENT.

9. INDEMNIFICATION

9.1 Mutual Indemnification. Each Party (the "Indemnifying Party") agrees to indemnify and hold harmless the other Party (the "Indemnified Party") from and against any and all causes of action, claims, damages, liabilities, losses, judgments, and costs (including reasonable attorneys' fees and disbursements) (collectively, "Claims") by third parties arising out of or relating to: (a) the Indemnifying Party's gross negligence or willful misconduct; or (b) any alleged infringement or misappropriation of such third parties' intellectual property rights by, the Customer Data (as to Customer) or Subscription Service (as to Cayuse).

9.2 Indemnification Procedure. The Parties' indemnification obligations are conditioned upon: (a) the Indemnified Party promptly notifying the Indemnifying Party of any Claim for which indemnification is sought, provided, that any failure or delay to provide such notice shall not constitute a breach of this Agreement and shall not excuse the Indemnifying Party from its obligations under this Section 9 (Indemnification), except to the extent (if any) that the Indemnifying Party is prejudiced by such failure or delay; (b) the Indemnified Party cooperating with the Indemnifying Party in its defense or settlement of any such Claim; (c) the Indemnifying Party completely controlling the defense or settlement of any such Claim; and (d) the Indemnified Party using commercially reasonable efforts to mitigate the damages, if applicable. The Indemnified Party shall be entitled to participate in (but not control) the defense of such action, with its counsel and at its own expense. The foregoing notwithstanding, the Indemnifying Party shall not finalize any settlement that prejudices or materially, adversely affects the Indemnified Party without the prior written consent of the Indemnified Party.

10. LIMITATION OF LIABILITY

10.1 Disclaimer of Consequential Damages. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY FOR ANY INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, INDIRECT, OR SPECIAL DAMAGES OR COSTS (INCLUDING LOST PROFITS, LOST REVENUES, LOST DATA, COSTS OF RECREATING LOST DATA, OR LOSS OF USE) RESULTING FROM ANY CLAIM OR CAUSE OF ACTION BASED ON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE (INCLUDING STRICT LIABILITY), OR ANY OTHER LEGAL THEORY, EVEN IF EITHER OR BOTH OF THEM KNEW, OR SHOULD HAVE KNOWN, OF THE POSSIBILITY THEREOF.

10.2 Cap on Direct Damages. NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY OR TO ANY OTHER PERSON OR ENTITY FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE FEES PAID OR PAYABLE BY CUSTOMER TO CAYUSE IN THE TWELVE (12) FULL CALENDAR MONTHS IMMEDIATELY PRECEDING THE MONTH IN WHICH THE EVENT GIVING RISE TO THE CLAIM OCCURRED.

10.3 Exclusions. NOTWITHSTANDING THE FOREGOING OR ANYTHING TO THE CONTRARY CONTAINED IN THIS AGREEMENT, THE LIMITATIONS UPON THE TYPES AND AMOUNTS OF EACH PARTY'S LIABILITY, AND THE EXCLUSIONS OF CERTAIN TYPES OF DAMAGES, SET FORTH IN THIS SECTION 10 (LIMITATION OF LIABILITY), SHALL NOT APPLY TO THE FOLLOWING: (A) DAMAGES RESULTING FROM CUSTOMER'S BREACH OF SECTION 2 (LICENSE GRANTS AND RESTRICTIONS); (B) DAMAGES RESULTING FROM A BREACH OF SECTION 6 (CONFIDENTIALITY); OR (C) CLAIMS SUBJECT TO OR AMOUNTS PAYABLE PURSUANT TO THE PARTIES' INDEMNIFICATION OBLIGATIONS HEREUNDER.

11. GENERAL

11.1 Nature of Relationship. In entering this Agreement, Customer does so as an independent party and not as an agent, partner, or joint venturer of Cayuse. Customer does not have any right or authority, nor shall Customer hold itself out as having any right or authority, to assume, create, or enter into any contract or obligation, either express or implied, on behalf of, in the name of, or binding upon, Cayuse.

11.2 Non-solicitation. During the term of this Agreement and each SOW and for twelve (12) months after their respective expiration or termination, neither party will, either directly or indirectly, solicit for employment or employ (except as permitted below) by itself any employee of the other party who was involved in the performance of the party's obligations, unless the hiring party obtains the written consent of the other party. The foregoing provision will not prohibit a general solicitation of employment in the ordinary course of business or prevent either party from employing any employee who contacts such party as a result of such a general solicitation or at his or her own initiative without any direct or indirect solicitation by or encouragement from such party

11.3 Press Release. Each Party will have the right to issue a press release about the relationship between the Parties with the other Party's prior written approval (which shall not be unreasonably withheld or delayed). Cayuse may include Customer's name on Companies customer list and may describe briefly, and in general terms, the nature of the work performed by Cayuse for Customer.

11.4 Construction. The section headings in this Agreement are for convenience of reference only, will not be deemed to be a part of this Agreement, and will not be referred to in connection with the construction or interpretation of this Agreement. Any rule of construction to the effect that ambiguities are to be resolved against the drafting Party will not be applied in the construction or interpretation of this Agreement. As used in this Agreement, the words "include" and "including," and variations thereof, will not be deemed to be terms of limitation, but rather will be deemed to be followed by the words "without limitation."

11.5 Inapplicability of UCITA. THE PARTIES AGREE THAT NO PROVISION OF THE UNIFORM COMPUTER INFORMATION TRANSACTIONS ACT (UCITA) IS INTENDED TO APPLY TO THE INTERPRETATIONS OF THIS AGREEMENT, WHETHER OR NOT UCITA IS ENACTED IN THE LEGAL JURISDICTION WHOSE LAW GOVERNS THIS AGREEMENT AS SET FORTH IN THIS AGREEMENT.

11.6 Governing Law; Severability. This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and constructed in accordance with United Kingdom law and venue shall be in the United Kingdom; In the event that one or more of the provisions herein shall be invalid, illegal, or unenforceable in any respect, the validity, legality, and enforcement of the remaining provisions shall not be affected or impaired.

11.7 Assignment. Customer shall not assign this Agreement or any

rights or obligations hereunder, without the express written consent of Cayuse save as described in the agreement. Any assignment or transfer in violation of the foregoing will be null and void. Cayuse reserves the right to assign this Agreement in connection with the sale, combination, or transfer of all or substantially all of the assets or capital stock or from any other corporate form of reorganization by or of Cayuse. Subject to all of the terms and conditions hereof, this Agreement inures to the benefit of and is binding upon the Parties hereto and their successors and assigns.

11.8 Waiver. The failure to enforce or the waiver by either Party of one default or breach of the other Party shall not be considered to be a waiver of any subsequent default or breach.

11.9 Force Majeure. Except with regard to payment obligations, either Party shall be excused from delays in performing or from failing to perform its obligations under this Agreement to the extent the delays or failures result from causes beyond the reasonable control of the Party, including, but not limited to, default of subcontractors or suppliers, failures of third party software, default of third party vendors, acts of God or of the public enemy, U.S. or foreign governmental actions, labor shortages or strikes, communications or utility interruption or failure, fire, flood, epidemic, and freight embargoes. However, to be excused from delay or failure to perform, the Party must act diligently to remedy the cause of the delay or failure.

11.10 Remedy. The rights and remedies of the Parties will be cumulative (and not alternative). In the event of any litigation between the Parties relating to this Agreement, the prevailing Party will be entitled to recover its reasonable attorneys' fees, expert witness fees, and court costs from the other Party.

11.11 Entire Agreement. This Agreement, and each Order Form and SOW, together constitute the entire understanding of the Parties with respect to the subject matter hereof, and supersedes all prior and contemporaneous written and oral agreements with respect to the subject matter. No modification of this Agreement shall be binding on either Party unless it is in writing and signed by both Parties. In the event of any conflict or inconsistency between this Agreement, order form, and/or any exhibit, the terms and conditions of this Agreement shall prevail. The terms on any purchase order or similar document submitted by Customer to Cayuse will have no effect and are hereby rejected.

11.12 Notices. All notices, consents and approvals under this Agreement must be delivered in writing by courier, by facsimile, or by certified or registered mail, (postage prepaid and return receipt requested) to the other party at the address set forth above.

11.13 Counterparts. This Agreement may be executed in counterparts, each of which will be deemed an original and all of which taken together shall constitute one and the same Agreement.

IN WITNESS WHEREOF, the Parties have caused their duly authorized representatives to execute this Agreement as of the Effective Date.

CAYUSE, LLC

BY: _____

NAME: _____

TITLE: _____

CUSTOMER: _____

BY: _____

NAME: _____

TITLE: _____

Appendix 1

Cayuse Maintenance and Support Policy

During the Subscription Term, Cayuse shall provide standard technical support for End Users for the Subscription Service between the hours of 8:00 am and 5:00 pm, GMT, Monday through Friday, excluding Cayuse companywide holidays ("Business Hours"). Cayuse shall make available applications and technical staff to assist with questions about the Subscription Service and to assist Customer in solving any problems. The Cayuse technician responding to Customer's inquiry will be experienced, technically competent, and familiar with the Subscription Service. Customer shall submit a help desk request through Cayuse' website, with verifiable and reproducible evidence of problem, questions, or requests for assistance. Upon receipt of a help desk request, Cayuse shall respond by email to acknowledge receipt of the request based on the priority status Customer notes on the request.

- i) Urgent – Production Down. Reserved for issues when the production environment is down. Cayuse will respond within one (1) hour from the time the request is received (during Business Hours or within one (1) hour of opening if the request is not received during Business Hours).
- ii) High – Production Critical. Reserved for issues when the production environment is threatened, but not actually down. Cayuse will respond the same day the request is received (if the request is received by 4:00 pm GMT of any day the help desk is open or, if received later, the next business day).
- iii) Medium – Time Sensitive. Cayuse will respond within 24 hours of the time the request is received, excluding in the computation of such 24 hours any days outside of Business Hours. (For example, if such a request is received at 1:00 pm on a Friday, Cayuse will respond by 1:00 pm on the following Monday, if such Monday is within Business Hours.)
- iv) Low – Non Essential Timeline. Cayuse will respond within 48 hours of the time the request is received, excluding in the computation of such 48 hours any days during which the help desk is not open. (For example, if such a request is received at 1:00 pm on a Friday, Cayuse will respond by 1:00 pm on the following Tuesday, if neither such Tuesday nor the preceding Monday is outside of Business Hours.)

Cayuse may undertake scheduled maintenance of the Subscription Service during time periods designated by Cayuse. Cayuse will provide Customer with no less than 48 hours prior electronic mail or other notice of any scheduled maintenance that is likely to make the Subscription Service inaccessible or unusable and will only perform this type of scheduled maintenance outside of Business Hours.

Appendix 2

Cayuse Maintenance and Support Policy

1. DEFINITIONS.

Certain capitalized terms, not otherwise defined in this Appendix 2, will have the meanings set forth in the Agreement. The following capitalized terms will have the definitions set forth below:

1.1 "Availability" will mean, with respect to any particular calendar month, the ratio obtained by subtracting Unscheduled Downtime during such month from the total time during such month, and thereafter dividing the difference so obtained by the total time during such month.

Represented algebraically, Availability for any particular calendar month is determined as follows:

$$\text{Availability} = \frac{\text{Total Monthly Time} - \text{Unscheduled Downtime}}{\text{Total Monthly Time}}$$

1.2 "Scheduled Downtime" will mean the total amount of time during any calendar month, measured in minutes, during which Customer is not able to access the Service, according to the Documentation, due to planned system maintenance performed by Cayuse. Cayuse will exercise reasonable efforts to perform scheduled system maintenance between the hours of 12:00 AM and 3:00 AM GMT and one Saturday a month for 12 hours. Cayuse may change planned maintenance windows at its sole discretion and will notify Customer of any such changes that affect previously notified plans, provided such maintenance is done during low volume times.

1.3 "Total Monthly Time" is deemed to include all minutes in the relevant calendar month, to the extent such minutes are included within the Access Term.

1.4 "Unscheduled Downtime" will mean the total amount of time during any calendar month, measured in minutes, during which Customer is not able to access the Production Service according to the Documentation, other than Scheduled Downtime, as defined above.

2. **PERFORMANCE.** Cayuse will undertake commercially reasonable measures to ensure that Availability equals or exceeds ninety-nine and nine tenths percent (99.9%, which equates to 44 minutes of Unscheduled downtime per month) during each calendar month (the "Service Standard"), provided that any Unscheduled Downtime occurring as a result of circumstances beyond Cayuse's reasonable control including (i) Customer's breach of any provision of the Agreement; (ii) non-compliance by Customer with any provision of this Appendix 2; (iii) incompatibility of Customer's equipment or software with the Service; (iv) poor or inadequate performance of Customer's systems; (v) Customer's equipment failures; (vi) acts or omissions of Cayuse's suppliers; or (vii) force majeure (as contemplated in the Agreement), shall not be considered toward any reduction in Availability measurements. Customer may report Unscheduled Downtime by calling (877)-689-3661 ext. 1 or (503)-297-1311 ext. 1 or by email at support@cayuse.com during Cayuse's normal business hours (8 am to 5 pm GMT). Cayuse will exercise commercially reasonable efforts to respond to reports of Unscheduled Downtime by telephone or email acknowledgement within one (1) business day of each such report.

3. **MEASUREMENT AND REPORTS.** Cayuse will provide for monitoring of Availability on an ongoing basis. All measurements of Availability will be calculated on a monthly basis for each calendar month during the Access Term. In the event Unscheduled Downtime occurs, Cayuse will provide a report setting forth measurements thereof and a calculation of Availability within a reasonable time thereafter. If Customer disagrees with any measurement or other information set forth in any such report, it must so inform Cayuse in writing within five (5) calendar days after receipt. Accuracy of any such report shall be deemed conclusive unless such notice is provided by Customer. Any such notice must indicate specific measurements in dispute and must include a detailed description of the nature of the dispute. Cayuse and Customer agree to attempt to settle any such disputes regarding Availability and/or related measurements in a timely manner by mutual good faith discussions.

4. **CUSTOMER REQUIREMENTS.** Customer is responsible for maintenance and management of its computer network(s), servers, software, and any equipment or services needed to access the Service; and (ii) correctly configuring Customer's systems in accordance with the Documentation. Customer must promptly notify Cayuse in the event Unscheduled Downtime occurs. Unscheduled Downtime will be deemed to begin when Cayuse receives accurate notification thereof from Customer, or when Cayuse first becomes aware of such Unscheduled Downtime, whichever first occurs. The obligations of Cayuse set forth in this Appendix 2 will be excused to the extent any failures to meet such obligations result in whole or in part from Customer's failure(s) to meet the foregoing requirements.

5. **REMEDIES.** In the event Unscheduled Downtime occurs, Cayuse will undertake commercially reasonable efforts to remedy such Unscheduled Downtime within a commercially reasonable timeframe. Customer's sole and exclusive remedy, and Cayuse's sole and exclusive liability, for Cayuse's breach of this Appendix 2 will be the following credits:

Uptime Calculation	Service Credit
<99.9% of unscheduled downtime	1 day of fees credited
<99.7% of unscheduled downtime	2 days of fees credited
<99.5% of unscheduled downtime	5 days of fees credited

6. OTHER

Customer's instance will be hosted on AWS and controlled VPN access is for OS-level administrative access managed by Cayuse. Currently there are no restrictions on the access to the endpoint URL. Administrative tasks (host (OS) level) are for Cayuse managed hosting. Cayuse works with AWS to implement tools for tracking irregular activity. Upon request, we will provide reporting to Customer. Data is backed up incrementally daily, with a full backup completed on a weekly basis. All data is retained for one week.

APPENDIX 3

Personal Data Processing Agreement

This agreement is dated: [DATE].

PARTIES

(1) [FULL COMPANY NAME], a [STATE OF ORGANIZATION] [TYPE OF ENTITY], with offices located at [ADDRESS] (the "Customer").

(2) Haplo Services, LTD, located at Rm 4.10, 201 Borough High Street, London, SE1 1JA (the "Provider").

RECITALS

WHEREAS, Customer and Provider entered into the Master Agreement (the "**Master Agreement**") that may require Provider to process Personal Information provided by or collected for Customer; and

WHEREAS, this Personal Data Processing Agreement (the "**PDPA**") sets out the additional terms, requirements, and conditions on which Provider will obtain, handle, process, disclose, transfer, or store Personal Information when providing services under the Master Agreement;

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

1. Definitions and Interpretation

The following definitions and rules of interpretation apply in this PDPA.

"**Authorized Persons**" means the persons or categories of persons that Customer authorizes to give Provider personal information processing instructions.

"**Business Purpose**" means the services described in the Master Agreement.

"**Data Subject**" means an individual who is the subject of Personal Information.

"**Personal Information**" means any information Provider processes for Customer that (a) identifies or relates to an individual who can be identified directly or indirectly from that data alone or in combination with other information in Provider's possession or control or that Provider is likely to have access to, or (b) the relevant Privacy and Data Protection Requirements otherwise define as protected personal information.

"**Processing, processes, or process**" means any activity that involves the use of Personal Information or that the relevant Privacy and Data Protection Requirements may otherwise include in the definition of processing, processes, or process. It includes obtaining, recording, or holding the data, or carrying out any operation or set of operations on the data including, but not limited to, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring Personal Information to third parties.

"**Privacy and Data Protection Requirements**" means all applicable federal, state, and foreign laws and regulations relating to the processing, protection, or privacy of the Personal Information, including where applicable, the guidance and codes of practice issued by regulatory bodies in any relevant jurisdiction.

"Security Breach" means any act or omission that compromises the security, confidentiality, or integrity of Personal Information or the physical, technical, administrative, or organizational safeguards put in place to protect it. The loss of or unauthorized access, disclosure, or acquisition of Personal Information is a Security Breach whether or not the incident rises to the level of a security breach under the Privacy and Data Protection Requirements.

"Standard Contractual Clauses (SCC)" means the European Commission's Standard Contractual Clauses for the transfer of Personal Information from the European Union to processors established in third countries (controller-to-processor transfers), as set out in the Annex to Commission Decision 2010/87/EU, a completed copy of which comprises Exhibit B.

2. Included Documents; Precedence. This PDPA is subject to the terms of the Master Agreement and is incorporated into the Master Agreement. Interpretations and defined terms set forth in the Master Agreement apply to the interpretation of this PDPA.

The Exhibits form part of this PDPA and will have effect as if set out in full in the body of this PDPA. Any reference to this PDPA includes the Exhibits.

A reference to writing or written includes email.

In the case of conflict or ambiguity between:

any provision contained in the body of this PDPA and any provision contained in the Exhibits, the provision in the body of this PDPA will prevail;

the terms of any accompanying invoice or other documents annexed to this PDPA and any provision contained in the Exhibits, the provision contained in the Exhibits will prevail;

any of the provisions of this PDPA and the provisions of the Master Agreement, the provisions of this PDPA will prevail; and

any of the provisions of this agreement and any executed Standard Contractual Clauses, the provisions of the executed Standard Contractual Clauses will prevail.

3. Personal Information Types and Processing Purposes

Customer retains control of the Personal Information and remains responsible for its compliance obligations under the applicable Privacy and Data Protection Requirements, including providing any required notices and obtaining any required consents and for the processing instructions it gives to Provider.

Exhibit A describes the general Personal Information categories and Data Subject types the Provider may process to fulfill the Business Purposes of the Master Agreement.

4. Provider's Obligations

Provider will only process, retain, use, or disclose the Personal Information to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with Customer's instructions. Provider will not process, retain, use, or disclose the Personal Information for any other purpose or in a way that does not comply with this PDPA or the Privacy and Data Protection Requirements. Provider will promptly notify Customer if, in its opinion, Customer's instruction would not comply with the Privacy and Data Protection Requirements.

Provider will promptly comply with any Customer request or instruction requiring Provider to amend, transfer, or delete the Personal Information, or to stop, mitigate, or remedy any unauthorized processing.

Provider will maintain the confidentiality of all Personal Information, will not sell it to anyone, and will not disclose it to third parties unless Customer or this PDPA specifically authorizes the disclosure, or as required by law. If a law requires Provider to process or disclose Personal Information, Provider must first inform Customer of the legal requirement and give Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.

Provider will reasonably assist Customer with meeting Customer's compliance obligations under the Privacy and Data Protection Requirements, taking into account the nature of Provider's processing and the information available to Provider.

Provider will promptly notify Customer of any changes to Privacy and Data Protection Requirements that may adversely affect Provider's performance of the Master Agreement.

Customer acknowledges that Provider is under no duty to investigate the completeness, accuracy, or sufficiency of any specific Customer instructions or the Personal Information other than as required under the Privacy and Data Protection Requirements.

5. Provider's Employees

Provider will limit Personal Information access to:

those employees who require Personal Information access to meet Provider's obligations under this PDPA and the Master Agreement; and

the part or parts of the Personal Information that those employees require for the performance of their duties.

Provider will ensure that all employees:

are informed of the Personal Information's confidential nature and use restrictions;

have undertaken training on the Privacy and Data Protection Requirements relating to handling Personal Information and how it applies to their particular duties; and

are aware both of Provider's duties and their personal duties and obligations under the Privacy and Data Protection Requirements and this PDPA.

Provider will take reasonable steps to ensure the reliability, integrity, and trustworthiness of all of Provider's employees with access to the Personal Information.

6. Security

Provider will at all times implement appropriate technical and organizational measures designed to safeguard Personal Information against unauthorized or unlawful processing, access, copying, modification, storage, reproduction, display, or distribution, and against accidental loss, destruction, or damage.

The Provider will take reasonable precautions to preserve the integrity of any Personal Information it processes and to prevent any corruption or loss of the Personal Information, including but not limited to establishing effective back-up and data restoration procedures.

7. Security Breaches and Personal Information Loss

Provider will promptly notify Customer if any Personal Information is lost or destroyed or becomes damaged, corrupted, or unusable. Provider will restore such Personal Information at its own expense.

The Provider will, within 48 hours, notify Customer if it becomes aware of:

- any unauthorized or unlawful processing of the Personal Information; or
- any Security Breach.

Immediately following any unauthorized or unlawful Personal Information processing or Security Breach, the parties will co-ordinate with each other to investigate the matter. Provider will reasonably co-operate with Customer in Customer's handling of the matter, including:

- assisting with any investigation;
- providing Customer with physical access to any facilities and operations affected;
- facilitating interviews with Provider's employees, former employees and others involved in the matter; and
- making available all relevant records, logs, files, data reporting, and other materials required to comply with all Privacy and Data Protection Requirements or as otherwise reasonably required by Customer.

Provider will not inform any third party of any Security Breach without first obtaining Customer's prior written consent, except when law or regulation requires it.

Provider agrees that Customer has the sole right to determine whether to provide notice of the Security Breach to any Data Subjects, regulators, law enforcement agencies, or others, as required by law or regulation or in Customer's discretion, including the contents and delivery method of the notice.

Provider will cover all reasonable expenses associated with the performance of the obligations under this Section 7 unless the matter arose from the Customer's specific instructions, negligence, willful default, or breach of this PDPA, in which case the Customer will cover all reasonable expenses.

8. Cross-Border Transfers of Personal Information

If the Privacy and Data Protection Requirements restrict cross-border Personal Information transfers, Customer will only transfer that Personal Information to Provider under the following conditions:

Provider, either through its location or participation in a valid cross-border transfer mechanism under the Privacy and Data Protection Requirements, may legally receive that Personal Information, however Provider must immediately inform Customer of any change to that status;

Customer obtained valid Data Subject consent to the transfer under the Privacy and Data Protection Requirements; or

the transfer otherwise complies with the Privacy and Data Protection Requirements.

If any Personal Information transfer between Provider and Customer requires execution of Standard Contractual Clauses in order to comply with the Privacy and Data Protection Requirements, the parties will complete all relevant

details in, and execute, the Standard Contractual Clauses contained in Exhibit B, and take all other actions required to legitimize the transfer.

Provider will not transfer any Personal Information to another country unless the transfer complies with the Privacy and Data Protection Requirements.

9. Subcontractors

Provider may only authorize a third party (subcontractor) to process the Personal Information if:

Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this PDPA; and

Provider maintains control over all Personal Information it entrusts to the subcontractor.

Where the subcontractor fails to fulfill its obligations under such written agreement, Provider remains fully liable to Customer for the subcontractor's performance of its agreement obligations.

The parties consider Provider to control any Personal Information controlled by or in the possession of its subcontractors.

10. Complaints, Data Subject Requests, and Third Party Rights

Provider will notify the Customer promptly if it receives any complaint, notice, or communication that directly or indirectly relates to the Personal Information processing or to either party's compliance with the Privacy and Data Protection Requirements.

Provider will notify Customer within three working days if it receives a request from a Data Subject for access to or deletion of their Personal Information.

Provider will give Customer its full co-operation and assistance in responding to any complaint, notice, communication, or Data Subject request.

Provider will not disclose the Personal Information to any Data Subject or to a third party unless the disclosure is either at Customer's request or instruction, permitted by this PDPA, or is otherwise required by law.

11. Term and Termination

This PDPA will remain in full force and effect so long as:

the Master Agreement remains in effect; or

Provider retains any Personal Information related to the Master Agreement in its possession or control (the "**Term**").

Any provision of this PDPA that expressly or by implication should come into or continue in force on or after termination of the Master Agreement in order to protect Personal Information will remain in full force and effect.

If a change in any Privacy and Data Protection Requirement prevents either party from fulfilling all or part of its Master Agreement obligations, the parties will suspend the processing of Personal Information until that processing complies with the new requirements. If the parties are unable to bring the Personal Information processing into

compliance with the Privacy and Data Protection Requirement, they may terminate the Master Agreement upon written notice to the other party.

12. Data Return and Destruction

At Customer's request, Provider will give the Customer a copy of or access to all or part of the Customer's Personal Information in its possession or control in an industry-standard format.

On termination of the Master Agreement for any reason or expiration of its term, Provider will securely destroy or, if directed in writing by Customer, return and not retain, all or any Personal Information related to this agreement in its possession or control.

If any law, regulation, or government or regulatory body requires Provider to retain any documents or materials that Provider would otherwise be required to return or destroy, it will notify Customer in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. Provider may only use this retained Personal Information for the required retention reason or audit purposes.

13. Records. Provider will keep accurate records regarding any processing of Personal Information it carries out for Customer, approved subcontractors and affiliates, the processing purposes, and any other records required by the applicable Privacy and Data Protection Requirements (the "**Records**").

14. Audit

At least once per year, Provider will conduct audits of its Personal Information processing practices and the information technology and information security controls for all facilities and systems used in complying with its obligations under this PDPA, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices.

Upon Customer's written request, Provider will make all of the relevant audit reports available to the Customer for review. Customer will treat such audit reports as Provider's confidential information under this Agreement.

Provider will promptly address any issues, concerns, or exceptions noted in the audit reports with the development and implementation of a corrective action plan by Provider's management.

15. Warranties

Provider warrants and represents that:

its employees, subcontractors, agents, and any other person or persons accessing Personal Information on its behalf are reliable and trustworthy and have received the required training on the Privacy and Data Protection Requirements relating to the Personal Information;

it and anyone operating on its behalf will process the Personal Information in compliance with both the terms of this PDPA and all applicable Privacy and Data Protection Requirements and other laws, enactments, regulations, orders, standards, and other similar instruments;

it has no reason to believe that any Privacy and Data Protection Requirements prevent it from providing any of the Master Agreement's contracted services; and

considering the current technology environment and implementation costs, it will take appropriate technical and organizational measures to prevent the unauthorized or unlawful processing of Personal Information and the accidental loss or destruction of, or damage to, Personal Information, and ensure a level of security appropriate to:

the harm that might result from such unauthorized or unlawful processing or accidental loss, destruction, or damage; and

the nature of the Personal Information protected; and

comply with all applicable Privacy and Data Protection Requirement and its information and security policies.

Customer warrants and represents that Provider's expected use of the Personal Information for the Business Purpose and as specifically instructed by Customer will comply with all Privacy and Data Protection Requirements.

IN WITNESS WHEREOF, THE PARTIES HERETO HAVE EXECUTED THIS AGREEMENT AS OF THE DATE SET FORTH ABOVE.

HAPLO SERVICES, LTD

By _____

Name:

Title:

[PARTY NAME]

By _____

Name:

Title:



EXHIBIT A

Personal Information Processing Purposes and Details

Business Purposes:

Personal Information Categories:

Data Subject Types:

Approved Subcontractors:

Identify the Provider's legal basis for receiving Personal Information with cross-border transfer restrictions (select one):

Located in an EEA Member State or in a country with a current determination of adequacy (list country):

Binding Corporate Rules

Standard Contractual Clauses

Other (describe in detail): _____]

EXHIBIT B

Standard Contractual Clauses

Standard Contractual Clauses for Personal Data Transfers from an EU Controller to a Processor Established in a Third Country (Controller-to-Processor Transfers)

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) 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

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

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.]

SECTION II – OBLIGATIONS OF THE PARTIES

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 (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 Regulation of (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 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 [*Specify time period*] 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. 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 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) 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.

(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;

(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 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.

SECTION IV – FINAL PROVISIONS

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 _____ (*specify Member State*).]

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 _____ (*specify Member State*).
- (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.

ANNEX I

A. LIST OF PARTIES

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

1. Name: ...

Address: ...

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

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

Signature and date: ...

Role (controller/processor): ...

2. ...

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

1. Name: ...

Address: ...

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

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

Signature and date: ...

Role (controller/processor): ...

2. ...

B. DESCRIPTION OF TRANSFER


Categories of data subjects whose personal data is transferred

...

Categories of personal data transferred

...

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation,



access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

...

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

...

Nature of the processing

...

Purpose(s) of the data transfer and further processing

...

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

...

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

...

C. COMPETENT SUPERVISORY AUTHORITY

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

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

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

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

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

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

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

Measures for user identification and authorisation

Measures for the protection of data during transmission

Measures for the protection of data during storage

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

Measures for ensuring events logging

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

Measures for certification/assurance of processes and products

Measures for ensuring data minimisation

Measures for ensuring data quality

Measures for ensuring limited data retention

Measures for ensuring accountability

Measures for allowing data portability and ensuring erasure]

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorization of sub-processors (Clause 9(a)).

The controller has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

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

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. ...