END USER LICENSE AGREEMENT

For federal customers only

This End User License Agreement ("EULA"/ "Agreement") applies to customers and users who are accessing or using one or more Services (defined below) on behalf of the United States Federal government (the "or "you" or "Customer", "Licensee"- where Licensee shall also mean the entity acquiring a license in the Services that accompanies this EULA).

The Services shall be provided by International Council of E-Commerce Consultants, Inc ("EC-Council").

This EULA governs your use of the Services provided to you pursuant to an applicable federal procurement instrument which may include a purchase contract, quote, order form, invoice or online procurement process, by whatever name it shall be called (each, an "Order");

If you accept this EULA, then you agree to this EULA unless you already have a signed agreement with EC-Council or its affiliates that includes licensing terms that govern your use of the Services ("Pre-Existing Agreement"). If you accept this EULA on behalf of the Customer , then you represent that you have authority to take those actions, and this EULA will be binding unless the entity already has a Pre-Existing Agreement. If you do not agree to this EULA, do not use the Services.

To the extent that applicable federal laws or regulations (including, without limitation, the Federal Acquisition Regulation (FAR)) prohibit the Customer from accepting this End User License Agreement (EULA) via click-through, electronic acceptance, or other informal means, the terms and conditions of this EULA shall be deemed incorporated by reference into the Order under which the Services are acquired.

The Customer's authorized use of the Services shall constitute acceptance of the EULA to the extent permitted under federal law. In the event of any inconsistency between this EULA and the terms of any Order or related documentation, the terms of this EULA shall control with respect to the use, licensing, and access to EC-Council's Services, except to the extent such inconsistency would cause the Customer to violate applicable federal law or regulation.

You will receive the Services only pursuant to acceptance of an Order either by Contractor or directly by EC-Council as the case may be.

1. Definitions

(a) "**Affiliate(s)**" shall mean an entity that is under direct, indirect or common control of an engaging entity. For clarity, the term "Control" refers to the direct or indirect ownership or control of more than 50% of the voting interests of the engaging entity. Subsequently, the terms "EC-Council's Affiliates" refers the affiliates directly, or indirectly, or commonly controlled or owned by EC-Council.

(b) **"Account**" shall mean the e-learning account created by the User on the Platform;

(c) **"API Connection"** refers to an Application Programming Interface (API) connection that enables the integration of the Services with the Customer's Learning Management System (LMS);

(d) **"Capture the Flag Challenges"/ "CTF Challenges"** means the cybersecurity competition hosted by EC-Council or its affiliates on the Platform where the participants, based on their professional experience and expertise compete in security-themed challenges for the purpose of obtaining the highest score and are expected to "capture the flags"

(e) **"Certification" refers** to the credentials earned by a Certified Member upon successfully completing a certification course offered by EC-Council and which is delivered through iLearn**;**

(f) **"Certified Members"** are the Users who have successfully completed and earned a Certification ;

(g) ***"*Certification Examination*"*** is an assessment designed to evaluate a User's comprehension of EC-Council Official Courseware, leading to certification for the Program;

(h) ***"*Contractor"** shall mean the authorized distributor of EC-Council under this contract with whom EC-Council has a public sector distribution agreement to distribute Services to Customers.

(i) **"Customer" or "Licensee**" means the United States Federal agency or department that is authorized to use the Services pursuant to an Order placed either with the Contractor or EC-Council, but only to the extent the Services are used by the User in their official capacity as a U.S. Federal Government official, employee, or agent, and solely for the internal use of the Customer and its Affiliates. For the purposes of clarity, any User who is not accessing or using the Services on behalf of a U.S. Federal agency or department shall be subject to the Terms of Service available here.

(j) "**Customer Content**" shall mean information, materials, etc. provided by Customer and/or its End Users, regardless of form, including (without limitation) its trademarks, trade names, service marks, logos and designs, and images, graphics, and text, in connection with the use of Service;

(k) "**Data Subject**" is an identifiable natural person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(l) "**EC-Council Legal Documentation**" refers to the Privacy Policy, and Data Processing Agreement, attached as Annexure I and Annexure II to this Agreement, respectively.

(m) **"EC-Council Official Courseware"** shall mean EC-Council course materials, Certification Examination(s) vouchers, preparation materials, labs, instructor-slides, worksheets, drawings and/or diagrams related to such course materials and any accompanying materials for Certification

(n) "**Intellectual Property Rights**" means any right in copyright, database rights, trade secrets, trademarks, tradename, logos, service marks, symbols, trade dress, design, circuit layout, know-how, show-how, plans, studies, concepts, methods, proposals, mathematical models, materials, articles, analysis, trial results, patents, and all rights and forms of protection of a similar nature or having equivalent effect to any of them which may subsist anywhere in the world, whether or not registered and including applications for registration of any of them, and including without limitation all and any goodwill inherent or generated in any of them;

(o) "**iLearn**" shall mean asynchronous, self-study environment which delivers Certification in a streaming video format and includes the following components: (i) e-content with one-year validity; (ii) one examination voucher with one year validity; (iii) self-paced learning videos with one year validity; (iv) iLabs with six months' validity;

(p) **"IMSCC file"** means a standardized ZIP file format that allows components of the Services to be imported into the Customer's Learning Management System (LMS);

(q) **"Labs"** means interactive cyber-security environments comprising of virtual machines that allow Users to practice the cybersecurity concepts and methodologies as part of the Services;

(r) **"Learning Management System" or "LMS"** means a software application or web-based platform used by the Customer to access and utilize Services, in accordance with the terms of this Agreement.

(s) **"Learning Tools Interoperability" or "LTI"** refers to a third-party interoperability standard that enables the Services to be launched and accessed within an LMS. LTI integration allows Users to seamlessly navigate between Services and other online tools within the LMS environment.

(t) **"Log-In Credentials"** means the authentication credentials used to verify the identity of a User, which would grant them access to Services;

(u) "**Microdegree**" means a structured program which may comprise of online videos, eBooks, cloud-based cyber ranges, lab manuals, assessments, or quizzes.

(v) "**Personally Identifiable Data/Personal Data and/or Sensitive Data**" means any information relating to an identified or identifiable natural person ('Data Subject');

(w) "**Platform**" shall mean the EC-Council Learning platform used for accessing Services and viewing and subscribing to video course and delivering Services by EC-Council;

(x) "**SCORM File" or "Shareable Content Object Reference Model File**" means a standardized file format that enables components of the Services to be imported into the Customer's Learning Management System (LMS);

(y) **"Service(s)**" shall mean the suite of services provided by EC-Council that enables the Customer and their Users to access EC-Council's services as provided on the Platform, which may include Microdegree courses, short courses, iLearn, Labs, CTF challenges ,and Certifications. The Service also includes any additional features or integrations that facilitate access to these resources, including but not limited to API connections, LTI (Learning Tools Interoperability), and/or LMS (Learning Management System) integrations;

(z) "**User"** shall mean and include an authorized employee or contractor of the Customer who uses and accesses the Service; and

(aa) **"User License"** means the total number of individual licenses purchased by the Customer under the applicable license plan, which may be assigned to authorized Users for accessing the Services.

1. **Services and Means of Provisioning**.

Upon Contractor's acceptance of your Order, EC-Council shall provide the Services to the Customer in accordance with the terms of this Agreement and as specified in the applicable Order. The Customer may procure the Services based on its requirements. To facilitate access to the Services, the Customer may opt for additional integration services, including but not limited to API Connections, LTI, and/or LMS integration. The terms and conditions governing such additional services shall be set forth in separate addendums, which are annexed hereto and form an integral part of this Agreement. Such addendums shall become effective upon the Customer opting for the respective integrations, and acceptance of any such integration shall be deemed to constitute the Customer's acceptance of the corresponding addendum and its terms.

2. License Tiers and Additional Features.

(a) ***License Tiers.*** EC-Council Learning offers different license options to the Customer, and the Customer may opt for any of the license plans based on their requirements. The specific details of pricing, components will be provided in the Order.

(b) ***Additional Features.*** Customer acknowledges that certain features or functionalities of Service may not be accessible license as per the license granted to the Customer, regardless of whether such features or functionalities are mentioned in the documentation, brochures, specification sheets, etc. Furthermore, Customer understands that accessing such features or functionalities may necessitate the payment of additional fees or the acquisition of supplementary licenses.

3. Users.

(a) ***Log-In Credentials*.** Only individuals who are either employees or contractors of the Customer, as authorized by the Customer, are permitted to utilize the Services via Log-in Credentials shared by EC-Council, which shall be unique to each User and usage of Services are limited to the number specified in the relevant Order. Each User is required to maintain the confidentiality of their Log-in Credentials and must not share them with any other person. The Customer is responsible for ensuring that its Users comply with this Agreement. In the event of any compromise or unauthorized access to any Log-in Credentials, the Customer must promptly notify EC-Council. EC-Council may process Log-in Credentials in connection with the provision of Services or for EC-Council's internal business purposes.

(b) ***Registration of Individual Users***. Depending on the specific License Tiers, registered for, ordered, or renewed by the Customer, the Customer is entitled to designate one of its employees as an admin ("**Admin**"). The Admin as authorized by the Customer, will have the privilege to access User data and content, procure additional licenses, invite Users to utilize the Service's features, and manage Users through the administrative functionalities provided by the Platform. Upon execution of an Order, a predetermined number of employes/contractors may be registered as Users based on the User Licenses procured by the Customer and granted access to Service. It is the responsibility of the Customer or their designated Admin to distribute User License to the Users, who will subsequently be invited to register an Account and gain access to the Service.

(c) ***Modification of User Count. :*** Except for Users availing Certification , the Customer or its designated Admin has the authority to include additional Users at any point during the Initial Term or any Renewal Term, as applicable. In order to access the Service, payment must be made immediately for each newly added User. The payment amount will be prorated based on the number of days remaining in the Customer's existing Term and will be paid by the Customer accordingly. It is important to note that the number of individual Users allowed in the Customer's subscribed to Service cannot be reduced during the Term, and no refunds will be granted for licenses that remain unused or unassigned.

(d) ***Reallocation of User License:*** Except for Users availing Certification, the Customer shall have the right to reallocate User Licenses assigned under this Agreement. In the event that a User is no longer employed by the Customer , the Customer may, at its sole discretion, reassign the remaining term of that User License to another User, provided that such reallocation does not extend the original license term or increase the total number of User Licenses procured by the Customer under the relevant Order.

(e) ***Non-Transferability of User Access***. Except as permitted under Clause 4(d) above, the Customer acknowledges that access to the Services is intended solely for the individual Users designated by the Customer or its Admin. Unless otherwise expressly permitted in an applicable Order or under Clause 4(d), such access is non-transferable and may not be shared, transferred, or reassigned to any other individual. The Customer shall ensure that its Users do not provide or grant access to the Platform to any individual who is not a User.

(f) **Proctoring**: Users may give Certification examinations: (a) via-remote proctoring services provided by EC-Council directly subject to additional fees as may be provided in the Order or any other Documentation; or (b) or via a third-party remote proctoring service provider which shall be designated by EC-Council.

4. Fees and Payments.

(a) ***Fees and Payment Terms:*** The Customer is responsible for paying EC-Council the specified fees and any other amounts due under this Agreement, as outlined in the applicable Order, from the Start Date, irrespective of allocation of the licenses by the Customer. Unless otherwise stated in the Order, all amounts owed by the Customer must be paid within fifteen (15) days of the date of the invoice. Subject to Prompt Payment Act (31 USC 3901 et seq) and Treasury regulations at 5 CFR 1315, the Customer shall make payments timely and any unpaid amounts beyond the due date may incur finance charges equal to 2% of the outstanding balance per month or the maximum rate allowed by applicable laws, whichever is lower.. All payments are to be made in USD, unless specified otherwise in the Order.

(b) ***Excess Usage***. If the Customer uses Service in violation of the granted scope, such as unauthorized rotation of User Licenses or adding active Users exceeding the limits specified in the Order, it may be considered "Excess Use." EC-Council reserves the right, at its sole discretion, to invoice the Customer for Excess Use at the rates defined in the applicable Order or, if not specified, at EC-Council's current list price for the features included in the Customer's plan for such Excess Use.

(c) ***Taxes.*** Subject to applicable laws and regulations, including GSAR Clause 552.212-4(k), the Customer is responsible for all taxes, duties, bank charges, and other governmental charges resulting from their purchase of the license, including any withholding taxes. The Customer agrees to pay any additional taxes necessary to ensure that the net amounts received by EC-Council, after deducting all taxes, are equal to the amounts that EC-Council would have been entitled to under the Order if such additional taxes did not exist. Further, if Customer is a tax-exempt entity under applicable federal, state, or local laws, Customer shall provide EC-Council with appropriate documentation evidencing such tax-exempt status, including any applicable exemption certificates, upon execution of this Agreement or as soon as reasonably practicable thereafter. EC-Council shall not be obligated to honor any tax exemption unless and until such documentation has been received and verified. Customer shall promptly notify EC-Council of any changes to its tax-exempt status and provide updated documentation as necessary.

(d) ***Order and Billing:*** An Order may be issued either by the Contractor or EC-Council directly to the Customer, which shall include details such as the number of User Licenses, license term, billing, payment terms, and other relevant information. The Customer acknowledges and agrees that any EC-Council Affiliate is authorized to issue an Order for the Services, and the Customer shall make payments directly to the entity that issued the respective Order, in accordance with the terms specified therein.

(e) All fees are non-cancellable and non-refundable.

5. Grant of License and Restrictions on Use.

(a) ***Grant.*** Upon acceptance of your order by the Contractor or by EC-Council and subject to the terms and conditions set forth in this Agreement, EC-Council grants Customer a limited, worldwide, non-exclusive, non-transferable license to allow use of Services by authorized Users as per number of User Licenses procured by the Customer. The Customer shall use the Services solely for internal purposes of the Customer. The details of the number of User Licenses procured by the Customer shall be captured in the Order. Customer acknowledges and agrees that any breach of the terms and conditions of this Agreement by any of its Users will be deemed a breach by Customer. Further, if the Customer violates any of the terms, the Customer's rights under this section may be terminated in accordance with the Contract Disputes Act.

(b) ***Restrictions on use.*** The Customer will use Services in compliance with applicable law and will ensure that each of their Users comply with applicable laws while using Services. Customer acknowledges that the Customer shall neither themselves nor procure to, without limitation:

(i) use Services for any illegal purpose or in violation of any local, state, national or international law;

(ii) reverse engineer, modify, decompile, or disassemble, modify, adapt, translate, copy Service either whole or in part and/or any associated documentation or software made available as part of Services;

(iii) reproduce, redistribute, transmit, assign, sell, broadcast, rent, share, lend, modify, adapt, edit, create derivative works of, license, capture, download, save, upload, print, or otherwise retain information and content available on the Platform and provided to Customer through Services;

(iv) permit unauthorized access to Customer's Account;

(v) remove, delete, obfuscate or modify any trademark or copyright notices and/or legends;

(vi) violate, encourage others to violate, or provide instructions on how to violate, any right of a third party, including by infringing or misappropriating any third-party intellectual property right;

(vii) use Services to violate the security or integrity of any network, computer or communications system, or breach the security mechanisms of the Platform. Such behavior may result in criminal or civil liability;

(viii) interfere with the operation of Services or any user's enjoyment of the Service, including by: (a) uploading or otherwise disseminating any virus, adware, spyware, worm, or other malicious code; (b) making any unsolicited offer or advertisement to another user of the Service; (c) collecting or sharing personal information about another user or third party without consent; or (d) interfering with or disrupting any network, equipment, or server connected to or used to provide the Service;

(ix) attempt to gain unauthorized access to the Platform or assist others to do so;

(x) sell or otherwise transfer the access granted under this Agreement or any right or ability to view, access, or use any materials made available via the Service

(xi) post to the discussion forums or any other portion of the Platform any inappropriate, offensive, racist, hateful, sexist, pornographic, false, misleading, infringing, defamatory, or libelous content

(xii) archive, reproduce, distribute, modify, display, perform, publish, license, create derivative works from, offer for sale, or use (except as explicitly authorized in this Agreement and Terms of Service) content and information contained on or obtained from or through the Services

(xiii) circumvent, remove, alter, deactivate, degrade or thwart any of the content protections in the Services;

(xiv) use any robot, spider, scraper or other automated means to access the Services;

(xv) insert any code or product or manipulate the content of the Services in any way; or use any data mining, data gathering or extraction method;

(xvi) upload, post, e-mail or otherwise send or transmit any material designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment associated with the Services, including any software viruses or any other computer code, files or programs.

(c) **Grant of License by the Customer:** Customer shall be solely responsible for the accuracy of all Customer Content provided in connection with Customer's use of Services. Customer grants limited, non-exclusive, irrevocable, and non-transferable right to use the Customer Content solely for the purpose of accessing and using Services. When accessing and using Services, Customer shall not include Customer Content that is illegal, harmful, obscene, offensive, inappropriate, libelous, tortious, defamatory, threatening, abusive, objectionable, infringing, hateful or that violates any applicable law or regulation, contract, privacy or any other third party right, or that otherwise exposes EC-Council to civil or criminal liability. Services may not be used in a manner which purposely alters or forges your identity for the purpose of creating a deception or impersonating identity information.

6. Modification of Service.

EC-Council reserves the right to make modifications or discontinuations to any or all of the Service, including any Microdegrees, video courses or Certifications provided as part of the Services, either in part or in its entirety, with or without notice to the Customer. This includes the potential limitation or discontinuation of specific Service features. EC-Council shall not be held liable for any changes to the Service, including any paid functionalities, or for any suspension or termination of the Customer's access to the Service. To ensure the preservation of Customer Content, it is recommended that the Customer retains copies of any uploaded or input data in the Service, in case access to Customer Content is affected by future modifications to the Service. In the event that EC-Council discontinues or materially diminishes functionality of a Service that Customer has contracted for, Customer shall be entitled to a pro rata refund for any fees paid not used.

7. Term and Termination.

(a) This Agreement will become effective only after EC-Council notifies the Customer of its acceptance of the Order. This notification—sent in writing or electronically—may also include access details for the Platform. The Agreement shall be deemed accepted and binding on both parties from the date of this notification. Each Order will remain in effect for the duration specified in it (" ***Order Term***") and may be terminated only as provided under Section 7(b) .

(b) ***Termination for Material Breach*.** If the Customer is an "executive agency" of the United States Government (as defined by 41 USC 7101-8), then all Claims (as defined in FAR 52.233-1-c) by EC-Council against the United States for any alleged breach of this Agreement must be brought as a dispute as set forth in the Contract Disputes Act (41 USC 7101).

(c) ***Reserved.***.

(d) ***Post-Termination Obligations*.** If this Agreement is terminated for any reason, (a) Customer will pay to EC-Council any fees or other amounts that have accrued prior to the effective date of the termination, (b) any liabilities accrued prior to the effective date of the termination will survive, and (c) the following clauses – Clause 6(b), 7(d), 8, 9, 10, 11, 12, 13, 16, 18, 19 – shall survive the termination of an Order or this Agreement.

8. **Covenants by Parties:**

(a) Parties will comply with all applicable laws and regulations pertaining to Services including without limitation the applicable data protection laws such as GDPR including its amendments from time to time and the protection of trademarks and copyrights.

(b) Customer will ensure each of their User must keep the Log-In Credentials in connection with the use and access of Service confidential and not disclose any such credentials to any third party. Each Log-In credential shall be unique and allows only one User to access Service and/or Platform. The Customer and/or its User(s) shall not share one User's credentials at any cost with any other User and/or with any third party. In addition, the Customer shall promptly notify EC-Council in the event of any accidental disclosure of Log-In Credentials or upon the termination of any User who had access to such credentials, so that the credentials can be deactivated or changed if the User License has been reallocated to another User for the remaining term of the license. EC-Council is not responsible for (i) User's access to the Internet, (ii) interception or interruptions of communications through the Internet, (iii) changes or losses of data through the Internet, or (iv) your hardware capacity and/or its conditions to run Service.

(c) The Customer acknowledges that EC-Council may suggest licenses to Customer based on the information and preferences the Customer provides regarding their Users' skills and desired career path. However, EC-Council will not be held accountable or liable for any licenses the Customer chooses to subscribe. It is sole responsibility of the Customer to assess the appropriateness of a license as per their requirement. EC-Council provides recommendations, but the final decision and suitability of the license rests with the Customer. No refunds shall be provided in this situation.

9. Confidentiality.

(a) Customer acknowledges that the Service and related documentation, tools, metadata, trade-secret, source code, and other confidential information, if any, that may be provided by EC-Council or its authorized representative (collectively "Confidential Information") is confidential information of EC-Council.

(b) Subject to the Freedom of Information Act ("FOIA") (5 U.S.C. §552)**,** Customer agrees not to disclose the Confidential Information to third parties or use the Confidential Information other than in connection with its license rights under this Agreement. Customer will use at least the same security measures as the Customer uses to protect their own confidential and trade secret information but no less than reasonable measures to protect the Confidential Information. Confidential Information shall not include information:

(i) already in your possession at the time of disclosure,
(ii) that is or later becomes part of the public domain through no fault of yours, or
(iii) is required to be disclosed pursuant to law or court order provided that you shall notify EC-Council prior to such required disclosure and assist EC-Council in preventing or limiting such required disclosure.

(c) EC-Council acknowledges that U.S. Federal Agencies may be required to disclose information requested under FOIA unless an exemption applies. The EC-Council Legal Documentation, Services, and EC-Council materials are EC-Council's Confidential Information and are exempt from disclosure under FOIA. Customer must notify EC-Council in writing prior to releasing any EC-Council Learning Documentation, Services, and/or EC-Council materials in response to a FOIA request and will provide EC-Council the opportunity to review and object to the proposed disclosure.

(d) Reserved.

(e) If the Customer provides EC-Council with any information marked as confidential for the purpose of receiving the Services, EC-Council shall maintain the confidentiality of such information for the Term of the Agreement and shall not disclose it to any third party, except as required to provide the Services or as otherwise required by law.

10. Intellectual Property.

(a) The Customer agrees that all the materials, documents, products, and services, including all copyrights, trademarks, patents, trade secrets and other intellectual property, whether registered or un-registered, or in the application process developed by EC-Council and provided through Services are the property of EC-Council, its Affiliates, directors, officers, employees, agents, suppliers, or licensors.

(b) Customer acknowledges that the software, the technology underlying Services, and all other software, designs, materials, information, communications, text, graphics, links, electronic art, animations, illustrations, artwork, audio clips, video clips, photos, images, and other data or copyrightable materials, including the selection and arrangements thereof, provided or made available to Customer in connection with Service are the proprietary property of EC-Council and/or its affiliated and/or third party providers and suppliers (the "Third Parties"). Unless otherwise specified, when any content is downloaded to your computer and/or any other device, the Customer does not obtain any ownership interest in such content or any use of the content for any other purpose. EC-Council reserves all rights not expressly granted to the Customer.

(c) The Customer agrees that they will not reproduce or redistribute EC-Council's Intellectual property in any way.

11. Warranties and Disclaimer.

(a) ***Mutual Warranties***. Each Party represents and warrants to the other that: (a) this Agreement has been duly executed and delivered and constitute a valid and binding agreement enforceable against such Party in accordance with its terms and (b) no authorization or approval from any third party is required in connection with such Party's execution, delivery, or performance of these terms.

(b) EC-COUNCIL WARRANTS THAT THE SERVICE AND PLATFORM WILL, FOR A PERIOD OF SIXTY (60) DAYS FROM THE DATE OF YOUR RECEIPT, PERFORM SUBSTANTIALLY IN ACCORDANCE WITH SERVICE AND PLATFORM WRITTEN MATERIALS ACCOMPANYING IT. EXCEPT AS EXPRESSLY SET FORTH IN THE FOREGOING, EXCEPT FOR ANY EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN THIS SECTION 12 OR AN ORDER OR ADDENDUM, EC-COUNCIL MAKES NO ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND WHETHER EXPRESS, IMPLIED (EITHER IN FACT OR BY OPERATION OF LAW), OR STATUTORY, AS TO ANY MATTER WHATSOEVER. EC-COUNCIL EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, ACCURACY, TITLE, AND NON-INFRINGEMENT. EC-COUNCIL DOES NOT WARRANT AGAINST INTERFERENCE WITH THE ENJOYMENT OF THE SERVICE. EC-COUNCIL DOES NOT WARRANT THAT THE SERVICE, PLATFORM ARE ERROR-FREE OR THAT OPERATION OF THE SERVICE WILL BE SECURE OR UNINTERRUPTED. EC- COUNCIL DOES NOT WARRANT THAT ANY INFORMATION PROVIDED BY THE SERVICE OR PLATFORM IS ACCURATE OR COMPLETE OR THAT ANY SUCH INFORMATION WILL ALWAYS BE AVAILABLE. EC-COUNCIL EXERCISES NO CONTROL OVER, AND EXPRESSLY DISCLAIMS ANY LIABILITY ARISING OUT OF OR BASED UPON THE RESULTS OF, CUSTOMER'S USE OF THE SERVICE OR PLATFORM.

12. Indemnification

(a) **By EC-Council:** EC-Council shall have the right to I intervene to defend the Customer against any third-party claim alleging that the Services provided under this Agreement infringe such third party's Intellectual Property Rights or EC-Council's breach of applicable laws and shall indemnify the Customer against any resulting damages, reasonable legal fees, and related costs and expenses ("Losses") that are finally awarded by court of competent jurisdiction or settled with EC-Council's consent. If any portion of the Services becomes, or in EC-Council's reasonable opinion is likely to become, the subject of such infringement claim, EC-Council may, at its discretion and expense:

(i) modify the Services to make them non-infringing without materially reducing their functionality;
(ii) obtain a license to allow continued use of the Services by the Customer; or
(iii) terminate the affected Order(s) or this Agreement and issue a pro-rated refund for any Services not delivered beyond the termination date.

This clause sets out EC-Council's entire liability and the Customer's exclusive remedy with respect to any claim that the Services infringe third-party intellectual property rights. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. EC-Council shall have no obligation under this clause if the claim arises from:

(i) use of the Services by the Customer in violation of the terms of this Agreement; or
(ii) modification of the Services by or on behalf of the Customer without EC-Council's prior written approval.

(b) Each Party shall be liable to the User/ Data Subject, and the User/Data Subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the Data Subject by breaching the third-party beneficiary rights under the terms of this Agreement or Data Processing Agreement that is incorporated by reference into this Agreement. The Customer further acknowledges that if EC-Council is held liable for any third-party claims relating to breach of third-party beneficiary rights then EC-Council shall be entitled to claim back from the Customer that part of the compensation corresponding to their responsibility for the damage.

13. **Mutual Limitation of Liability.**

(a) Except in connection with the Customer's obligation to pay for the Services, the Customer's breach of the License Grant or License Conditions under this Agreement, or any infringement of EC-Council's Intellectual Property Rights, neither party shall be liable for any loss of profits, income, or savings, or for any consequential, incidental, special, punitive, or indirect damages, whether arising in contract, tort, warranty, or otherwise—even if such damages were foreseeable or the party had been advised of their possibility. The foregoing limitation of liability shall not apply to (1) personal injury or death resulting from Licensor's negligence; (2) for fraud; or (3) for any other matter for which liability cannot be excluded by law.

(b) Except Customer's obligation to pay for the Services, the Customer's breach of the License Grant or License Conditions under this Agreement, or any infringement of EC-Council's Intellectual Property Rights, each party's total aggregate liability to the other party shall not exceed the total amount actually paid by the Customer to EC-Council in the twelve (12) months preceding the event giving rise to the claim.

14. **Export Laws.**

Customer may not use or otherwise export or re-export EC-Council Learning Services except as authorized by United States law and the laws of the jurisdiction in which EC-Council Learning Services were obtained. Without limitation, EC-Council Learning Services may not be exported or re-exported (a) into (or to a national or resident of) any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Person's List or Entity List. By using EC-Council Learning Services, you represent and warrant that you are not located in or under control of, or a national or resident of any such country or on any such list.

15. Anti-Corruption.

Neither party has received, nor has been offered, any unlawful or improper bribe, kickback, payment, gift, or item of value from any employee or representative of the other party in relation to this Agreement. However, customary gifts and entertainment provided in the ordinary course of business shall not be deemed a violation of this restriction.

16. Data Security.

(a) ***By Customer.*** The Customer is solely responsible for ensuring that the Customer Content generated via Service is appropriate for Customer's intended use and Customer is solely responsible to maintain the security of Customer Content

(b) ***By EC-Council.*** If and to the extent that the EU Directive 95/46/EC, the EU General Data Protection Regulation (EU) 2016/679 (together with any transposing, implementing, or supplemental legislation, "GDPR"), and/or any other applicable data protection and privacy laws apply to the processing of Personal Data (as defined under the GDPR or relevant legislation), EC-Council shall process such Personal Data on behalf of the Customer in accordance with a Data Processing Agreement ("DPA"), which is incorporated by reference into this Agreement.

17. Third-Party Terms and Linked Websites.

(a) ***Third-party Services and Linked Websites:*** EC-Council may offer tools within the Services that allow you to export information, including Customer Content, to third-party services. This can be done through features like linking your Account with accounts on platforms such as Twitter or Facebook, or by utilizing third-party buttons like "like" or "share." By using these tools, you authorize EC-Council to transfer the information to the respective third-party service in accordance with Federal privacy and data protection regulations . Please note that third-party services operate independently from EC-Council, and to the maximum extent permitted by law, EC-Council assumes no responsibility for how these services utilize your exported information. Services may also contain links to third-party websites. These linked websites are not under the control of EC-Council, and EC-Council is not liable for their content. It is advisable to review the terms of use and privacy policies of any third-party services before sharing Customer Content or information with them. Once sharing occurs, EC-Council will have no control over the shared information.

(b) ***Third-Party Software***. Service may include or incorporate third-party software components, commonly available under licenses that grant recipients broad rights to copy, modify, and distribute such components ("Third-Party Components"). While the Service is provided to you under this Agreement, it does not restrict or prevent you from obtaining Third-Party Components under the relevant third-party licenses.

18. **Governing Law**.

This Agreement and any disputes arising out of or related hereto shall be governed by and construed in accordance with the Federal laws of the United States, without giving effect to its conflicts of laws rules, and will be subject to the exclusive jurisdiction of the federal courts located in New Mexico. Notwithstanding the foregoing, each party reserves the right to file a suit or action in any court of competent jurisdiction as such party deems necessary to protect its Intellectual Property Rights or other proprietary rights. The United Nations Convention on the International Sale of Goods and the Uniform Computer Information Transactions Act do not apply to this Agreement.

19. **Assignment.**

Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the prior written consent of the other party (not to be unreasonably withheld), except that either party may assign this Agreement in its entirety, without the consent of the other party, to (a) an Affiliate; or (b) in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party. Customer may assign to a successor agency as part of formal reorganization provided that Customer is authorized to do so by FAR 42.1204 or other applicable agency supplement, law, or regulation. Any attempt by a party to assign its rights or obligations under this Agreement in breach of this Section 20 shall be void and of no effect. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

20. **Publicity**.

EC-Council reserves the right refer to Customer as one of its Customer on EC-Council Learning website and in other marketing material, including a joint press release to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71. Customer grants permission to EC-Council to use Customer's trademark and/or logo on EC-Council Learning's website, or any other marketing material solely for the purpose of referring to Customer. The Customer will retain all title and rights to such trademarks and/or logos and EC-Council shall use Customer's trademarks and/or logos only for the purpose as defined herein. The Customer may promptly notify EC-Council in writing at legal@eccouncil.org should they have a good faith belief that their trademark or logo as being used on EC-Council Learning's website is beyond the scope of authorization granted or may be infringing upon Customer's rights. EC-Council strongly recommends that the Customer amicably discusses the issue regarding use of Customer Content with us before initiating any formal dispute.

21. **Force Majeure**.

In accordance with GSAR Clause 552.212-4(f), Except for payment obligations, neither party will be responsible for failure of performance due to an event beyond the affected party's reasonable control, including accidents, severe weather events, acts of God, actions of any government agency, endemic and/or pandemic, acts of terrorism, or the stability or availability of the Internet or portions thereof.

22. Subcontractors (including Other EC-Council Entities)

(a) EC-Council may use other EC-Council Affiliates (each of which is a separate legal entity) to provide EC-Council Learning Services. We remain solely responsible for EC-Council Learning Services.

(b) The Customer agrees, and shall ensure that its subsidiaries, affiliates, and related entities do not bring any claim (including negligence) against EC-Council or any of its Affiliates in connection with the provision of the EC-Council Learning Services, except against the specific EC-Council entity identified in the applicable Order. All disputes shall be subject to the provisions set forth in Clause 20.

(c) Clause 23 is for the benefit of other EC-Council Affiliates. Customer agrees that each of the other EC-Council entities may rely on clause 23 as if they are a party to this Agreement. Each Affiliate that assists in providing EC-Council Learning Services relies

on the protection in clause 34.

23. **Survival.**

In addition to the provision under Clause 7(d), the provisions of this Agreement which by their terms call for performance subsequent to termination of the Agreement or an Order, shall so survive such termination, whether or not such provisions expressly state that they shall so survive.

24. **Waiver**.

Failure to enforce any right under this Agreement will not waive that right.

25. **Entire Agreement.**

This Agreement, including relevant Orders, addendums, amendments, and any annexures constitutes the entire agreement between the parties with respect to the use of the EC-Council Learning Services hereunder and supersedes all prior or contemporaneous understandings regarding such subject matter.

26. **Amendment; Modifications.**

No amendment to or modification of this Agreement will be binding unless in writing and signed by EC-Council. The parties hereto confirm that they have requested that this Agreement and all related documents be drafted in English. Should this Agreement be translated into any other language then in case of conflict, the English version of this Agreement shall always prevail over translated version.

27. U.S. Government Restricted Rights.

The Services and the underlying software are "commercial items", "commercial computer software", as that term is defined in 48 C.F.R. §2.101. Accordingly, the Customer will receive only those rights with respect to the Service and EC-Council Documentation as are granted to all other end users under license, in accordance with (a) 48 C.F.R. §227.7201 through 48 C.F.R. §227.7204, with respect to the Department of Defense and their contractors, or (b) 48 C.F.R. §12.212, with respect to all other U.S. Government licensees and their contractors.

28. Addendums:

The LTI, LMS, and API Integration Addendums incorporated into this Agreement shall become applicable to the Customer upon the Customer's use of such integration services or if specified in the Order. If the Customer wishes to avail any of these integration services and they are not already specified in the Order, the Customer shall either raise a new Order or notify EC-Council accordingly. The terms of the relevant Addendum shall be deemed accepted and binding on the Customer upon the use of the respective integration service, regardless of whether a separate Order has been issued.

29. **Order of Precedence**

In this Agreement, the following documents will be read in the following order of preference (in order from highest to lowest):

a) Order
b) Addendums
c) Terms
d) EC-Council Legal Documentation
e) other documents created in accordance with this Agreement or incorporated by reference.

LEARNING MANAGEMENT SYSTEM (LMS) ADDENDUM

This Addendum shall come into effect on the date the Customer starts using the benefits as outlined here and will be incorporated as part of the Agreement.

For the purposes of this Addendum, EC-Council shall provide the Services and their components in an IMSCC file format ("LMS Materials"), which the Customer may upload to its Learning Management System (LMS) solely to make such materials accessible to Users for their personal, non-commercial use. Any use of the LMS Materials beyond this defined purpose under the Agreement (the "Purpose"), including general production or broader distribution, is strictly prohibited.

1. Definitions

For the purpose of this Addendum, the capitalized terms shall have the same meaning as provided in the "Definition" clause of the Agreement.

2. Effective Date

This Addendum shall come into effect on the date the Customer starts using the benefits as provided herein.

3. Customer Obligations, Representations and Covenants:

(a) The Customer shall not copy or distribute Services and/or LMS Materials for purposes other than for the purpose defined in the Agreement and this Addendum.

(b) The Customer shall not analyze, decompile, reverse engineer, reproduce, or assist any third party to analyze, decompile or reverse engineer any information/material that belongs to EC-Council, including but not limited to the Services, LMS Materials for any purpose whatsoever.

(c) The Customer shall not replicate any of the components of Services or LMS Materials in any other e-learning, mobile, electronic, or video- based learning platform, except as authorized under this Agreement. The Customer shall not create any derivative works including but not limited to ancillary products such as lab solutions, video solutions, and e- learning solutions, of the Services without the written consent of EC-Council.

(d) The Customer shall ensure it shall not distribute, transmit, sell, publish, reproduce, replicate the LMS Materials whether partly or fully, in any form or medium and shall not divulge the content of LMS Materials other than for the defined Purpose to any person.

(e) The Customer shall use the LMS Materials only in conjunction with the official the Services and not in isolation.

(f) The Customer shall not bundle LMS Materials or Services with any other third party services.

(g) The Customer shall only integrate the LMS Materials in the LMS being used by Customer upon prior written authorization by EC-Council.

(h) The Customer covenants that the LMS Materials may contain EC-Council's logo or watermark. The Customer shall not remove or blur the embedded EC-Council logo or watermark in the Confidential Information provided to the Customer by EC-Council.

(i) The Customer acknowledges that all EC-Council materials are copyrighted and may not be reproduced, copied, or provided in any manner other than approved distribution under this Agreement. EC-Council reserves the right in its sole discretion to require the removal of EC-Council's materials, including but not limited to courses, video courses, LMS Materials from any site which EC-Council deems unacceptable or inconsistent with EC-Council's policies.

(j) To the extent permitted by applicable Law, Customer shall not and shall prevent "grey market" sales of LMS Materials and/or Services and, at a minimum, utilize safeguards, not lesser than the safeguards adopted by the Customer to safeguard its own proprietary materials, to prevent such "grey marketeering".

(k) The Customer acknowledges that the LMS Materials and other EC-Council materials are proprietary information of EC-Council which are unique and valuable and any threatened breach or actual breach of proprietary information may result in immediate and irreparable harm, damage and/or injury to EC-Council for which there might not be an adequate remedy at law; therefore, the Parties agree that in the event of a breach or threatened breach of this Agreement, EC-Council shall be entitled to seek an injunction or any other order of a court of competent jurisdiction in addition to, and not in lieu of, any other available legal or equitable remedies.

4. Term and Termination

(a) The term of this Addendum shall be coterminous with the term of the Agreement or Order(s), however termination of this Addendum shall not affect the validity of the Agreement.

(b) Termination : When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, EC-Council shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

(c) Upon termination of the Agreement or the Addendum, subject to applicable laws, the Customer shall return and/or destroy all the proprietary information, LMS Materials, including but not limited to the back-up copies of EC-Council's proprietary materials, if any, immediately upon request by EC-Council. Any destruction that is carried out shall be certified in writing to EC-Council by the authorized officer or director of the Customer supervising such destruction. To the extent destruction is not reasonably practicable due to significant time and costs associated with inactive electronic data or data in other storage devices, the Customer hereto agrees to continue to comply with the protections set forth herein until it is returned or destroyed.

(d) Subject to applicable laws, upon termination of this Addendum, all payment obligations shall become due immediately.

LEARNING TOOLS INTEROPERABILITY (LTI) ADDENDUM

This Addendum shall become effective on the date the Customer begins using the benefits outlined herein and shall be deemed incorporated into the Agreement. It sets forth the terms and conditions under which the Customer is authorized to enable User access to the Services via LTI integration.

1. Definitions

For the purpose of this Addendum, the capitalized terms shall have the same meaning as provided in the "Definition" clause of the Agreement, unless specifically defined herein:

2. Effective Date and Term

This Addendum shall come into effect on the date the Customer starts using the benefits as provided herein. The term of the Addendum shall be coterminous with the Agreement or the Order

3. Terms of integration:

(a) EC-Council grants the Customer a non-exclusive, non-transferable, limited license to access and use the Platform via LTI integration solely for the purpose of delivering the Services to its Users.

(b) EC-Council shall provide the Customer with the necessary credentials, documentation, and technical support to enable LTI integration with the Customer's LMS.

(c) Tool Description, including specific application(s) and/or product(s) names shall be provided in the relevant Order capturing the details of LTI integration.

(d) The Customer is responsible for the integration of the Platform LTI link into its LMS, ensuring compatibility and functionality. The Customer must ensure that the integration complies with LTI standards and does not negatively impact the performance or security of the Platform.

(e) The Customer agrees to adhere to all LTI guidelines and standards as provided by EC-Council and IMS Global Learning Consortium.

(f) The Customer agrees and acknowledges that they agree to be billed on actual usage basis post LTI integration of the resources to their LMS, whether or not such usage is provided in an itemized invoice and/or Order.

(g) The Customer agrees that they shall be provided with full trust, billable consumption links only once they have tested the staging links in their own environment. The Customer shall be solely responsible for testing the staging or full trust billable consumption links on their environment.

(h) By testing the staging links, accepting the full trust and billable links and by utilizing the resources monthly, the Customer agrees to be bound by the terms of this Addendum and the payment obligation for the actual usage of the resources on the Platform.

(i) All data generated or collected through the use of the Platform via LTI, including User data, course progress, and performance metrics, shall remain the property of EC-Council.

(j) Customer is granted limited rights to access and use this data solely for the purpose of providing the Services to Users. Any other use, including data mining or analytics, requires prior written consent from EC-Council.

(k) The Customer must implement and maintain appropriate security measures to protect the data exchanged through LTI integration from unauthorized access, disclosure, or alteration.

(l) The Customer agrees to keep all LTI credentials, documentation, and other proprietary information confidential and not to disclose it to any third party without the prior written consent of the Customer.

4. **Termination:**

(a) .

(b) Upon termination of the Agreement or the Addendum, subject to applicable laws, the Customer shall return and/or destroy all the proprietary information, including but not limited to the back-up copies of EC-Council's proprietary materials, if any, immediately upon request by EC-Council. Any destruction that is carried out shall be certified in writing to EC-Council by the authorized officer or director of the Customer supervising such destruction. To the extent destruction is not reasonably practicable due to significant time and costs associated with inactive electronic data or data in other storage devices, the Customer hereto agrees to continue to comply with the protections set forth herein until returned or destroyed.

(c) Subject to applicable laws, upon termination of this Addendum, all payment obligations shall become due immediately.

APPLICATION PROGRAMMING INTERFACE (API) CONNECTIONS ADDENDUM

This Addendum shall become effective on the date the Customer begins utilizing the benefits outlined herein and shall be incorporated into, and form an integral part of, the Agreement. It sets forth the terms and conditions under which the Customer is authorized to facilitate User access to the Services through API integration. For the purposes of this Addendum, "Documentation" refers to any related documentation, guidelines, or materials provided by EC-Council in connection with the use of the API.

1. Purpose

This Addendum sets forth the terms and conditions under which the Customer is authorized to enable User access to the Platform via API integration.

2. Terms and Conditions:

(a) Subject to the terms and conditions of this API Addendum, EC-Council grants Customer a non-exclusive, non-transferable, revocable license to use the API and Documentation solely for the purpose of integrating and interacting with Services.

(b) Customer shall not, without the express written consent of EC-Council, (a) sublicense, sell, lease, or otherwise transfer the API or Documentation to any third party; (b) reverse engineer, decompile, disassemble, or attempt to derive the source code of th e API; (c) modify, adapt, or create derivative works from the API; (d) use the API in any manner that violates applicable laws or regulations.

(c) EC-Council retains all rights, title, and interest in and to the API and Documentation, including all intellectual property rights.

(d) The Customer may provide feedback regarding the API. EC-Council may use such feedback without any obligation to Customer.

(e) EC-Council may provide support and maintenance for the API at its discretion. Customer agrees that EC-Council has no obligation to provide any updates, upgrades, or support unless explicitly stated

(f) The Customer will comply with all applicable law, regulation, and third-party rights (including without limitation laws regarding the import or export of data or software, privacy, and local laws). The Customer will not use the API to encourage or promote illegal activity or violation of third-party rights. The Customer will not violate any other terms of service with EC-Council.

(g) EC-Council sets and enforces limits on your use of the APIs (e.g. limiting the number of API requests that you may make or the number of users you may serve), in our sole discretion. Customer agrees to, and will not attempt to circumvent, such limitati ons documented with each API. If Customer would like to use any API beyond these limits, Customer must obtain EC-Council's express consent (and EC-Council may decline such request or condition acceptance on Customer's agreement to additional terms and/or charges for that use). To seek such approval, contact your account manager.

When using the APIs, the Customer may not (or allow those acting on your behalf to):

a) Sublicense an API for use by a third party. Consequently, Customer will not create an API that functions substantially the same as the APIs and offer it for use by third parties.

b) Perform an action with the intent of introducing to EC-Council products and services any viruses, worms, defects, Trojan horses, malware, or any items of a destructive nature.

c) Interfere with or disrupt the APIs or the servers or networks providing the APIs.

d) Reverse engineer or attempt to extract the source code from any API or any related software, except to the extent that this restriction is expressly prohibited by applicable law.

3. **Term and Termination**

(a) The term of this Addendum shall be coterminous with the term of the Agreement, however termination of this Addendum shall not affect the validity of the Agreement.

(b) Termination :When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, EC-Council shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

(c) Upon termination of the Agreement or the Addendum, subject to applicable laws, the Customer shall return and/or destroy all the proprietary information, including but not limited to the back-up copies of EC-Council's proprietary materials, if any, immediately upon request by EC-Council. Any destruction that is carried out shall be certified in writing to EC-Council by the authorized officer or director of the Customer supervising such destruction. To the extent destruction is not reasonably practicable due to significant time and costs associated with inactive electronic data or data in other storage devices, the Customer hereto agrees to continue to comply with the protections set forth herein until it is returned or destroyed.

(d) Upon termination of this Addendum, all payment obligations shall become due immediately.

Annexure I Privacy Policy

EC-Council recognizes the importance of maintaining your privacy and is committed to protecting it and developing technology that gives you the most powerful and safe online experience. This Statement of Privacy applies to current and former visitors to all our EC-Council websites and governs data collection and usage. By using the EC-Council website, you consent to the data practices described in this statement. At EC-Council, the privacy and security of our customers, respondents, and visitors are of paramount importance. We value your privacy and appreciate your trust in us.

1. What type of personal information do we gather?

EC-Council collects certain personal information about you during your relationship with us. EC-Council, through various web-platforms that help our members to register, reset passwords, get training, partner with us, etc. collects personally identifiable information/personal information that may include:

a. Contact information. We might collect your name, e-mail, home or work addresses, telephone numbers, organization names, etc.

b. Identification Documents. For certain Services, we may require you to provide a copy of government-issued identification, such as a passport, national identity card, driver's license, or other similar documents, to verify your identity. However, such identification documents shall be provided to us subject to clause 9 of this Privacy Policy.

c. Payment and billing information. We might collect your billing name, billing address, the legal age as permitted by your country of origin/residency and as per the payment method used by you. We NEVER collect your credit card number or credit card expiry date or other details pertaining to your credit card on our website. We will not be storing any Bank related information on our records and none of our employees will hold or be exposed to this information.

d. Information you post. We collect information you post in a public space on our website or on a third-party social media page of EC-Council.

e. Demographic information. We may collect anonymous demographic information, which is not unique to you, such as your ZIP code, age, gender, preferences, interests, favorites, or any other information provided by you during the use of our website. We might collect this as a part of a survey also.

f. Other information. If you use our website, we may collect information about your IP address and the browser you're using. This may also include interactions through our website, training centers, meetings with our representatives and representatives from our authorized partners and other third parties or the duration of time spent on our website.
EC-Council does not collect, use, and/ or disclose sensitive personal information, such as race, religion, health information or political affiliations without your explicit consent.

2. Minor's Online Privacy

Protecting the privacy of young children is especially important. We do not automatically process or profile any information belonging to minors unless a parent or guardian gives us express permission for it. Any person under the age of majority can only use our services under the supervision of their parents or legal guardians as per our Terms of Use, located here. If you are under the age of majority as per the jurisdiction of your residence or citizenship and have provided us with your personal information without the consent of your parents or legal guardian or if you are a parent or legal guardian of a child who has subscribed to our services without your authorization or by mistake, please contact us at dpo@eccouncil.org. We will take appropriate steps to identify and remove the information or take any other actions as required by applicable laws.

3. Where do we collect Personal Information about you?

We collect information in different ways.

a. We collect information directly from you. We collect information directly from you when you register or partner with us. You may choose to apply for specific information or services on topics such as products, training, white papers, brochures, etc. which may require you to fill out forms and share your personal information. This information is irrespective of your membership. EC-Council asks you to allow representatives of EC-Council to contact you for the purpose asked.

EC-Council may collect different data from or about you depending on how you use EC-Council Services. When you create an account and use our Services, including through a third-party platform, we collect any data you provide directly, including, but not limited to data about your accounts on other Services.

b. We collect information from you passively. We receive and store certain types of information whenever you interact with us. We use browser cookies and web beacons, for collecting information about your usage of our website or any of our subdomains, advertisements, and other content served by or on behalf of EC-Council on other websites. We may use this information for internal analysis and to provide you with location-based services, such as advertising, search results, and other personalized content.

To help us make our emails communication more useful and interesting, we often receive confirmation when you open email from EC-Council, if your computer supports such capabilities. If you do not want to receive e-mail or other mail from us, please edit your customer communication preferences.

c. We get information about you from third parties. If you access or use our Services through a third-party platform or service, or if you use an integrated social media feature on our websites, or click on any third-party links, the collection, use, and sharing of your data will also be subject to the privacy policies and other agreements of that third party.

We may obtain certain information through your social media or other online accounts if they are connected to your EC-Council account. If you login to EC-Council via social media platforms e.g., Facebook or join EC-Council sponsored WhatsApp Group, or any other third-party platform or service, we ask for your permission to access certain information about that other account. The third-party social media site may give us certain information about you. For example, depending on the platform or service we may collect your name, profile picture, membership account ID, login email address, location, physical location of your access devices, gender, birthday, and list of friends or contacts. Those platforms and services make information available to us through

their APIs. The information we receive depends on what information you (via your privacy settings) or the platform or service decide to give us.

d. We get information about you from other sources. We might receive information about you from other sources and add it to our account information.

4. How and why do we use your personal information?

a. We use information to provide you our Services: Certain EC-Council services require you to provide your personal information, so as to enable us to provide you the whole range of that Service.

b. We use information to contact/respond to your requests or questions: We might use the information you provide to contact you to deliver the services you have requested or administering and processing your certification exams.

c. We use information to improve our products and services. We might use your information to analyze and customize our products, websites, newsletters, and other communications to support and improve your online experience with us.

d. We use information to look at site trends and customer interests. We may use your information to make our website and products better. We may combine information we get from you with information about you we get from third parties. EC-Council may also contact you via surveys to conduct research about your opinion of current services or of potential new services that may be offered.

e. We use information for security purposes. We may use information to protect our company, our customers, or our websites.

f. We use information for marketing purposes. We may use your information for sending communications to you, including for marketing and promotional or customer satisfaction purposes to inform you of other products or services available from EC-Council and its affiliates.

g. We use information to send you transactional communications. We might send you emails or SMS about your account or a product or service purchase.

h. We use information as otherwise permitted by law. To comply with our obligations under the law, including record-keeping, reporting, accounting, tax, etc.

5. Who do we share your personal information with?

EC-Council does not sell, rent, or lease your personal information to third parties without your explicit consent.

EC-Council shares personal information in the following ways:

a. We will share your personal information with our Group companies for internal reasons, primarily for business and operational purposes.

b. We will share information with our authorised Vendors. We share information with vendors who help us to manage our online registration process or payment processors or transactional message processors. Some vendors may be located outside of the country where you reside in. .

c. We will share information with our business partners/ third parties who perform services on our behalf. EC-Council may, from time to time, contact you on behalf of external business partners about a particular offering that may be of interest to you. In those cases, your unique, personal information (for instance your e-mail, name, address, telephone number) is not transferred to the third party. However, EC-Council may share data with trusted partners to help us perform statistical analysis, send you email or postal mail, provide customer support, or arrange for deliveries. All such partners are prohibited from using your personal information except to provide these services to EC-Council, and they are required to maintain the confidentiality of your information.

d. We may share information if we think we must comply with the law or to protect ourselves.
EC-Council websites will disclose your personal information, without consent, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on EC-Council or the site; (b) protect and defend the rights or property of EC-Council; and, (c) act under exigent circumstances to protect the personal safety of users of EC-Council or the public.

e. We may share your information for reasons not described in this policy.
We will tell you before we do this. EC-Council does not transfer any sensitive personal information. By using or continuing to use the site you agree to our use of your information (including sensitive personal information) in accordance with this Priv acy Notice, as may be amended from time to time by EC-Council at its discretion. You also agree and consent to us collecting, storing, processing, transferring, and sharing information (including sensitive personal information) related to you with third parties or service providers for the purposes as set out in this Privacy Notice.

We may be required to share the aforementioned information with government authorities and agencies for the purposes of verification of identity or for the prevention, detection, investigation, prosecution, or punishment of cyber incidents or any other legal offenses. You agree and consent to EC-Council, at its sole discretion, disclosing the required information with government authorities and agencies in such cases.

f. Corporate Transactions. Your information may be disclosed to third parties in connection with a corporate transaction, such as a merger, sale of assets or shares, reorganization, financing, change of control, or acquisition of all or a portion of our business.

EC-Council encourages you to review the privacy statements of websites you choose to link to from EC-Council's website so that you can understand how those websites collect, use, and share your information. EC-Council is not responsible for the privacy statements or content on websites outside of the EC-Council's family of websites.

g. Messaging: We do not sell your mobile number to any unaffiliated third parties or affiliates for marketing or promotional purposes. Your mobile number and any consent you provide for text messaging will be used exclusively for the purposes for which you have given consent, such as service notifications or account-related communications, and will never be sold. Your information may be shared with third-party service providers solely to facilitate message delivery on our behalf. These providers are bound by contractual obligations to protect your data and may not use it for any other purpose. We require your explicit consent before sending any

marketing or promotional messages, and you may withdraw your consent or opt out of messaging at any time. We retain records of your consent in accordance with applicable legal requirements and will delete your data upon request or when it is no longer necessary for the stated purpose

6. How EC-Council stores the personal information it collects?

EC-Council stores your personally identifiable information such as name, contact number, email address, etc. on a secure server which is encrypted and is accessible only to EC-Council's applications. EC Council may be required to share personal information with its affiliates, advisors, and auditors in other countries where it may be processed. If we or our affiliates or our service providers transfer personal information outside of the country of origin, we always require that appropriate safeguards are in place to protect the information when it is processed.

7. How EC-Council secures your personal information?

We take appropriate technical and organizational measures to secure your information and to protect it against unauthorized or unlawful use and accidental loss or destruction.

EC- Council uses secure servers to store your information and only shares and provides access to your information to the minimum extent necessary, subjected to confidentiality restrictions where appropriate, and on an anonymized basis wherever possible. We also verify the identity of any individual who requests access to information prior to granting them access to requested information.

EC-Council also uses Secure Sockets Layer (SSL) software or other similar encryption technologies to encrypt any payment transactions you make on or via our website. EC-Council also adopts comprehensive standards such as ISO/IEC 27001:2013 for selected Services.

8. How long do we keep your personal information?

We will retain your personal information as needed to fulfill the purposes for which it was collected. We will retain and use your personal information as necessary to comply with our business requirements, legal obligations, resolve disputes, protect our assets, and enforce our agreements.

We determine standard retention periods for different categories of personal information in our possession. Where it isn't possible to determine standard retention periods, we do so, based on the following criteria:

- our relationship with you
- the legal obligations we are subject to.
- the legal basis we have for processing your data (consent, performance of contract, etc.).
- the purposes and uses of your data (this include present and future uses).
- the level of risk with retaining or using your data.
- your rights under the GDPR and other relevant laws.
- any other relevant circumstances.

As EC-Council is a certification body, we store users' information relevant to the upgrading or renewing their certification which includes submission of ECE Credits in line with the certification ECE policy.

9. Masking Personal Information in Government Issued Identification

You agree to mask all personal or sensitive information, except your name and photo, in any government-issued identification document ("Pseudonymized Document") submitted to us for availing certain services. By submitting such Pseudonymized Documents, you accept sole responsibility for masking any personal or sensitive information not required by us for providing such services and further agree to indemnify, defend, and hold harmless EC-Council, its affiliates, and their officers, directors, and shareholders from any claims or liabilities arising from unmasked Pseudonymized Document. We reserve the right to reject and discard documents not properly masked, and you assume all liability for any resulting loss.

10. What legal basis do we have for using your personal information?

We process your personal information on the following legal bases:

a. **Consent**

We use consent to process your data for certain purposes such as when you consent to receive marketing communication, when you express interest in associating with us or to know more about us, etc. You can withdraw your consent at any time by writing to us at the e-mail addresses provided below

b. **Performance of Contract**

To perform the contract between us, we process various types of contact/financial/service-related information. This also enables us to provide you with our products and/or services in line with the contractual obligations of our contract along with our Terms of Use via the EC-Council websites.

c. **Legitimate Interests**

Provided that such processing shall not outweigh your rights and freedoms, we may use your personal information for our legitimate interests which include legal obligations, direct marketing, market research, web analytics/profiling, compliance abidance, customer service, record-keeping, review, research, and analysis, to fulfil our legal obligations under applicable laws, security, storage, etc. You've the right to object, on grounds relating to your situation, at any time to processing of personal data concerning you which is based on legitimate interests. More information on this right and on how to exercise it, is set out below under "Right to Object" clause of this Privacy Statement.

11. EC-Council Cookie Policy

A cookie is a small text file which is placed onto your computer or electronic device when you access our website. Cookies are used to track users' actions and activities, and to store specific information about your preferences, location, session details, etc. about them. We use these cookies and/or similar technologies on this website for the only purpose of ensuring that you get the best experience. You can go to the preference or content setting of your web browser to delete the cookies pertaining to any website at any time.

12. Website Visitors

EC-Council collects, records, and may analyze information from visitors to our websites. We may record your IP address and use cookies. Furthermore, EC-Council collects and processes any personal data that you volunteer to share with us via our website forms, such as when you register for events or sign up for information and newsletters. This data is used to deliver customized content and advertising within EC-Council to customers whose behavior indicates that they are interested in a subject area. If you provide EC-Council with your social media details, EC-Council will retrieve publicly available information about you from social media.

13. Consent for Cookies

In most cases we will need your consent to use cookies on this website. The exceptions are where the cookie is essential for us to provide you with service you have requested, or essential to the inherent functionality of the website. Where we wish to use cookies that require your consent you will be asked to consent through a checkbox pop-upon the website homepage that you will have to answer to gain full access to the website.

14. Turn Off or Opt-Out of Cookies

Rejecting cookies may restrict your browsing experience on EC-Council websites related to important features such as login, location-specific data, and other demographic dependent information. However, you will be provided with an opportunity to opt-out of the use of cookies while consenting by controlling the collection of cookies in the cookie settings provided on the cookie banner.

15. Third-Party Cookies

EC-Council does not share cookie information with any other website, nor do we sell this data to any third party. We work with third party suppliers who may also set cookies on our website.. By consenting to the use of cookies on our site you will be consenting to the use of these cookies.

16. What rights do you have in relation to the personal information we hold on you, in compliance to GDPR?

The **General Data Protection Regulation** (GDPR) provides you the benefit of several rights when it comes to your personal information.

a. The Right to be Informed.

EC-Council is publishing this Privacy Policy Statement to keep our users informed as to what we do with their personal information and what are their rights, in a clear, transparent, and easily understandable manner.

b. The Right of Access

You have the right to obtain access to your information that we are processing and certain other information, in accordance with data protection law. Contact EC-Council if you wish to access the personal information EC-Council holds about users/data subjects.

c. The Right to Rectification

You are entitled to have your information corrected if it's inaccurate or incomplete.

d. The Right to Erasure

This is also known as 'the right to be forgotten'. If users want EC-Council to erase all personal data and we do not have a legal reason to continue to process and hold it, please contact us at legal@eccouncil.og or dpo@eccouncil.org. This is not a general right to erasure; there are exceptions. If however, you do not fall within the ambit of exceptions, we will delete your data within a period of thirty (30) days.

e. The Right to Restrict Processing

You have rights to 'block' or suppress further use of your information. Users have the right to ask EC-Council to restrict how we process user data. This means we are permitted to store the data but not further process it. We keep just enough data to make sure we respect our users request in the future.

f. The Right to Data Portability

EC-Council allows to obtain and reuse personal data for purposes across services in a safe and secure way without this effecting the usability of user data.

g. The Right to Withdraw Consent

If users have given us their consent to process their data but change their mind later, they have the right to withdraw their consent at any time, and EC-Council stop processing their data. Users can write to dpo@eccouncil.org or www.eccouncil.org/unsubscribe.

h. The Right to Object to Processing and Automated Processing

You have right to object to the processing and automated profiling of your personal information as per applicable data protection laws. If you wish to object to the processing or automated processing of your personal information, please contact us at dpo@eccouncil.org.
.

Further information and advice about your rights can be obtained from the data protection regulator in your country.

17. Data Protection Officer

In accordance with the applicable data privacy laws and rules of the jurisdictions in which EC-Council operates, including General Data Protection Regulation (EU) 2016/679 (GDPR), the contact details of the appointed Data Protection Officer are provided below:

Email: dpo@eccouncil.org

If you have any questions about this Policy or other privacy concerns, you can also email us at the abovementioned details.

18. What is our Opt-Out Policy?

a. Users may unsubscribe from our marketing communications by clicking on the "unsubscribe" link located on the bottom of our e-mails, and by sending us email at dpo@eccouncil.org or www.eccouncil.org/unsubscribe. Customers cannot opt out of receiving automated emails related to their account with us or our Services, like aspen emails, certification renewal emails. Further, certain U.S. state privacy laws, including the California Consumer Privacy Act (CCPA/CPRA), Colorado Privacy Act (CPA), Virginia Consumer Data Protection Act (VCDPA), Connecticut Data Privacy Act (CTDPA), and other applicable state laws, grant residents the right to opt out of the sale or sharing of their personal information and targeted advertising. Residents of the following states may exercise their opt-out rights under applicable law by writing to dpo@eccouncil.org: California (CA), Colorado (CO), Connecticut (CT), Virginia (VA), Utah (UT), Texas (TX), Oregon (OR), Montana (MT), Nebraska (NE), Iowa (IA), Indiana (IN), Kentucky (KY), Tennessee (TN), Maryland (MD), District of Columbia (DC), Delaware (DE), New Jersey (NJ), Rhode Island (RI), and New Hampshire (NH).

b. If you would like to opt-out of sharing of your personally identifiable information/personal information submitted on our website with third parties or otherwise, contact us at dpo@eccouncil.org and indicate your unwillingness to share such information with third parties or otherwise. However, this shall restrict your access to certain services as our services are linked internally to various platforms.

c. However, under the following circumstances, we may still be required to share your personal information:
    i. If we are responding to court orders or legal process, or if we need to establish or exercise our legal rights or defend against legal claims.
    ii. If we believe it is necessary to share information to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of our Terms of Use or as otherwise required by law.
    iii. If we believe it is necessary to restrict or inhibit any user from using any of our websites, including, without limitation, by means of "hacking" or defacing any portion thereof.

19. Third Party sites

If you click on one of the links to third party websites, you may be taken to websites we do not control. This policy does not apply to the privacy practices of those websites. Read the privacy policy of other websites carefully. We are not responsible for these third-party sites.

20. Breach of Privacy Policy

EC-Council reserves the right to terminate or suspend any account or delete certain contents from any profile or public domain within the ambit of this website if the said account or content is found to be in violation of our Privacy Policy Statement. We request you to respect privacy and secrecy concerns of others. The jurisdiction of any breach or dispute shall be determined in accordance with the terms of use of the website.

21. No Reservations

EC-Council does not accept any reservation or any type of limited acceptance of our Privacy Policy Statement. You expressly agree to each, and every term and condition as stipulated in this Policy Statement without any exception whatsoever.

22. No Conflict

This Privacy Policy Statement constitutes a part of Terms of Use and Terms of Service appearing on EC-Council's family of websites. We have taken utmost care to avoid any inconsistency or conflict of this policy with any other terms, agreements, or guidelines available on our family of websites. In case there exists a conflict, we request you to kindly contact us at dpo@eccouncil.org for the final provision and interpretation.

23. How can you contact us?

EC-Council welcomes your comments regarding this Privacy Policy Statement. If you believe that EC-Council has not adhered to this Privacy Policy Statement, please contact EC-Council at dpo@eccouncil.org. We will use commercially reasonable efforts to promptly determine and remedy the problem. We usually act on requests and provide information free of charge but may charge a reasonable fee to cover our administrative costs of providing the information for, baseless or excessive/repeated requests, or further copies of the same information. Alternatively, the law may allow us to refuse to act on the request.

Updates to this EC-Council Privacy Policy Statement

This Privacy Policy was last updated on the date provided below. EC-Council will occasionally update Privacy Policy Statement to reflect company and customer feedback. We will notify you of any material changes to this policy as required by law. We will also post an updated copy on our website. EC-Council encourages you to periodically review this Policy Statement to be informed of how EC-Council is protecting your information.

Annexure II

Data Processing Agreement

This Data Processing Agreement ("DPA") and its Annexes reflects the parties' agreement with respect to the processing and Security of Personal Data on the Company's behalf in connection with EC-Council Services provided to the Company and the related Services agreement between Company and EC-Council, along with any annexures, appendices, order forms etc, or for any other services provided by EC-Council pursuant to a formal agreement between EC-Council and Company, (also referred collectively referred to in this DPA as the "Principal Agreement"). All references to the 'Company' herein shall, where the context permits, be deemed to include the 'Customer

This DPA is supplemental to and forms an integral part of the Principal Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

This DPA is subject to Data Protection Laws of the appropriate jurisdiction, including the State of California, the European Union, the European Economic Area and/or its member states, Switzerland and/or the United Kingdom. The parties agree to comply with the terms and conditions in this DPA in connection with such Personal Data.

The term of this DPA will follow the term of the Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

The parties shall be collectively referred as "Parties", the Company shall be generally referred as "Company" and EC-Council shall be generally referred as "EC-Council.

1. Definitions

1.1. "Applicable Law" means all applicable laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the Personal Information Protection and Electronic Documents Act, 2000 ("PIPEDA"); the UK Data Protection Act 2018 the GDPR as it forms part of United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018, and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419) (the "UK GDPR"); the Swiss Federal Act on Data Protection; the European Union ("EU") General Data Protection Regulation 2016/679 ("GDPR") as applied, supplemented, modified and/or replaced from time to time by the laws of the United Kingdom, Switzerland and/or the relevant member state of the European Union and European Economic Area (as the case may be); EU Directive 2002/58/EC on Privacy and Electronic Communications ("e-Privacy Directive"); the California Consumer Privacy Act of 2018 and any regulations promulgated thereunder, as amended from time to time ("the CCPA"); and any other directly applicable laws or regulation relating to privacy and data rights of natural persons having effect or enacted in the United States, Switzerland, United Kingdom, the European Economic Area, and/or the European Union or a relevant state or member state thereof (as the case may be), or anywhere else in the world, in each of the foregoing instances, as applicable to the Processing of Personal Data by Processor.

1.2. "Company" shall mean to include any partnership, corporation, consortium, association, firm or any body corporate whether incorporated or not.

1.3. "Company Personal Data" means any Personal Data processed by EC-Council on behalf of Company pursuant to or in connection with the Principal Agreement;

1.4. "Contracted Processor" means a Sub-processor;

1.5. "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the applicable data protection or privacy laws of any other country;

1.6. "Data Transfer" means:
(a) a transfer of Company's Personal Data from the Company to EC-Council ; or
(b) an onward transfer of Company's Personal Data from a EC-Council to a Subcontracted Processor, or between two establishments of EC-Council,
in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.7. "EEA" means the European Economic Area;

1.8. "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.

1.9. "Europe" means the European Union, the European Economic Area and/or their member states, Switzerland, and the United Kingdom.

1.10. "European Data" means Personal Data that is subject to the protection of European Data Protection Laws.

1.11. "GDPR" means EU General Data Protection Regulation 2016/679;

1.12. “Instruction” means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

1.13. "Personal Data" means any information relating to an identified or identifiable individual where (i) such information is contained within Company’s Data; and (ii) is protected similarly as personal data, personal information or personally identifiable information under Applicable Laws

1.14. "Personal Data Breach" a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

1.15. "Platform" shall have the meaning set forth in the specific Terms of Service for any EC-Council Service and where not defined therein shall mean EC-Council’s platform through which EC-Council provides the Service availed by the Company.

1.16. "Service(s) " means the services provided by EC-Council to the Company under the Principal Agreement.

1.17. "Sub-Processor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Controller in connection with the Principal Agreement.

1.18. The terms, "Commission", "Data Controller", "Data Subject", “Data Processor” "Member State", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Data Processing

2.1. **Scope and Roles.** This DPA applies only when Company’s Personal Data is processed by EC-Council, under the Principal Agreement. Company and EC-Council agree that Company is the Data Controller of Company Personal Data and EC-Council is the Data Processor of such data, except when Company acts as a Data Processor of Personal Data, in which case EC-Council is a Sub-processor. Where the Parties are acting as independent Controllers, then each Party shall act as an independent Data Controller and not as Joint Controller.

2.2. **Legitimacy of Processing**. The Company is responsible for ensuring a valid legal basis for processing the Company Personal Data.

2.3. **Compliance with Law**. Each party agrees it will comply with its obligations under the Applicable Laws relating to any Company Personal Data it processes under or in relation to this Agreement. Without prejudice to the foregoing, EC-Council will not process Company’s Personal Data in a manner that will, or is likely to, result in the Data Controller breaching its obligations under the Data Protection Law. EC-Council will promptly inform the Company if any of the Company’s Instruction(s) infringes Applicable Law.

3. Company’s Responsibilities:

3.1. **Company Personal Data**. In particular but without prejudice to the generality of the foregoing, Company acknowledges and agrees that Company shall be solely responsible for: (i) the accuracy, quality, and legality of Company Personal Data and the means by such data is acquired; (ii) complying with all necessary transparency and lawfulness requirements under Applicable Laws for the collection and use of the Company Personal Data, including obtaining any necessary consents and authorizations; (iii) ensuring Company has the right to transfer, or provide access to, the Company Personal Data to EC-Council for Processing in accordance with the terms of the Principal Agreement (including this DPA); (iv) ensuring that Company’s Instructions to EC-Council regarding the Processing of Company Personal Data comply with applicable laws, including Data Protection Laws; (v) making an independent determination as to whether the technical and organizational measures for Services meet Company’s requirements, including any of its security obligations under applicable data protection requirements. Company acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of Company Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by EC-Council provide a level of security appropriate to the risk with respect to such data. The Company is responsible for implementing and maintaining privacy protections and security measures for components that Company provides or controls. The Company shall inform EC-Council without undue delay if Company is not able to comply with their responsibilities under this DPA or Applicable Laws.

3.2. **Company’s Instructions**. The Parties agree that the Principal Agreement and this DPA, together with Company’s use of the

Service in accordance with the Principal Agreement, constitute the Company's complete Instructions to EC-Council in relation to the Processing of Company Personal Data. The Company may provide additional Instructions as long as additional Instructions, during the term of the Principal Agreement, are consistent with the Principal Agreement, this DPA, and lawful use of the Service under applicable laws. In any instance where the GDPR applies and Company is a Processor, Company warrants to EC-Council that Company's instructions, including appointment of EC-Council as a processor or Sub-processor, have been authorized by the relevant Controller.

3.3. **Security**. The Company is responsible for independently determining whether the data security provided for in the Service adequately meets Company's obligations under Applicable Laws. Company is also responsible for the Company's secure use of the Service, including protecting the security of Company Personal Data in transit to and from the Service (including to securely backup or encrypt any such Company Personal Data).

4. EC-Council's Obligations

4.1. **Compliance with Instructions**. EC-Council will only Process Company Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of the Company's lawful Instructions, except where and to the extent otherwise required by Applicable Law.

4.2. **Conflict of Laws**. If EC-Council becomes aware of any situation where it cannot Process Company Personal Data in accordance with the Company's Instructions due to a legal requirement under any applicable law, EC-Council will (i) act promptly as per notification provided by Company of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Company issues new Instructions with which EC-Council is able to comply. If this provision is invoked, EC-Council shall not be liable to the Company under the Principal Agreement for any failure to perform the applicable Services until such time as the Company issues new lawful Instructions with regard to the Processing.

4.3. **Limits on Updates.** When Company renews an existing membership to a Service or subscribes to a new Service, the then-current DPA Terms will apply and will not change during Company's membership for that Service.

4.4. **New Features, Supplements, or Related Software.** Notwithstanding the foregoing limits on updates, when EC-Council introduces features, offerings, supplements, or related Services that are new (i.e., that were not previously included with the Service offering), EC-Council may provide terms or make updates to this DPA that apply to Company's use of those new features, offerings, supplements, or related Service. If those terms include any material adverse changes to the DPA Terms, EC-Council may provide the Company a choice to use the new features, offerings, supplements, or related Service, without loss of existing functionality of a generally available Service. If the Company does not use the new features, offerings, supplements, or related Service, the corresponding new terms will not apply.

4.5. **Government Regulation and Requirements.** Notwithstanding the foregoing limits on updates, EC-Council may modify or terminate a Service in any country or jurisdiction where there is any current or future government requirement or obligation that (i) subjects EC-Council to any regulation or requirement not generally applicable to businesses operating there, (ii) presents a hardship for EC-Council to continue offering the Service without modification, and/or iii) causes EC-Council to believe the DPA or the Service may conflict with any such requirement or obligation. EC-Council may amend the terms of this DPA where required to comply with Data Protection Requirements and to reflect any changes in the applicable Data Protection Requirements, so long as any such revisions continue to ensure the protection of Personal Data processed by EC-Council in the course of providing the Service to the Company.

5. Details of Data Processing

5.1. **Subject matter**. The subject matter of the data processing under this DPA is Company's Personal Data. The processing activities that EC-Council shall carry out are strictly limited to those necessary to fulfil the scope of the Principal Agreement signed by the parties or for the provisioning of Services provided by EC-Council.

5.2. **Duration.** As between the parties, the duration of the data processing under this DPA shall be for the duration of the Services.

5.3. **Purpose**. The purpose of the data processing under this DPA is the provision of the Services.

5.4. **Nature of the processing**. EC-Council will process Company Personal data as per EC-Council's Privacy Policy and Applicable Laws.

5.5. **Categories of data subjects**. The data subjects could include Company's customers, employees, suppliers, partners, end users or any individual whose Personal Data is provided to EC-Council by Company for processing.

6. Processor Personnel

EC-Council shall take commercially reasonable steps to ensure the reliability of any employee, agent or contractor of any Sub-Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Company Personal Data, as necessary for the purposes of the Principal Agreement, or to comply with Applicable Laws in the context of that individual's duties to the Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

7. Security

7.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing

as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, EC-Council shall, in relation to the Company Personal Data, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR, to the extent required by Applicable Laws. EC-Council periodically monitors the internal processes and the technical and organizational measures to ensure that processing activities pertaining to it are carried out in accordance with the requirements of Applicable Law and the protection of Data Subjects' rights.

7.2. In assessing the appropriate level of security, EC-Council will take into account the risks that are presented by processing, from a Personal Data Breach.

8. Sub-processing

The Company agrees that EC-Council may engage Sub-Processors to Process Company Personal Data on Company's behalf. Company may write to EC-Council at dpo@eccouncil.org to know about EC-Council's Sub Processor(s). Where EC-Council engages Sub-Processors, adequate data protection terms are imposed on the Sub-Processors which provides the same level of protection for Personal Data as those in this DPA , to the extent applicable to the nature of the services provided by such Sub-Processors. To the extent required by Applicable Laws, EC-Council will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that causes EC-Council to breach any of its obligations under this DPA.

9. Data Subject Rights

9.1. Taking into account the nature of the Processing, EC-Council shall assist the Company by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of EC-Council's obligations, as reasonably understood by EC-Council, to respond to requests to exercise Data Subject rights under the Applicable Laws.

9.2. EC-Council shall:

9.2.1. promptly notify the Company of receipt of a request from a Data Subject under any Applicable Law in respect of Company Personal Data; and

9.2.2. ensure that EC-Council does not respond to that request except on the instructions of Company or as required by Applicable Laws, in which case EC-Council shall to the extent permitted by Applicable Laws and shall inform Company of the legal requirement before responding to the request.

10. Personal Data Breach

10.1. EC-Council shall notify Company without undue delay of a Personal Data Breach affecting Company Personal Data and shall provide sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of such Personal Data Breach under the Applicable Laws.

10.2. EC-Council shall co-operate with the Company and shall take reasonable commercial steps to assist in the investigation, mitigation, and remediation of such Personal Data Breach.

11. Data Protection Impact Assessment and Prior Consultation

EC-Council shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which Company reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Applicable Law, in each case solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to the Contracted Processors.

12. Deletion or return of Company's Personal Data

12.1. Subject to this section, EC-Council shall promptly and in any event within thirty (30) business days of the receipt of request from the Company delete and procure the deletion of all copies of Company Personal Data. However, EC-Council may not be able to provide certain services upon deletion of such data, including records of certification.

12.2. EC-Council shall upon request provide written confirmation to Company that it has complied with this section within thirty (30) business days from the date of deletion.

13. Audit rights

13.1. Subject to Section 13.2, EC-Council may make available to the Company, on Company's expense and request, information necessary to demonstrate compliance with this Agreement, solely in relation to the Processing of the Company Personal Data by EC-Council.

13.2. Information and audit rights of the Company only arise under Section 13.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Applicable Law. The Company shall

request such information only upon providing prior written notice of thirty (30) days. Provided further still that EC-Council shall be obliged to provide only such information as shall be mutually agreed between the parties.

14. Data Transfer

Company acknowledges and agrees that EC-Council may access and Process Company Personal Data on a global basis as necessary to provide the Service in accordance with the Agreement, and in particular that Company Personal Data may be transferred to and Processed by EC-Council in jurisdictions where EC-Council affiliates and Sub-Processors have operations. Wherever Company's Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Applicable Laws. EC-Council will also comply with its Privacy Policy and the annexed applicable module of Standard Contractual Clauses provided by European Commission in "Annexure B" for any such transfer of data..

15. General Terms

15.1. **Confidentiality.** Each Party must keep this agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:
(a) disclosure is required by law;
(b) the relevant information is already in the public domain.

15.2. **Notices.** All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address. For EC-Council, all notices must be sent on dpo@eccouncil.org.

15.3. **Amendment.** No amendment, change or suspension of this Data Processing Agreement shall be valid unless agreed upon in writing between Company and the Processor and unless this Data Processing Agreement is expressly referred to.

15.4. **Independent Parties**. Company and Service Provider are independent parties and the processing activities with respect to Processor under this Data Processing Agreement are solely the responsibility of Processor for their services.

15.5. **Governing law.** Ireland

Annexure A

Documentation of Data Protection Measures

The documentation of data protection measures and data security can be obtained from EC-Council by writing at dpo@eccouncil.org.

Annexure B

Standard Contractual Clauses

For the purpose of this DPA and compliance with the GDPR, the Parties agree to enter into the applicable module of Standard Contractual Clauses issued by the EU Commission on June 4, 2021.

For purposes of this DPA and compliance with the UK GDPR, the Parties agree to enter into the IDTA issued by the UK Information Commissioner's Office on March 21, 2022, as set out in Annexure C. The IDTA will only apply to Personal Data that is transferred outside the UK, either directly or via onward transfer, to any country not recognized by the UK as providing an adequate level of protection for personal data.

Module I (Controller to Controller)

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.

(a) 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").

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

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

Clause 2

Effect and invariability of the Clauses

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

in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

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

Clause 3

Third-party beneficiaries

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7 - Optional

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

8.1 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. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

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

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

8.5 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 personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

---

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) 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 personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 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 or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

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

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

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

---

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

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

Sub-Processor

Controller to Controller- Not Applicable

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[4] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

---

[4] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

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.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body[5] at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

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

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

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

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

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

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

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

Clause 12

Liability

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

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

Clause 13

Supervision

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

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

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

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and

[5] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[6];

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(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 [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland. (*specify Member State*).]

Clause 18

Choice of forum and jurisdiction

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

(g) The Parties agree that those shall be the courts of Ireland.

(h) 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.

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

Module II (Controller to Processor)

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)[7] for the transfer of personal data to a third country.

(b) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-party beneficiaries

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

(e) 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.

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[8] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (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.[9] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

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

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

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

Clause 10

Data subject rights

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

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

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

(g) 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.

(h) 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.

(i) 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.

(j) 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.

(k) 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.

(l) 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.

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

Clause 13

Supervision

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

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[10];

(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). [For Module Three: The data exporter shall forward the notification to the controller.]

(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 [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

15.1 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.). [For Module Three: The data exporter shall forward the information to the controller.]

(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.

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 dataThe data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

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

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

(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.

Module III (Processor to Processor)

SECTION I

Clause 1

Purpose and scope

(e) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[11] for the transfer of personal data to a third country.

(f) The Parties:

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

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

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

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

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

Clause 2

Effect and invariability of the Clauses

(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

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

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

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

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

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

(v) Clause 13;

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

(vii) Clause 16(e);

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

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

Clause 4

Interpretation

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

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

(m) 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

(n) 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.

(o) 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.

(p) 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 THREE: Transfer processor to processor

8.1 Instructions

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

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

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

(t) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the

contract or other legal act under Union or Member State law between the controller and the data exporter[12].

8.2 Purpose limitation

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

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the

Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the reda cted information.

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

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

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

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

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

8.7 Sensitive data

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

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[13] (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:

[13] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including

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

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

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

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

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

8.9 Documentation and compliance

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

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

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

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

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

(dd) 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.

(ee) 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 THREE: Transfer processor to processor

(ff) OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least ten working days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(gg) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[14] 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.

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

(ii) 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.

Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

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

(jj) 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 THREE: Transfer processor to processor

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

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

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

Clause 11

Redress

(nn) 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.

(oo) 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.

(pp) 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.

(qq) 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.

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

(ss) 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

(tt) 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.

(uu) 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.

(vv) 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.

(ww) 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.

(xx) 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.

(yy) 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.

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

Clause 13

Supervision

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

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1)

of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE THREE: Transfer processor to processor

(c) 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.

(d) 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[15];

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

(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.

(e) 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.

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

(g) 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). [For Module Three: The data exporter shall forward the notification to the controller.]

(h) 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 [for Module Three: , if appropriate in consultation with the controller].

The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

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

MODULE THREE: Transfer processor to processor

15.1 Notification

(i) 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.

[For Module Three: The data exporter shall forward the notification to the controller.]

(j) 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.

(k) 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.). [For Module Three: The data exporter shall forward the information to the controller.]

(l) 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.

(m) 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

---

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

(n) 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).

(o) 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. [For Module Three: The data exporter shall make the assessment available to the controller.]

(p) 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

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

(r) 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).

(s) 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 [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(t) [For Modules One, Two and Three: 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.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] 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.

(u) 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 THREE: Transfer processor to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

MODULE THREE: Transfer processor to processor

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

(w) The Parties agree that those shall be the courts of Ireland.

(x) 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.

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

Annexure C

INTERNATIONAL DATA TRANSFER ADDENDUM

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

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

Addendum EU SCCs	**The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:** **Date:** **Reference:** **Other Identifier:** **the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:**

Module	Module in Operation	Clause 7 Docking Clause	Clause 11 (Option)	Clause 9 a (Prior Authorisation / General Authorisation)	Clause 9 a (Time Period)	Is personal data received from the Importer combined with personal data collected by the Exporter
1	No					
2	Yes	No	No	Yes	30 Business Days	
3	No					
4	No					

Start Date	**The Start date for this Addendum shall coincide with the start data of each Agreement between the Parties.**	
The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
	The Exporter is the Customer as identified in Annex I.A. of the EU SCCs found in Addendum I to the DPA.	The Importer is EC-Council.
Parties Details	Exporters' details are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.	Importer's details are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.
Key Contact	Exporters' Key Contact details are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.	Importer's Key Contact details are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.
Signature	The Parties agree that their acceptance to the DPA or the EU SCCs in Annex I.A. of Addendum I shall serve to legally bind the Parties to this Addendum.	

Table 2: Selected SCCs. Modules and Selected Clauses

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:

Annex 1A: List of Parties:	Parties are as set forth in Annex I.A. of the EU SCCs found in Addendum I to the DPA.
Annex 1B: Description of Transfer:	Description of Transfer is as set forth in Annex I.B. of the EU SCCs found in Addendum I to the DPA.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:	TOMs are as set forth in Annexure A to the DPA.

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: [ ] Importer [ ] Exporter [X]Neither Party. Clause 18 will apply in the event the Approved Addendum changes in accordance therewith.

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 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. Not applicable. Intentionally left blank;

e. Clause 8.8(i) of Module 2 is replaced with:

"the onward transfer is to a country befitting 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. Not applicable. Intentionally left blank;

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.

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 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 the 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.**