Terms of Service Agreement

THIS AGREEMENT – INCORPORATING THE "DATA PROCESSING ADDENDUM", "STANDARD CONTRACTUAL CLAUSES" AND THE ATTACHED SCHEDULES AND ANNEXES – BETWEEN COMPLYWORKS LTD., A BRITISH COLUMBIA COMPANY WITH OFFICES AT SUITE 200, 4838 RICHARD RD. SW, CALGARY, AB, T3E 6L1 CANADA ('**COMPLYWORKS**') AND CUSTOMER IS MADE AS OF THE DATE CUSTOMER ACCEPTS THIS AGREEMENT. THIS AGREEMENT WILL BE DEEMED ACCEPTED BY THE CUSTOMER UPON THE CUSTOMER EITHER CLICKING THE BOX INDICATING ITS ACCEPTANCE OF THIS AGREEMENT, BY EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, OR BY UTILIZING ANY SERVICES. CONTEMPLATED HEREUNDER OR ON THE COMPLYWORKS.COM WEBSITE

IF YOU ARE AN INDIVIDUAL ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY AND ITS AFFILIATES TO THESE TERMS AND CONDITIONS, IN WHICH CASE THE TERM "CUSTOMER" SHALL REFER TO SUCH ENTITY AND ITS AFFILIATES ON WHOSE BEHALF INDIVIDUAL USERS ACCESS THE SERVICES. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE SERVICES.

WE MAY AMEND THIS AGREEMENT AT ANY TIME AND FROM TIME TO TIME BY POSTING THE AMENDED AGREEMENT ON THE COMPLYWORKS HOMEPAGE (www.complyworks.com). ALL AMENDMENTS SHALL AUTOMATICALLY BE EFFECTIVE UPON POSTING.

To make an inquiry about this Agreement contact:

ComplyWorks Ltd.

Suite 200, 4838 Richard Rd SW Calgary
AB T3E 6L1
cw-support@veriforce.com

You may not access the Services if You are Our direct or indirect competitor, except with Our prior written consent (which consent may be arbitrarily withheld). In addition, you may not access the Services for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes. The mirroring, scraping or data-mining of any of Our websites or any of their content in any form and by any means is strictly prohibited.

This Agreement was last updated April 2022 to incorporate the new UK Addendum for transfers of personal data out of the UK.

TABLE of CONTENTS

DEFINITIONS

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

"Customer" means a corporation, other legal entity, an unincorporated professional entity or a sole proprietor together with any of its Authorized Affiliates that uses the "Services" or '"Purchased Services" and agrees to this user agreement, and is also referred to as a Contractor.

"Customer Data" means all data or information, regardless of format, submitted by Customer or any employee or other representative or authorized user of Customer to the Purchased Services or Services.

"DPA" means the Data Processing Addendum, which is incorporated into and forms part of this Agreement.

"Employer" means a corporation or another legal entity together with any of its Authorized Affiliates that uses the "Services" or "Purchased Services" to manage the compliance of its contractors with its own requirements.

"Employer Connection" means the sharing of the Customer Data as processed by the Services with an Employer also known as a Hiring Client, as authorized by the Customer or the Customer's account administrators via the online, web-based application or otherwise.

"Malicious Code" means viruses, worms, time bombs, Trojan horses, malware, back door, drop dead device, spyware and other harmful or malicious code, files, scripts, agents or programs designed to (i) disrupt, disable or harm the operation of, or provide unauthorized access to, a computer system or network or other device on which such code is stored or installed, or (ii) compromise the privacy or data security of a user or damage or destroy any data or rile, in each case, without authorization and without the applicable user's consent.

"Order Form" means the ordering documents for purchases hereunder, including addenda thereto, that are entered into between Customer and ComplyWorks from time to time. Order Forms shall be deemed incorporated herein by reference.

"Purchased Services" means additional services that Customer purchases or may purchase under an Order Form or any other separate agreement between ComplyWorks and the Customer which may include the provision of professional services, additional modules, functionality and additional support. For the avoidance of doubt, Purchased Services do not include Services.

"Services" means the online, web-based applications and platform provided by ComplyWorks, including support services but excluding Third Party Applications.

"Third-Party Applications" means online, web-based applications and offline solutions and products that are owned, licensed or provided by third parties, interoperate with the Services, and are identified as third-party applications, including but not limited to those listed in the User Guide.

"User Guide" means the online User Guide for the Services, accessible via http://www.complyworks.com and/or other designated websites as described in the User Guide, as updated from time to time.

"Users" means individuals who are authorized by Customer to Use the Services, for whom subscriptions to a Service have been purchased, and who have been supplied User identifications and passwords by Customer (or by ComplyWorks at Customer request). Users may include but are not limited to Customer employees, consultants, contractors and agents or third parties with which Customer transacts business.

"We", "Us" or "Our" means ComplyWorks Ltd, a Veriforce company.

1. ELIGIBILITY

The Services are available only to unincorporated professional entities, corporations, sole proprietors and other legal entities that can form legally binding contracts under applicable law. Without limiting the foregoing, the Services are not available to minors or to temporarily or indefinitely suspended Users.

2. IDENTITY VERIFICATION

To access the Services a valid email and password are required. ComplyWorks Ltd. cannot and does not confirm each User's purported identity beyond verification of the User's authentication credentials. Customer is solely responsible for (i) maintaining confidentiality of passwords, (ii) not allowing others to use the email and password to access the Services, (iii) promptly informing ComplyWorks Ltd. in writing of the need to deactivate a User due to actual or potential security concerns, and (iv) any losses that may be incurred or suffered as a result of Customer failure to maintain password confidentiality.

3. PURCHASED SERVICES

3.1 Provision of Purchased Services We shall make the Purchased Services available to Customer pursuant to this Agreement and the relevant Order Forms during a subscription term as defined in the Order Forms (the "Subscription Term"). Customer agrees that its purchases hereunder are neither contingent on the delivery of any future functionality or features nor dependent on any oral or written statements made by Us regarding future functionality or features.

3.2 User Subscriptions Purchase of a corporate subscription grants to the Customer access for an unlimited number of Users within Customer organization. Customer is responsible for the administration of its Users and any and all issues related to its Users.

4. FEES AND PAYMENT FOR PURCHASED SERVICES

4.1 User Fees Customer shall promptly pay all fees and other charges (the "Fees") specified hereunder including without limitation in an Order Form. Except as otherwise specified herein (including in an Order Form), (i) Fees are quoted and payable in either Canadian Dollars or US Dollars as specified on the invoice (ii) Fees are based on Services purchased and not actual usage of the Services, (iii) payment obligations are non-cancelable and Fees paid are entirely non-refundable, (iv) the Customer shall have no right to reduce the level of Services or subscriptions purchased during the relevant Subscription Term, and (v) We may change Our Fees for the Services from time to time, and such changes to the Fees will not apply to Customer until the next renewal of the Subscription Term.

4.2 Invoicing and Payment Customer will provide Us with valid and updated credit card information or with a valid purchase order or cheque or alternative instrument acceptable to Us in our sole discretion. If Customer provides credit card information to Us, Customer authorizes Us to charge such credit card for all Services listed in the Order Form for the applicable Subscription Term(s) and all renewals. For all

subscription renewals, We will invoice Customer approximately 120 days in advance of subscription expiry. Unless otherwise stated, invoiced charges are due prior to renewal of subscription. Customer is responsible for ensuring that the billing and contact information it provides to ComplyWorks in connection with the Services are at all times accurate and complete.

4.3 Suspension of Service If the Customer has failed to pay any Fees or other amount owing under this Agreement by 30 days following the expiry date of the subscription, We will without limiting Our other rights and remedies under this Agreement and at law, require that Customer immediately pay any and all unpaid Fees and other obligations to Us under this Agreement (or otherwise) so that all such obligations become immediately due and payable, and forthwith suspend the Services (and any other of Our services and/or obligations to Customer) until all such Fees and other amounts are paid in full. Once Services are suspended, Customer will be required to pay a reactivation fee in addition to any other Fees and other charges owing on the outstanding Order Form or agreement in order to access the Services again.

4.4 Taxes Unless otherwise stated, Our Fees and other charges do not include any taxes, levies, duties or similar governmental or other assessments of any nature, including but not limited to value-added, sales, use or withholding taxes, assessable by any local, state, provincial, federal or foreign jurisdiction (collectively, "Taxes"). Customer is responsible for paying all Taxes associated with its purchases hereunder. If We have the legal obligation to pay or collect Taxes for which Customer is responsible under this Section 4.4, the appropriate amount shall be invoiced to and promptly paid by Customer, unless Customer provides Us with a valid and satisfactory to Us (in our sole discretion) tax exemption certificate authorized by the appropriate taxing authority.

5. USE OF THE SERVICES

5.1 Our Responsibilities We shall: (i) provide to Customer basic support for the Purchased Services at no additional charge, and/or upgraded support if purchased separately, (ii) use commercially reasonable efforts to make the Purchased Services available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which We shall give at least 8 hours' notice via the Purchased Services and which We shall schedule to the extent practicable during weekend hours between 6:00 p.m. Mountain Time Friday to 3:00 a.m. Mountain Time Monday), or (b) any unavailability caused by circumstances beyond Our reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, pandemic or global health emergencies, acts of terror, strikes or other labor problems, or Internet service provider failures or delays, and (iii) provide the Purchased Services only in accordance with applicable laws and government and other rules and regulations.

5.2 Customer Responsibilities Customer shall (i) be responsible for Users' compliance with this Agreement and will take reasonable and appropriate steps to ensure such compliance, (ii) be solely responsible for the accuracy, quality, integrity and legality of Customer Data and of the means by which Customer acquired the Data, (iii) ensure that all necessary notices have been provided, and all required consents and/or approvals have been obtained, in order to allow ComplyWorks and ComplyWorks Affiliates to Process (as defined in the DPA) Customer Data in connection with the Services, (iv) use best efforts to prevent unauthorized access to or Use of the Services, and notify Us promptly in writing of any such unauthorized access or use, and (v) use the Services only in accordance with the User Guide and the rules and/or terms and conditions which We may from time to time post on the ComplyWorks homepage (www.complyworks.com) and all applicable laws and government and other rules and regulations. Customer shall not (a) make the Services available to anyone other than Users, (b) sell, resell, rent, lease, lend, loan, distribute, sublicense or otherwise assign or transfer the Services or any rights thereto in whole or in part, (c) use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party rights (including privacy rights), (d) use the Services to store or transmit Malicious Code, (e) interfere with or disrupt the integrity or performance of

the Services or third-party data contained therein, or (f) attempt to gain unauthorized access to the Services or related systems and/or networks.

5.3 Usage Limitations Services may be subject to other limitations, such as, for example, but without limiting the generality of the foregoing, limits on disk storage space, on the number of calls Customer is permitted to make against Our application programming interface, and, for Services that enable Customer to provide public websites, on the number of page views by visitors to those websites.

6. INFORMATION CONTROL

6.1 Responsibility for Information ComplyWorks Ltd. does not control, or assume any responsibility for, and shall not be liable in any way related to, any information provided by Users that may be made available through or by Our Services. Customer may find some Users' information to be offensive, inaccurate, harmful, or deceptive but acknowledges and agrees that We shall have no responsibility or liability for such Users' information or content. Customer shall, and shall ensure that all of its Users shall, exercise caution, safe practices, and common sense when accessing the Services.

6.2 Verification Process Dependent upon the type of subscription purchased, ComplyWorks Ltd. may perform a review and comparison of submitted data and documentation to determine validity and correctness. During this process ComplyWorks Ltd. may assist on Customer's behalf to adjust Customer provided information to achieve a higher level of completion or help the information display correctly. ComplyWorks Ltd. will not adjust information that is not included or supported by provided documentation. Ongoing maintenance of the subscription remains Customer sole responsibility and any assistance provided by ComplyWorks Ltd. should not be construed as an ongoing expectation.

7. THIRD-PARTY PROVIDERS

7.1 Acquisition of Third-Party Products and Services We may offer Third-Party Applications for sale through our site or Services. You acknowledge and agree that any acquisition of third-party products or services through our site or Services, including but not limited to Third-Party Applications and any implementation, customization or other consulting services, and any exchange of data between Customer and any third-party provider, is solely between Customer and the applicable third-party provider. We do not warrant or support third-party products or services, including without limitation Third Party Applications, whether or not they are designated as "certified" or otherwise and you acknowledge and agree that (i) We are not and will not be liable in any way for any issues, liabilities, damages or expenses Customer or Users may suffer or incur as a result of accessing, acquiring or using such third party products or services, including without limitation such Third Party Applications, and (ii) Customer shall at all times be liable for any and all issues, liabilities, damages or expenses it or its Users incur as a result of using such third party products or services, including without limitation such Third Party Applications. Customer is not required to purchase third-party products or services , including without limitation Third Party Applications, in order to use the Services.

7.2 Third-Party Applications and Customer Data If Customer installs or enables Third-Party Applications for use with the Services or otherwise, Customer acknowledges and agrees that We may allow providers of those Third-Party Applications to access its Customer Data as required for the interoperation of such Third-Party Applications with the Services. By installing or enabling such Third Party Applications, Customer consents to the fact that We may allow providers of those Third Party Applications to access Customer Data (including Personal Data, as defined in the DPA, regarding Users and other individuals that may be contained in such data), and Customer confirms that it has provided any required notices and obtained any consents required to allow such access to the Personal Data (as defined in the DPA), if any, contained in the Customer Data. We shall not be responsible for any disclosure, modification or deletion of Customer Data resulting from any such access by Third-Party Application providers. Customer shall have

the ability, through its use of the Services, to restrict such access by restricting Users from installing or enabling such Third-Party Applications for use with the Services.

8. EMPLOYER CONNECTIONS

8.1 Right to Share Data. Customer may, at its sole and exclusive discretion, share, or authorize any third party or related party to the Customer to share, any data (including Customer Data) in its account with Employers. The Customer acknowledges and agrees that if it shares or authorizes the sharing of Customer Data with an Employer, that Employer shall have the authority to provide Processing (as defined in the DPA) instructions to ComplyWorks with respect to such Customer Data, including (without limitation) instructions to amend or delete all or part of the Customer Data. Moreover, Customer agrees that ComplyWorks shall comply with the Employer's Processing instructions instead of the Customer's instructions, if the Employer's instructions conflict with, or are otherwise inconsistent with, Customer's instructions in any manner.

8.2 Liability for Sharing Data. Customer acknowledges and agrees that it remains at all times solely and exclusively liable and responsible for any and all access, use, disclosure or other Processing (as defined in the DPA) of such Customer Data, including without limitation with respect to any disclosure of such Personal Data included or contained within the Customer Data, with Employers, and Customer represents and warrants that it has, and will ensure that all of its Users have, provided any required notices and obtained any and all consents required under all applicable privacy legislation from any and all individuals with respect to collection, use, disclosure and other Processing of their Personal Data which may be contained within the Customer Data. Furthermore, the parties agree that ComplyWorks shall bear no liability or responsibility for any actions or omissions with respect to the Customer Data, which are taken by ComplyWorks pursuant to instructions from any Employer(s) as described at Section 8.1.

9. PROPRIETARY RIGHTS

9.1 Reservation of Rights Subject to the limited rights expressly granted hereunder, We reserve, retain and own all rights, title and interest in, to and associated with the Services, including without limitation all intellectual property rights, whether registered or unregistered. Customer acknowledges and agrees that neither Customer nor any User has or shall obtain any rights or license hereunder except as expressly set forth or granted herein. For the purposes of this Agreement, "intellectual property rights" shall include patents, trademarks, copyrights, trade secrets, design rights, and any other proprietary rights, whether registered or unregistered, and any application for registration of any of the foregoing, and any right to file any such application, which may subsist anywhere in the world.

9.2 Restrictions Customer shall not, directly or indirectly, (i) permit any third party to access the Services except as specifically permitted herein or in an Order Form, (ii) create derivative works based on the Services, (iii) copy, frame, translate or mirror any part or content of the Services, (iv) reverse engineer, decompile or disassemble the Services or any part thereof, or (v) access the Services in order to (a) build a competitive product or service, or (b) copy any features, functions, code or graphics of the Services.

9.3 Ownership of Customer Data As between ComplyWorks and Customer, except as otherwise provided herein or an Order Form, Customer exclusively owns all rights, title and interest in and to all of Customer Data.

9.4 Suggestions We shall have and Customer hereby grants to Us a royalty-free, worldwide, transferable, sublicensable, irrevocable, perpetual license to use or incorporate into the Services any suggestions,

enhancement requests, recommendations or other feedback provided by Customer, including Users, relating to the operation of the Services.

10. CONFIDENTIALITY

10.1 Definition of Confidential Information As Used herein, "Confidential Information" means all confidential information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure. Customer Confidential Information shall include Customer Data; Our Confidential Information shall include the Services; and Confidential Information of each party shall include all Order Forms as well as business and marketing plans, technology and technical information, product plans and designs, and business processes disclosed by such party. However, Confidential Information shall not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known (as evidenced by its written records) to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed (as evidenced by its written records) by the Receiving Party.

10.2 Protection of Confidential Information Except as otherwise permitted in writing by the Disclosing Party, (i) the Receiving Party shall use the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but in no event less than reasonable care) not to disclose or use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, and (ii) the Receiving Party shall limit access to Confidential Information of the Disclosing Party to those of its employees, contractors or agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein.

10.3 Compelled Disclosure The Receiving Party may disclose Confidential Information of the Disclosing Party if it is compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior written notice of such compelled disclosure (to the extent legally permitted) and reasonable assistance, at the Disclosing Party's cost, if the Disclosing Party wishes to contest the disclosure. If the Receiving Party is compelled by law to disclose the Disclosing Party's Confidential Information as part of a civil proceeding to which the Disclosing Party is a party, and the Disclosing Party is not contesting the disclosure, the Disclosing Party will reimburse the Receiving Party for its reasonable cost of compiling and providing secure access to such Confidential Information.

11. WARRANTIES, DISCLAIMER AND LIMITATION OF LIABILITY

11.1 Our Warranties We warrant that the Services shall perform materially in accordance with the User Guide. For any breach of such warranty, Customer's exclusive remedy shall be to terminate this Agreement and receive the return of Customer Data in accordance with Section 13.5.

11.2 Customer Warranties Customer represents and warrants to Us that (i) Customer has the legal power to enter into this Agreement and perform all of its obligations contemplated hereunder, (ii) Customer has all necessary rights, consents and/or waivers to share, use, store, disclose, process or otherwise handle any and all Data including without limitation any Personal Data (as defined in the DPA) contained within such Data; and (iii) Customer will not transmit to Us any Malicious Code.

11.3 NO ADDITIONAL WARRANTIES BY US EXCEPT AS OTHERWISE SPECIFICALLY PROVIDED IN SECTION 11.1, THE SERVICES AND ALL INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOLUTIONS) AND OTHER SERVICES INCLUDED WITH THE SERVICES OR OTHERWISE MADE AVAILABLE

TO CUSTOMER BY US ARE PROVIDED BY US ON AN "AS IS" AND "AS AVAILABLE" BASIS. CUSTOMER EXPRESSLY AGREES THAT CUSTOMER AND CUSTOMER USERS USE OF THE SERVICES IS AT ITS SOLE RISK.

11.4 DISCLAIMER AND LIMITATION OF LIABILITY EXCEPT AS EXPRESSLY PROVIDED IN SECTION 11.1, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE DISCLAIM ANY AND ALL WARRANTIES AND CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABLE QUALITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES ARISING BY STATUTE, OPERATION OF LAW, COURSE OF DEALING, PERFORMANCE OR USAGE OF TRADE. WE DO NOT GUARANTEE THAT THE SERVICES OR PURCHASED SERVICES WILL MEET YOUR REQUIREMENTS, THAT THEY WILL PERFORM ERROR-FREE OR UNINTERRUPTED, OR THAT THEY WILL BE AVAILABLE WHEN REQUESTED BY CUSTOMER OR ANY USER. FURTHER, EXCEPT FOR THE EXCLUSIVE REMEDY SPECIFIED IN SECTION 11.1, WE WILL NOT BE LIABLE FOR ANY DAMAGES OR LIABILITY OF ANY KIND ARISING OUT OF OR IN ANY WAY RELATED TO THIS AGREEMENT OR THE USE OF THE SERVICES OR FROM ANY INFORMATION, CONTENT, MATERIALS, PRODUCTS (INCLUDING SOLUTIONS) OR SERVICES INCLUDED ON OR OTHERWISE MADE AVAILABLE TO CUSTOMER THROUGH OR IN CONNECTION WITH THE SERVICES, INCLUDING, BUT NOT LIMITED TO, DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL AND CONSEQUENTIAL DAMAGES AND OUR TOTAL AGGREGATE LIABILITY FOR ANY SUCH DAMAGES SHALL BE CAPPED AT AN AMOUNT EQUAL TO THE TOTAL AMOUNT OF FEES PAID BY THE CUSTOMER TO US DURING THE 12 MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO THE LIABILITY CLAIM.

12. INDEMNIFICATION

12.1 Indemnification Customer covenants and agrees to indemnify and save harmless Us and Our Affiliates and our respective directors, officers, employees, agents and consultants of and from all liabilities, claims, demands, actions, causes of action, damages, losses, costs and expenses whatsoever (including legal fees on a solicitor and his own client basis) suffered or incurred by any of them, directly or indirectly, arising out of, under or pursuant to:

12.1.1 A breach of any agreement, term or covenant on Customer's part made or to be observed or performed pursuant to this Agreement, including (without limitation) any breach of Customer's obligations under the DPA;

12.1.2 Any acts or omissions of Customer and/or Customer Users in carrying out Customer obligations under the Agreement;

12.1.3 Any claim made or brought against Us alleging that Customer Data, or Customer or Customer Users' use of the Services in violation of this Agreement, infringes or misappropriates the intellectual property rights of a third party or violates applicable law including (without limitation) any Data Protection Laws (as defined in the DPA); and

12.1.4 Any claim of unauthorized use or infringement of any Users' or third party's privacy or intellectual property rights arising from any use of Data supplied by the Customer.

13. TERM AND TERMINATION

13.1 Term of Agreement This Agreement commences on the date Customer accepts it or is deemed to accept it and continues until all User Subscription Terms purchased by Customer and granted in accordance with this Agreement have expired or been terminated.

13.2 Term of Purchased User Subscriptions Customer acknowledges and agrees that each User subscription purchased by Customer commences on the start date specified in the applicable Order Form and continues for the Subscription Term specified therein. Except as otherwise specified, all User subscriptions shall trigger notification for renewal for additional periods equal to the expiring Subscription Term or one year (whichever is shorter), unless either party gives the other written notice of non-renewal at least 30 days before the end of the relevant Subscription Term.

13.3 Termination of Agreement We reserve the right to immediately terminate this Agreement upon delivering to the Customer written notice in the event that any of the following events occur:

13.3.1 Customer fails to pay to Us any Fees or other amount due under this Agreement, and such default continues for a period of 30 days after written notice thereof has been given to Customer by Us;

13.3.2 Except as specified in Section 13.3.1, Customer breaches any of the provisions of this Agreement;

13.3.3 Customer makes a general assignment for the benefit of creditors;

13.3.4 Customer institutes any proceedings under any statute or otherwise relating to insolvency or bankruptcy, or should any proceeding under any such statute or otherwise be instituted against Customer and not be dismissed or vacated within 30 days of the date of commencement of such proceeding;

13.3.5 A custodian, receiver, manager or any other person with like powers is appointed to take charge of all or any part of Customer undertaking, business, property or assets and such person is not discharged within 30 days of the date of such appointment; or

13.3.6 An order is made by a court of competent jurisdiction or articles of dissolution or the like are filled for Customer winding up or liquidation.

13.4 Payment upon Termination Upon any termination of this Agreement, all Fees which are outstanding as at the date of such termination, and all Fees remaining to be paid for the duration of the Subscription Term, shall become immediately due and payable and the Customer shall immediately pay all such unpaid Fees from all Order Forms. In no event shall any termination by Us relieve Customer of the obligation to pay any Fees and/or other amounts payable to Us up to and including the last day of the Subscription Term of all Order Forms.

13.5 Return of Customer Data Upon request by Customer made within 30 days after the effective date of termination of a Purchased Services subscription, We will make available to Customer for download a file of Customer Data in comma separated value (.csv) format along with attachments in their native format. After such a 30-day period. We shall have no obligation to maintain or provide any of Customer Data and shall thereafter, unless legally or contractually prohibited by obligations signed with Employers with access to Customer Data, delete all of Customer Data in Our systems or otherwise in Our possession or under Our control.

13.6 Consequences of Termination Immediately upon the effective date of termination of this Agreement, Customer shall (i) stop using the Services and ensure that any and all Users' access to the Services is blocked, and (ii) return or destroy, at Our option, any and all intellectual property, assets, Confidential Information, or other documentation which belongs to Us.

13.7 Surviving Provisions All provisions of this Agreement that by their nature would be expected to survive the termination or expiration of this Agreement shall survive any termination or expiration of this

Agreement including, without limiting the generality of the foregoing, Sections 4, 7, 8.2, 9, 10, 11.3, 11.4, 12, 13.4, 13.5, 13.6, 13.7, 14, 15 and 16.

14. WHO CUSTOMER IS CONTRACTING WITH, NOTICES, GOVERNING LAW AND JURISDICTION

14.1 General ComplyWorks Ltd. is a company incorporated under the laws of British Columbia with its head office located at Suite 200, 4838 Richard Rd. SW Calgary AB T3E 6L1. Telephone: (403) 219 4792 Facsimile: (403) 253 9647. Electronic mail: support@complyworks.com. Website: www.complyworks.com.

14.2 Manner of Giving Notice Except as otherwise specified in this Agreement, all notices, permissions and approvals hereunder shall be in writing and shall be deemed to have been given upon: (i) personal delivery, (ii) the second business day after mailing, (iii) the first business day after sending by confirmed facsimile, or (iv) the first business day after sending by email. Notices to Customer shall be addressed to the administrator designated by Customer for its relevant Services subscription, and in the case of billing-related notices, to the relevant billing contact designated by Customer.

14.3 Agreement to Governing Law and Jurisdiction This Agreement shall be governed and interpreted according to the laws of the Province of Alberta and the laws of Canada applicable therein (without giving effect to the choice of laws provisions thereof) and each party to this Agreement agrees to attorn to the non-exclusive jurisdiction of the courts of Alberta.

14.4 Waiver of Jury Trial Each party to this Agreement hereby waives any right to jury trial in connection with any action or litigation in any way arising out of or related to this Agreement.

15. LOGO AND COPYRIGHTED MATERIALS GUIDELINES

15.1 Use of ComplyWorks Ltd. Logo(s) ComplyWorks and ComplyWorks Get Ready to Work ("Logo(s)") are property of ComplyWorks Ltd. Printers, contractors, suppliers, employers, clients, graphic artists and any other organizations are able to request permission for use of the Logo(s) by completing the Logo and Copyrighted Materials Permission Form (Appendix A).

15.2 Use of Logo(s) Conditions Use of the Logo(s) is strictly prohibited without the express written consent of ComplyWorks Ltd. (which consent may be arbitrarily withheld). Any use of the Logo(s) must be for a purpose that supports the mission and goals of ComplyWorks Ltd. We reserve the right to request proofs for approval for any and all use of Our Logo(s). Utilization of the Logo(s) in a manner deemed to be inappropriate by Us or that is outside of the scope of the Logo and Copyrighted Materials Permissions Form shall be referred to ComplyWorks Ltd.'s legal counsel for possible prosecution. We also reserve the right and authority to withdraw permission for use of the Logo(s) or trademarked material without prior notice and the right and authority to approve or deny any request permission for use of the Logo(s) or trademarked material.

15.3 Copyrighted and Trademarked Materials COMPLYWORKS, the "Get Ready to Work." logo below in all possible versions, the ComplyWorks swoop graphic below ("Logo(s)"), "Active Compliance Monitor" and the "Get Ready to Work." Slogan (collectively, the "Marks") are all protected under the relevant copyright, trademark and related intellectual property legislation in Canada, the United States of America and/or South Africa. Customer acknowledges and agrees that it will, and will ensure that any User or third party authorized by Us will, only reproduce the Marks in accordance with the strict guidelines We provide and Customer will make no changes or modifications to the Marks (including without limitation to the size, colours, fonts, or shapes). Customer will at all times make clear in any reproduction or use of the Marks

that the Marks are the registered or unregistered Marks of ComplyWorks Ltd. and are being used by Customer under license. Customer shall display the following indicator with every use of the Marks: "© 20XX ComplyWorks Ltd., used under license" or "TM ComplyWorks Ltd., used under license" or for the United States ®ComplyWorks Ltd., used under license".

Get ready to work.®

15.4 Copyright All content included in or made available by Us including through any Service–such as text, graphics, logos, button icons, images, audio clips, digital downloads, data compilations, and solutions–is Our exclusive property or used under license (unless otherwise specified), and is protected by Canadian and international copyright laws. The compilation of all content included in or made available by Us through any Service is Our exclusive property or the property of our licensors and protected by Canadian and international copyright laws.

15.5 Trademarks In addition to the Marks, Our graphics, logos, page headers, button icons, scripts, and service names included in or made available by Us (including through any Service) are, unless otherwise specified, Our trademarks or trade dress in Canada and other countries, or the trademarks of our licensors. Such trademarks and trade dress may not be used in connection with any product or service that is not Ours, in any manner that is likely to cause confusion among consumers or third parties generally, or in any manner that disparages or discredits Us or our licensors.

16. DATA PROTECTION

16.1 Data Protection Customer and ComplyWorks will comply with principles of protecting Personal Information and Data, as well as the provisions of the Data Processing Addendum (DPA) and, if applicable, the Data Processing Terms (GDPR specific provisions) and Standard Contractual Clauses incorporated in this Agreement.

16.2 Privacy Policy Customer agrees that Customer has reviewed and understands our Privacy Policy, posted on www.complyworks.com, and Customer acknowledges and agrees that ComplyWorks may Process (as defined in the DPA) Personal Data (as also defined in the DPA) in accordance with such policy.

17. GENERAL PROVISIONS

17.1 Relationship of the Parties The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, or fiduciary or employment relationship between the parties.

17.2 No Third-Party Beneficiaries There are no third-party beneficiaries to this Agreement

17.3 Waiver and Cumulative Remedies No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right. Other than as expressly stated herein, the remedies provided herein are in addition to, and not exclusive of, any other remedies of a party at law or in equity.

17.4 Severability If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

17.5 Collection Fees Customer shall pay on demand all of Our reasonable fees and other costs incurred by Us to collect any fees or charges due Us under this Agreement.

17.6 Assignment Customer may not assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without Our prior written consent (which consent may be arbitrarily withheld). Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective heirs, personal representatives, successors and permitted assigns.

17.7 Entire Agreement This Agreement, including the DPA and all schedules and appendices hereto and all Order Forms, constitutes the entire agreement between the parties and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. Except as otherwise specified in this Agreement, no modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and either signed or accepted electronically by the party against whom the modification, amendment or waiver is to be asserted. However, to the extent of any conflict or inconsistency between the provisions in the body of this Agreement and any exhibit or addendum hereto or any Order Form, the terms of such exhibit, addendum or Order Form shall prevail. Notwithstanding any language to the contrary therein, no terms or conditions stated in Customer purchase order or other order documentation (excluding Order Forms) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void.

17.8 Language Each of the parties acknowledges having required that this Agreement and all documents, notices, correspondence and legal proceedings consequent upon, ancillary or relating directly or indirectly hereto, forming part hereof or resulting directly or indirectly here from be drawn up in English. Chacun des soussignés reconnait avoir exigé que cette convention ainsi que tous documents, avis, correspondance et procédures légales consécutifs à, ayant rapport directement ou indirectement avec, faisant partie ou découlant de cette convention soient rédigés en anglais.

DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") forms part of the Agreement or other written or electronic agreement between Customer and ComplyWorks for the purchase of Services from Us.

By signing the Agreement, Customer enters into this DPA as an unincorporated professional entity or as a company or other legal entity and, to the extent required under applicable Data Protection Laws, in the name and on behalf of Customer and its Authorized Affiliates, if and to the extent We process Personal Data on behalf of such Authorized Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" shall include the Customer and Authorized Affiliates. All capitalized terms not defined herein shall have the meaning specified in the Agreement.

This DPA shall not replace any comparable or additional rights relating to Processing of Customer Data contained in the Agreement. However, in the event of any conflict, this DPA shall govern with respect to the matters addressed herein.

In the course of providing the Services to Customer pursuant to the Agreement, We may Process Personal Data on Customer's behalf and we each agree to comply with the following provisions with respect to any Personal Data.

DATA PROCESSING TERMS (all jurisdictions)

DEFINITIONS

"**Authorized Affiliate**" means any of the Customer's Affiliate(s) which (a) is subject to the data protection laws and regulations of the European Union, the European Economic Area and/or their member states, Switzerland and/or the United Kingdom, and (b) is permitted to use the Services pursuant to the Agreement between the Customer and ComplyWorks, but has not signed its own Order Form with ComplyWorks and is not a "Customer" as defined under this DPA.

"Canadian Privacy Laws" means the *Personal Information Protection and Electronic Documents Act* and substantially similar provincial legislation, as well as any applicable federal or provincial privacy or data protection legislation applicable to public bodies or public institutions in Canada, each together with the regulations thereto and as amended from time-to-time.

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

"Controller" means the entity which determines the purposes and means of the Processing of Personal Data.

"Data Protection Laws" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states (including, without limitation, the GDPR), Switzerland, the United Kingdom, Canada (including, without limitation, the Canadian Privacy Laws), South Africa and the United States of America and its states (including, without limitation, the CCPA) to the extent applicable to the Processing of Personal Data under the Agreement as amended from time to time.

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

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), including as implemented or adopted under or into the laws of the member states of the European Union and the European Economic Area, Switzerland and the United Kingdom.

"Personal Data" means any information contained or included in Customer Data relating to (i) an identified or identifiable natural person and, (ii) an identified or identifiable legal entity where such information is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

"Processing" means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, accessing, recording, organization, structuring, storage, archiving, modification, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or otherwise, dissemination, communication, or otherwise making available, alignment or combination, restriction, erasure or destruction (and "**Processes**", "**Process**" and "**Processed**" shall be construed accordingly).

"Processor" means the entity which Processes Personal Data on behalf of the Controller, including as applicable any "service provider" as that term is defined by the CCPA or, where applicable, Canadian or other Privacy Laws.

"Regulatory Authority" means any governmental, regulatory or supervisory authority, including any privacy or data protection commissioner or ombudsman, and any industry self-regulatory body or organization, which is responsible for administering and/or enforcing any applicable Canadian or other Data Protection Laws.

"Standard Contractual Clauses" means the agreement pursuant to the European Commission's Implementing Decision EU 2021/914 of 4 June February 2021 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"Sub-processor" means any Processor engaged by ComplyWorks or one of the ComplyWorks's Affiliates engaged in the Processing of Personal Data.

"**Supervisory Authority**" means an independent public authority which is established by an EU or EEA Member State, Switzerland or the United Kingdom, pursuant to the GDPR.

18. PROCESSING OF PERSONAL DATA

18.1 Roles of the Parties Although ComplyWorks and the Customer each acknowledge that their respective status is determined by the Data Protection Laws, if in the course of the Agreement the Customer transfers Personal Data to ComplyWorks for ComplyWorks to Process in the course of providing any Services, or ComplyWorks collects Personal Data on behalf of Customer for the purpose of providing Services to Customer, the parties intend and are of the view that the Customer will be the Controller and ComplyWorks will be a Processor in relation to such Personal Data and that ComplyWorks or ComplyWorks Affiliates will engage Sub-processors in accordance with this DPA. Without limiting the foregoing, the parties agree that any Personal Data that the Customer transfers to ComplyWorks shall remain within the custody and control of the Customer, and as between the Customer and ComplyWorks, the Customer shall be the owner of such data. Notwithstanding the above, ComplyWorks and Customer acknowledge and agree that if Customer shares or authorizes any third party or related party to share Customer Data with any Employer, then such Employer shall also be considered an owner and Controller of such Customer Data.

18.2 Customer's Processing of Personal Data Where the Customer transfers or otherwise makes available Personal Data to ComplyWorks in relation to the Agreement, the Customer warrants and represents that (i) it has the necessary rights to transfer or make available such Personal Data to ComplyWorks (including that it has, or has procured, the necessary legal authority, permissions and/or consents for ComplyWorks to Process the Personal Data to provide the Services); (ii) the Customer's instructions to ComplyWorks comply with (and will not cause ComplyWorks to be in breach of) the Data Protection Laws; and (iii) the Customer has taken reasonable steps to ensure that any Data Subjects are aware of the nature of the Processing to be undertaken, including by providing any notices required by applicable law or Regulatory Authority, or has otherwise complied with applicable Data Protection Laws in relation to informing Data Subjects concerning the Processing of their Personal Data comprised in the Customer Data. The Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which the Customer acquired Personal Data. The Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject, including the rights of any Data Subject that has opted-out from sales or other disclosures of Personal Data to the extent applicable under the CCPA or other applicable Privacy laws.

18.3 ComplyWorks Processing of Personal Data Where ComplyWorks Processes Personal Data as a Processor on the Customer's behalf and as a Processor on an Employer's behalf, ComplyWorks shall:

(a) only Process such Personal Data on behalf of and in accordance with the Customer's and/or Employer's lawful written instructions from time-to-time (including as set out in this

Agreement) or as required for ComplyWorks to provide, manage and facilitate the provision of the Services, but only where such instructions are consistent with the terms of this Agreement and only in respect of the subject matter, duration, nature and purpose of the Services, and the type of Personal Data and categories of Data Subject relevant to the Services;

(b) ensure that only persons authorized by ComplyWorks Process such Personal Data and that such persons are subject to appropriate obligations to maintain the confidentiality of such Personal Data;

(c) without prejudice to Section 13.5 of the User Agreement and Section 24 of the DPA, when ComplyWorks ceases providing the Services to the Customer, subject to Employer's approval, delete all such Personal Data and copies of such Personal Data, unless applicable law or regulation or Employer instruction requires storage of such Personal Data or deletion of Personal Data is not technically possible, using all reasonable efforts.

18.4 Conflicting Instructions The parties agree that if ComplyWorks receives conflicting or inconsistent instructions from Customer and an Employer pursuant to Section 18.3(a), ComplyWorks will notify both the Employer and the Customer and seek clarification as to which instructions shall prevail. To the extent that any conflict or inconsistency remains following ComplyWorks' reasonable attempt to seek clarification, or in the event that the Customer and the Employer cannot agree on the instructions to be provided to ComplyWorks, the Customer agrees that ComplyWorks shall only comply with the Employer's instructions.

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

19. RIGHTS OF DATA SUBJECTS

Data Subject Request. ComplyWorks shall, to the extent legally permitted, promptly notify Customer if ComplyWorks receives a request from a Data Subject to exercise the Data Subject's rights, including, as applicable, rights of access, rights to rectification, restriction of Processing, erasure ("right to be forgotten"), data portability, objection to the Processing, and/or the right not to be subject to an automated individual decision making, each such request being a "Data Subject Request". Taking into account the nature of the Processing, ComplyWorks shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to a Data Subject Request under Data Protection Laws and Regulations. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, ComplyWorks shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request.

20. SUB-PROCESSORS

20.1 Appointment of Sub-processors Customer acknowledges and agrees that (a) ComplyWorks' Affiliates may be retained as Sub processors; and (b) ComplyWorks and ComplyWorks Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. ComplyWorks and any of ComplyWorks Affiliates have entered into a written agreement with each Sub-processor containing data protection obligations with respect to the Customer Data on equivalent terms to this DPA to the extent applicable to the nature of the Services provided by such Sub-processor.

20.2 List of Current Sub-processors and Notification of New Sub-processors. ComplyWorks shall make

available to Customer the current list of Sub-processors for the Services identified in Appendix 1 of the Standard Contractual Clauses attached hereto, as well as a mechanism to subscribe to notifications of new Sub-processors. If Customer subscribes, ComplyWorks shall provide notification of a new Sub-processor(s) before authorizing any new Sub-processor(s) to Process Personal Data in connection with the provision of the applicable Services.

21. SECURITY

21.1 Controls for the Protection of the Customer Data Taking into account the (i) state of the art, (ii) costs of implementation, (iii) nature, scope, context and purposes of the Processing, (iv) the risk and severity of potential harm, and (v) the sensitivity of the information as well as the amount, distribution, and format of the information and the method of storage, ComplyWorks shall maintain appropriate administrative, physical, technical and organisational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data), confidentiality, availability and integrity of Personal Data.

21.2 Data Protection Impact Assessment Upon the Customer's request, and at Customer's cost, ComplyWorks shall provide the Customer with reasonable cooperation and assistance needed to fulfil the Customer's obligation (if any) under the Data Protection Laws to carry out a data protection impact assessment related to the Customer's use of the Services, to the extent the Customer does not otherwise have access to the relevant information, and to the extent such information is available to ComplyWorks.

22. AUTHORIZED AFFILIATES

22.1 Contractual Relationship The parties acknowledge and agree that, by executing the Agreement, the Customer enters into the DPA on behalf of itself and, as applicable, in the name and on behalf of its Authorized Affiliates, thereby establishing a separate DPA between ComplyWorks and each such Authorized Affiliate, subject to the provisions of the Agreement. Each Authorized Affiliate agrees to be bound by the obligations under this DPA and, to the extent applicable, the Agreement. All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and any breach of the terms and conditions of the Agreement by an Authorized Affiliate shall be deemed a breach by the Customer.

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

(a) Except where applicable Data Protection Laws require the Authorized Affiliate to exercise a right or seek any remedy under this DPA against ComplyWorks directly by itself, the parties agree that (i) only the Customer that is the contracting party to the Agreement shall exercise any such right or seek any such remedy on behalf of the Authorized Affiliate, and (ii) the Customer that is the contracting party to the Agreement shall exercise any such rights under this DPA not separately for each Authorized Affiliate individually but in a combined manner for itself and all of its Authorized Affiliates together (as specified, for example, in sub-paragraph (b) below).

(b) The parties agree that the Customer that is the contracting party to the Agreement shall, when carrying out an audit of the procedures relevant to the protection of Personal Data pursuant to this DPA, take all reasonable measures to limit any impact on ComplyWorks and its Sub-Processors by combining, to the extent reasonably possible, several audit requests carried out on behalf of itself and all of its Authorized Affiliates in one single audit. Such audits will also be subject to such rules, restrictions and limitations as ComplyWorks considers necessary or

prudent, in its reasonable discretion, to protect confidential and proprietary information belonging to ComplyWorks and/or third parties or to protect ComplyWorks' networks, systems, property and personnel.

23. CUSTOMER DATA INCIDENT MANAGEMENT AND NOTIFICATION

ComplyWorks shall notify Customer without undue delay after becoming aware of the theft, loss, or accidental or unlawful destruction, alteration, unauthorized disclosure of, or access to, Customer Data which includes Personal Data, transmitted, stored or otherwise Processed by ComplyWorks or its Sub-processors of which ComplyWorks becomes aware (a "Customer Data Incident"). ComplyWorks shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as ComplyWorks deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within ComplyWorks's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Users.

24. RETURN AND DELETION OF CUSTOMER DATA

24.1 Customers without Employer Connections. Without prejudice to Section 13.5 of the User Agreement and Section 18.3 of the DPA, ComplyWorks shall return Customer Data to Customer upon written request from Customer within 30 days of termination of Agreement and, to the extent allowed by applicable law, delete Customer Data within 6 months of the termination of the Agreement, unless deletion of Personal Data is not technically possible, using all reasonable efforts.

24.2 Customers with Employer Connections. For the situations where Customer has authorized the sharing of its Customer Data with Employers, upon termination of the Agreement, ComplyWorks shall act upon the instructions of the Employers regarding data retention process and timelines, which shall be notified to the Customer by ComplyWorks upon termination of the Agreement.

25. LIMITATION OF LIABILITY

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA whether in contract, tort or under any other theory of liability, is subject to the 'Limitation of Liability' Section 11 of the User Agreement, and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement and all DPAs together.

For the avoidance of doubt, ComplyWorks' and its Affiliates' total liability for all claims from Customer and all of its Authorized Affiliates arising out of or related to the Agreement and all DPAs shall apply in the aggregate for all claims under both the Agreement and all DPAs established under the Agreement, including by Customer and all Authorized Affiliates, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Authorized Affiliate that is a contractual party to any such DPA.

DATA PROCESSING TERMS (CCPA specific provisions)

26. Scope of Data Processing Terms (CCPA specific provisions) Sections 26 to 28 apply only with respect to California Personal Information.

27. Roles of the Parties When processing California Personal Information in accordance with Customer

Instructions, the parties acknowledge and agree that Customer is a Business and ComplyWorks is a Service Provider for the purposes of the CCPA.

28. Responsibilities The parties agree that We will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA. ComplyWorks will not (a) sell any personal information; (b) retain, use or disclose any personal information for any purpose other than for the specific purpose of providing the Services, including retaining, using, or disclosing the personal information for a commercial purpose other than the provision of the Service; or (c) retain, use or disclose the personal information outside of the direct business relationship between the parties.

DATA PROCESSING TERMS (GDPR specific provisions)

Sections 29 to 36 apply if and to the extent that Processing of Personal Data by ComplyWorks in connection with the Agreement falls within the scope of the GDPR (which for this purpose means (as applicable) the General Data Protection Regulation (Regulation (EU) 2016/679) as well as any such Regulation as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (known as the UK GDPR)). For the purposes of these GDPR specific provisions, the terms "transfer" and "appropriate technical and organisational measures" shall be interpreted in accordance with the GDPR. In addition to the other provisions of this DPA, to comply with the requirements of applicable law ComplyWorks agrees to the following terms with respect to Processing of Personal Data that is subject to the GDPR (which terms shall prevail in the event of conflict with the other provisions of this DPA):

29. ComplyWorks Processing of Personal Data ComplyWorks will Process Personal Data in accordance with the GDPR requirements directly applicable to ComplyWorks's provision of its Services.

30. Controls Taking into account the nature of ComplyWorks's processing, ComplyWorks shall put in place appropriate technical and organisational measures, insofar as is possible, to assist the Customer to fulfil, at the Customer's cost and to the extent possible, the Customer's obligations to respond to Data Subjects' requests to exercise their rights under the Data Protection Laws over such Personal Data.

31. Accountability Subject to reasonable access arrangements being agreed with ComplyWorks and save for disclosure of information which is confidential and/or privileged (or where access is otherwise restricted by applicable law or regulation), ComplyWorks shall make available to the Customer all relevant information reasonably necessary to demonstrate compliance with the ComplyWorks's obligations under the GDPR and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer, at the Customer's cost.

32. Data Incident ComplyWorks shall notify the Customer without undue delay after becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data which is subject to the GDPR, transmitted, stored or otherwise Processed by ComplyWorks or its Sub-processors of which ComplyWorks becomes aware (a "**Customer Data Incident**"). ComplyWorks shall make reasonable efforts to identify the cause of such Customer Data Incident and take those steps as ComplyWorks deems necessary and reasonable in order to remediate the cause of such a Customer Data Incident to the extent the remediation is within ComplyWorks's reasonable control.

33. Supervisory Authority Cooperation ComplyWorks shall provide reasonable assistance to the Customer in the cooperation or prior consultation with the Supervisory Authority in the performance of its tasks relating to this DPA, to the extent required under the GDPR.

34. Sub-processors The following provisions shall apply in respect of Sub-processors of Personal Data to which the GDPR applies:

34.1 Affiliates The Customer acknowledges and agrees that (a) ComplyWorks's Affiliates may be retained as Sub-processors; and (b) ComplyWorks and ComplyWorks's Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. ComplyWorks will ensure that a written agreement is in place with each Sub-processor containing data protection obligations not less protective than those in the DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor.

34.2 List of sub-processors ComplyWorks shall, following request by the Customer, make available to the Customer the current list of Sub-processors for the Services. Such Sub-processor lists shall include the identities of those Sub-processors and their country of location.

34.3 Objections The Customer may object to ComplyWorks's use of a new Sub-processor by notifying ComplyWorks promptly in writing within thirty (30) days after notification by ComplyWorks. In the event the Customer objects to a new Sub-processor, as permitted in the preceding sentence, ComplyWorks will use reasonable efforts to make available to the Customer a change in the Services or recommend a commercially reasonable change to the Customer's configuration or use of the Services to avoid Processing of Personal Data subject to the GDPR by such new Sub-processor without unreasonably adversely affecting the Customer. If ComplyWorks is unable to make available such change within a reasonable period of time, which shall not exceed thirty (30) days, the Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by ComplyWorks without the use of such new Sub-processor by providing written notice to ComplyWorks.

34.4 Liability ComplyWorks shall be liable for the acts and omissions of its Sub-processors to the same extent ComplyWorks would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise specified in the Agreement.

35. Transfer Mechanism The Standard Contractual Clauses shall, to the extent such transfers are subject to such Data Protection Laws of such territories, apply to any transfers under the Agreement of Personal Data relating to individuals in the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom where such transfer is from any of those territories to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws of those territories.

35.1 SCCs The Standard Contractual Clauses incorporated in this DPA apply to the Services listed in Appendix 1 to the Standard Contractual Clauses (the "SCC Services").

35.2 Inaccurate and incomplete information If the information listed in Appendix 1 to the Standard Contractual Clauses is inadequate or incomplete the Customer shall, if requested by ComplyWorks, provide such information to ComplyWorks promptly for the purpose of giving full effect to the Standard Contractual Clauses.

35.3 Conflict If there is any conflict between the Agreement (including this DPA) and the Standard Contractual Clauses the terms of the Standard Contractual Clauses shall apply in relation to transfers to countries referred to in this Section 35.

35.4 UK data transfers Where the Standard Contractual Clauses apply to transfers of Personal Data relating to individuals in the United Kingdom, the Standard Contractual Clauses shall be read as though the appropriate terminology referring to the UK GDPR were included in place of the EU GDPR, but this shall not be an amendment to the Standard Contractual Clauses or affect their meaning or effect.

36. Further agreements and measures The parties acknowledge and agree that compliance with Data Protection Laws may necessitate that they enter into further agreements or undertake further technical and organisational measures relating to transfers of Personal Data to countries which do not ensure an adequate level of data protection within the meaning of the Data Protection Laws of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, Such measures and agreements may include (without limitation) supplementary measures following transfer impact assessments and provisions concerning the manner in which the parties will notify and process orders, requests or demands made by a non-EEA or non-Swiss or non-UK government or quasi-governmental or other regulatory authority (including law enforcement or intelligence agencies) seeking or requiring access to or disclosure of Personal Data. The parties will each cooperate with the other in relation to agreeing and adopting such measures, provisions and any standard clauses which may be adopted by Switzerland or the United Kingdom or the European Commission to supersede the Standard Contractual Clauses.

DATA PROCESSING TERMS (Canada specific provisions)

37. Scope of Data Processing Terms (Canada specific provisions) Sections 37 to 46 shall apply only with respect to Processing of Personal Data about Canadian Data Subjects on behalf of Customers or Employers operating within Canada.

38. Compliance with Canadian Privacy Laws ComplyWorks and Customer will each Process the Personal Data in accordance with all applicable Canadian Privacy Laws.

39. Protection of Personal Data ComplyWorks will take reasonable steps to protect the Personal Data against such risks as unauthorized access, use, disclosure, destruction or alteration.

40. Consent Requirements Without limiting the generality of Section 5.2 of the Agreement or Section 18.2 of this DPA, Customer shall provide any required notices and obtain any required consents, as needed, for ComplyWorks to access, use, store and otherwise Process Personal Data outside Canada. ComplyWorks will take reasonable steps to ensure that Personal Data transferred outside the province where such information is collected is not used for any unauthorized purpose, and that Personal Data accessed, used, stored or otherwise Processed outside Canada is protected by appropriate safeguards.

41. Customer Record Keeping Obligations. Customer shall keep appropriate records of all notices provided, and all consents obtained, pursuant to Section 5.2 of the Agreement and Sections 18.2 and 40 of this DPA, and Customer shall promptly provide evidence of such notices and consents to ComplyWorks upon ComplyWorks' request.

42. Data Minimization Customer shall ensure that the Customer Data contains only the minimum Personal Data (if any) required by ComplyWorks to provide the Services.

43. Cooperation the parties agree to reasonably cooperate and assist each other to comply with their respective obligations under applicable Canadian Privacy Laws, including, to the extent permitted by applicable laws, to respond to audits, requests, demands and investigations by any Regulatory Authority.

44. Roles and Responsibilities of the Parties ComplyWorks will Process Personal Data as a service provider strictly for the purpose of performing the Services under the Agreement (including as instructed by Customer or an Employer) or permitted by the Canadian Privacy Laws or required by applicable laws. Each party will designate a representative to be responsible for communicating and collaborating with the other party in connection with the matters addressed in this DPA, and each party shall provide the name and contact information of such representative to the other party promptly upon request.

45. Legally Required Changes. ComplyWorks and Customer acknowledge that laws relating to privacy and data protection, including the Canadian Privacy Laws, are evolving and that amendment to the Agreement and/or this DPA may be required to ensure compliance with such developments. The parties agree to take such action as is necessary to implement the standards and requirements of any Canadian Privacy Laws or other privacy and data protection laws applicable to one or both of the parties, including negotiating in good faith to amend the Agreement and this DPA as necessary or prudent for compliance with such laws.

AGREEMENT ACCEPTANCE

The parties' have duly executed this Agreement, including all Schedules and Annexes by electronically accepting the Agreement. If Customer wishes to obtain a physically signed Agreement, please contact privacy@veriforce.com.

SCHEDULE 1 Details of Processing

Duration of the Processing: The duration of data Processing shall be for the term agreed between Customer and ComplyWorks in the Agreement (or an applicable Order Form) which is the duration of the Agreement.

Nature and purpose of the Processing: The scope and purpose of Processing of the data subjects' Personal Data is:

- to provide, maintain and facilitate the Services and Purchased Services as well as to ensure safeguards of the Services and Purchased Services performance, upgrade and improve the functionality of the Services and Purchased Services;
- to provide Customer with access to its Personal Data (including chat content) and maintain this access for the duration of paid usage of the Services and Purchased Services (active subscription) as well as after the subscription is expired (inactive subscription), until the Services and Purchased Services are fully terminated in accordance with this Agreement;

- to secure (establish, investigate or defend) Customer's as well as ComplyWorks' claims that may arise due to the Purchased Services.

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

- Customer contacts and other end users including its employees, contractors, collaborators, applicants, trainees, directors and others whose Personal Data is shared by a Customer in the context of the services provided by ComplyWorks.

Categories of Personal Data: The Personal Data transferred concern the following categories of data in relation to the categories of data subjects described above:

- Identification data (name, surname, address, email address, company, phone numbers, system and devices data and other identifying information);
- Professional identification data (CV, professional status, education, awards, certificates, job description, hierarchical positioning);
- Training records, courses
- Specific incident related data, fit to work information
- Contractor compliance status
- other personal data that may be contained or derived from business related communications and interactions, including chats, phone recordings, emails etc, internal systems and log data

Special categories of data (if appropriate): Customer **may not submit** special categories of data to the Purchased Services. For the sake of clarity special categories of data are Personal Data with information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Competent Supervisory Authority

ComplyWorks EU and UK Representative is based in Ireland; the competent supervisory authority is the Data Protection Commission of Ireland.

SCHEDULE 2 Security and Organizational Measures

ComplyWorks will maintain administrative, organizational, physical, and technical safeguards for protection of the security, confidentiality, availability and integrity of Personal Data uploaded to the Services, as described in this Appendix. ComplyWorks will not materially decrease the overall security of the Services during a Subscription Term.

Security and Organizational measures

a) Access Controls

Outsourced processing: We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II, among other certifications.

Authentication: We implement a uniform password policy for our product. Customers who interact with the product via the user interface must authenticate before accessing non-public Customer Data.

Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in our product is designed to ensure that only the appropriately assigned Users can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key.

i) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented include security group assignment and traditional firewall rules.

ii) Limitations of Privilege & Authorization Requirements

Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Employee roles are reviewed at least once every six months.

Employee Security: All ComplyWorks employees undergo reference checks prior to being extended an employment offer, in accordance with and as permitted by the applicable laws and sign Confidentiality Agreements. All ComplyWorks employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards and sign off on our internal policies annually.

b) Transmission Control

In-transit: We make HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces. Our HTTPS implementation uses industry standard algorithms and certificates.

At-rest: We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel are responsive to known incidents.

Response and tracking: We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to You will be in accordance with the terms of the Agreement.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Backup and recovery: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

SCHEDULE 3 List of sub processors

List of sub-processors can be found here:
https://www.complyworks.com/en/information-security-and-privacy-overview/

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

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

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

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 Two: Clause 8.1(b), 8.9(a), (c), (d) and (e);

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

(iv) Clause 12 – 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);

(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.

MODULE TWO: Transfer controller to processor

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 ([4]) (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 benefiting 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

MODULE TWO: Transfer controller to processor

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([8]) 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

MODULE TWO: Transfer controller to processor

(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.

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(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

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(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 ([12]);

(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

MODULE TWO: Transfer controller to processor

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

MODULE TWO: Transfer controller to processor

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 the Republic of France.

Clause 18

Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(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 the Republic of France.

(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 Details of Processing

MODULE TWO: Transfer controller to processor

The information relevant for this Annex is contained in Schedule 1 of this Agreement.

ANNEX II Technical and organisational security measures

MODULE TWO: Transfer controller to processor

The information relevant for this Annex is contained in Schedule 2 of this Agreement.

ANNEX III List of sub processors

MODULE TWO: Transfer controller to processor

List of sub-processors can be found here:
https://www.complyworks.com/en/information-security-and-privacy-overview/

UK Addendum International Data Transfers **(applicable to transfers of personal data out of UK)**

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

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

Part 1: Tables

Table 1 Parties

See description of Parties on the first page of this Agreement.

Table 2 Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
2	Yes	Yes	General authorisation	30 days	No

Table 3 Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in Schedule 1, Schedule 2 and Schedule 3.

Table 4 Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: x Importer x Exporter

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.

Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

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

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

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

    b. In Clause 2, delete the words:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

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

b. reflects changes to UK Data Protection Laws;

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

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.