DATA PROCESSING ADDENDUM

This Data Processing Addendum ('DPA') applies to the extent Secure Code Warrior is a processor of customer data (defined below) and is automatically incorporated and effective alongside Secure Code Warrior's SaaS Subscription Agreement. If a separate agreement governs the relationship between the parties, this DPA becomes effective upon execution, as evidenced by signatures on Page 9.

1 Definitions

Applicable data protection law	All data protection laws and regulations applicable to Secure Code Warrior in connection with the processing of personal data, including those with extraterritorial effect.
Personal data, data subject, processing, controller, processor, personal data breach, sub-processor	These have the same meaning as the General Data Protection Regulation (EU) 2016/679 (GDPR) and may be interpreted to include similar terms or concepts used in other applicable data protection laws.
Governing agreement	The subscription agreement, terms of service or commercial SaaS terms that governs the relationship between the parties.
SCW Learning Platform	The software developed and owned by Secure Code Warrior and made available to the customer as a service via the internet (including documentation, updates, supplements, modification, addition and/or adaptation of the SCW Learning Platform to enable or include certain features and/or functionality) under the terms and conditions of the governing agreement.
Customer data	Personal data that is processed by Secure Code Warrior (or sub-processors) on behalf of the customer to fulfil Secure Code Warrior's obligations with respect to the provision of the services under the governing agreement, in accordance with this DPA.
SCW data	Personal data processed by Secure Code Warrior on its own behalf and for its own purposes in compliance with applicable data protection law.
Data subject request	Request related to processing of customer data that is sent to Secure Code Warrior by a data subject in accordance with their enforceable rights under applicable data protection law.
Transfer mechanisms	Legal instruments that permit the lawful transfer of personal data from one jurisdiction to another under applicable data protection law.

Third country	Country or territory not recognised under applicable data protection law as providing an adequate level of protection for personal data.
EU SCCs	The standard contractual clauses executed by and between customer and Secure Code Warrior (Exhibit A) for the transfer of customer data from the EU and European Economic Area ("EEA") to third countries in accordance with applicable data protection law. The current implementation of which was adopted by the European Comission on 4 June 2021 and is set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
UK addendum	The International Data Transfer Addendum to the EU SCCs executed by and between customer and Secure Code Warrior (Exhibit B) for the transfer of customer data from the United Kingdom to third countries in accordance with applicable data protection law. The current implementation of which came into force on 21 March 2022 following UK parliamentary approval and is set out at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/
Supervisory authority	Independent public authority which is responsible within its jurisdiction for monitoring and enforcing compliance with applicable data protection law.
Instruction	Direction (either in writing or through software) to process customer data in a particular way, issued by the customer or its representatives to Secure Code Warrior.

2 Data processing

2.1 This DPA applies when customer data is processed by Secure Code Warrior in order to facilitate and support customer's use of the SCW Learning Platform. In this context, Secure Code Warrior acts as processor and the customer is the controller of the customer data. Where there is a conflict between the governing agreement and this DPA in relation to the processing of personal data, the terms of the DPA prevail.

2.2 This DPA does not apply where Secure Code Warrior is acting as an independent controller and processes SCW data in accordance with its obligations under applicable data protection law. See our privacy policy for more information (https://www.securecodewarrior.com/trust/privacy-policy).

2.3 Details of data processing:

2.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer data.

2.3.2 **Duration.** As between Secure Code Warrior and the customer, the duration of the data processing is determined by the governing agreement.

2.3.3 **Nature and purpose.** Secure Code Warrior will process Customer data as necessary to perform the services pursuant to the governing agreement, and in accordance with further instructions by the customer in relation to the services.

2.3.4 **Type of customer data**:

- Phone number (trial users only)
- Email address
- Name (first and last)
- Device information (browser type, device identifier and IP address)
- Professional information (employer, team name, role, job title)
- Location information (country/region and geo-location derived from IP address)
- Platform performance metrics and assessment data

2.3.5 **Categories of data subjects.** The data subjects could include customers, contacts, prospects, employees or contractors of the customer.

2.3.6 **Processing operations.** The objective of the processing of customer data by Secure Code Warrior is the provision of services to the customer in accordance with the governing agreement.

3 Customer instructions

The parties agree that this DPA and the governing agreement constitute customer's documented instructions regarding Secure Code Warrior's processing of customer data ("**documented instructions**"). Secure Code Warrior will process customer data only in accordance with these documented instructions. Additional instructions outside the scope of the documented instructions (if any) require prior written agreement between Secure Code Warrior and the customer, including agreement on any additional fees payable by the customer to Secure Code Warrior for carrying out such instructions. The customer is entitled to terminate this DPA and the governing agreement if Secure Code Warrior declines to follow reasonable and lawful instructions that are outside the scope of, or changed from, those given or agreed to be given in this DPA. If Secure Code Warrior believes an instruction infringes applicable data protection law, it will promptly inform the customer and the customer is entitled to withdraw or modify such an instruction.

4 Customer obligations

The customer agrees that it is responsible for complying with its obligations under applicable data protection law to enable the lawful processing of customer data by Secure Code Warrior for the duration and purposes of this DPA and the governing agreement.

5 Confidentiality of customer data

Secure Code Warrior will not access or use, or disclose to any third party, any customer data, except as necessary to maintain or provide the services in accordance with the documented instructions, or as necessary to comply with the law or a valid and binding order of a governmental body (see Section 11 below).

6 Security of customer data

6.1 **Security Measures.** 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 varying likelihood and severity of risk to the rights and freedoms of natural persons, Secure Code Warrior shall maintain appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing customer data. The current technical and organisational security measures are described in Annex II.

6.2 **Confidentiality of Personnel.** Secure Code Warrior will ensure that all personnel and subcontractors who have access to customer data are under an appropriate obligation of confidentiality.

7 Location and international transfers of customer data

7.1 **Deployment locations.** Customer data will only be hosted in the region(s) that the customer chooses to deploy. At present Secure Code Warrior provides hosting facilities in the US and EU regions.

7.2 **Other processing locations.** Certain features/functionality of the services require transfers of customer data to a third country. When required by applicable data protection law, such transfers will be governed by the provisions of 7.4 below.

7.3 **Change of location.** With the exception of sub-processors covered under Section 9 of this DPA, Secure Code Warrior may not change the primary hosting location without the prior written authorization of the Customer.

7.4 **Transfer mechanism.** Where the transfer of customer data is from the EEA or the United Kingdom to a third country, Secure Code Warrior agrees to process that customer data in compliance with the provisions set out in Exhibit A and Exhibit B respectively. If the customer is transferring customer data from a different jurisdiction and an alternative transfer mechanism is required, it is the customer's responsibility to inform Secure Code Warrior and assist with drafting an appropriate addendum to this DPA if required.

8 Assistance with data subject requests

8.1 Secure Code Warrior shall, to the extent permitted by law, promptly notify the customer upon receipt of a data subject request. Secure Code Warrior will also advise the data subject to submit their request to the customer who will be responsible for responding to the data subject.

8.2 Secure Code Warrior shall, at the request of the customer and taking into account the nature of the processing related to any data subject request, apply appropriate technical and organisational measures to assist customer in complying with the customer's obligation to respond to the data subject request provided that:

a) the customer is itself unable to respond without Secure Code Warrior's assistance; and

b) Secure Code Warrior is able to do so in accordance with all applicable laws, rules, and regulations.

The customer shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance provided by Secure Code Warrior.

9 Sub-processing

9.1 **Authorised sub-processors.** The customer provides its general authorization for the appointment of the sub-processors listed in Annex III of the DPA.

9.2 Secure Code Warrior shall inform the customer of any intended changes concerning the addition or replacement of sub-processors at least thirty (30) days prior to such changes, thereby giving the customer the opportunity to raise reasonable objections (if any) prior to the engagement of the sub-processor(s).

9.3 To object to a sub-processor, the customer can write to privacy@securecodewarrior.com and provide reasons for such objection. Secure Code Warrior will make reasonable efforts to address the customer's concerns, including making reasonable efforts to find an alternative sub-processor. If Secure Code Warrior is not able to address the customer's concerns, the customer has the right to opt out from the service provided with the use of this sub-processor or terminate this DPA pursuant to the governing agreement, without penalty. Such termination shall not relieve the customer of any fees owed to Secure Code Warrior for the service provided until termination.

9.4 Secure Code Warrior will restrict the sub-processor's processing of customer data to what is necessary to provide or maintain the services in accordance with the governing agreement, and Secure Code Warrior will prohibit the sub-processor from accessing customer data for any other purpose.

9.5 Secure Code Warrior will enter into an agreement with the sub-processor and, to the extent necessary, Secure Code Warrior will impose on the sub-processor the same contractual obligations that Secure Code Warrior has under this DPA. For the sub-processors that are based in a third country, Secure Code Warrior will also ensure that an appropriate transfer mechanism is in place.

9.6 Secure Code Warrior will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processor that are in breach of this DPA.

10 Audits and data breach

10.1 At its own cost, the customer has the right to perform (itself or by a mandated auditor) a maximum of one (1) audit in any twelve (12) month period, to verify whether the provisions of this DPA and applicable data protection law are complied with as they relate to customer data.

10.2 The customer will notify Secure Code Warrior about the planned audit in writing, with as much notice as it is reasonably able to and at least fifteen (15) business days in advance.

10.3 Secure Code Warrior will provide all reasonable assistance to the audit and/or related assessments under applicable data protection law and will make available all information reasonably relevant in this respect.

10.4 In the event of a personal data breach involving customer data, Secure Code Warrior shall:

a) inform the customer (without undue delay and within no later than two (2) business days and take such steps Secure Code Warrior deems necessary and reasonable to remedy the breach (to the extent that doing so is within Secure Code Warriors reasonable control); and

b) provide the customer with reasonable cooperation and assistance necessary for the customer to comply with its obligations under applicable data protection law with respect to notifying (i) the relevant supervisory authority and (ii) affected data subjects without undue delay, taking into account the nature of the processing and the information available to Secure Code Warrior.

10.5 The obligations described in Sections 10.4 shall not apply in the event that a security incident and/or personal data breach results from the actions or omissions of the customer. Secure Code Warrior's obligation to report or respond to a personal data breach under Sections 10.4 will not be construed as an acknowledgement by Secure Code Warrior of any fault or liability with respect to the event.

11 Requests for customer data

11.1 If we receive a valid and binding legal order from any government or regulatory body for disclosure of customer data, Secure Code Warrior will use best efforts to redirect the authority to seek that information directly from the customer.

11.2 If, despite our efforts, we are compelled to disclose customer data, we will:

a) promptly notify the customer (if legally permitted) so that they may seek a protective order or other appropriate remedy. If we are prohibited from notifying customer, we will use best efforts to obtain a waiver of that prohibition;

b) challenge any overly broad or inappropriate order; and

c) disclose only the minimum amount of customer data necessary to satisfy the order.

12 Limitation of liability

The total liability of each of the customer and Secure Code Warrior (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this DPA, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate, exceed the limitation of liability set forth in the governing agreement.

13 Return or deletion of customer data.

Following completion of the services Secure Code Warrior shall return or delete customer data in accordance with the customer's instructions. In the absence of such an instruction, customer data will be retained in accordance with the timeframes set out in Secure Code Warrior's privacy policy (https://www.securecodewarrior.com/trust/privacy-policy)

14 Governing law

14.1 Subject to 14.2, this DPA is governed by the laws of the governing agreement. Any dispute arising from or relating to this DPA, shall be subject to the jurisdiction of the same courts as outlined in the governing agreement.

14.2 To the extent required to comply with applicable data protection law (and only in matters relating to compliance with this DPA or a party's actions under applicable data protection law) this DPA shall also be governed and interpreted by the laws, and subject to the courts, of the jurisdiction responsible for enacting and enforcing applicable data protection law.

14.3 Regarding 14.2, the parties recognise and agree to the jurisdiction of the laws of:

a) England and Wales (UK)
b) Belgium (EU / EEA)
c) New South Wales (Australia)

15 Customer data related to residents of California

15.1 When processing customer data related to residents of California, the parties acknowledge and agree that the customer is a “business” and Secure Code Warrior is a “service provider” for the purposes of the California Consumer Privacy Act (“CCPA”) as amended by the California Privacy Rights Act (“CPRA”) (collectively “applicable California law”) .

15.2 For the purposes of applicable California law, the “business purposes” for processing customer data related to residents of California are set out in 2.3.3 of the DPA and further include the processing and combination of analytics data generated by the SCW Learning Platform for Secure Code Warrior’s reporting and promotional purposes.

15.3 As a service provider, Secure Code Warrior will not (i) retain, use or disclose or otherwise process customer data for any purpose other than to perform the services under this agreement or as otherwise permitted by applicable California law; (ii) sell customer data related to residents of California; or (iii) retain, use or disclose customer data related to residents of California outside of the direct business relationship with the customer.

15.4 The parties certify that they understand and will comply with applicable California law and restrictions contained in the DPA. Secure Code Warrior agrees to promptly notify the customer should Secure Code Warrior determine that it is no longer able to comply with the obligations set forth in this DPA.

[Customer Name]	Secure Code Warrior [Entity]
Signature:	Signature:
Name:	Name:
Title:	Title:
Date:	Date:

EXHIBIT A

Standard Contractual Clauses
Controller-to-Processor Transfers

SECTION I

Clause 1

Purpose and scope

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

b) The Parties:

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

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

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

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

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

---

[1] *Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the Standard Contractual Clauses included in Decision 2021/915.*

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 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

3) 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

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

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

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

8.2 Purpose Limitation

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

8.3 Transparency

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

8.4 Accuracy

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

8.5 Duration of processing and erasure or return of data

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

8.6 Security of processing

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

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

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

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation,

or data relating to criminal convictions and offences (hereinafter “sensitive data”), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if: (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer; (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question; (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

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

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

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

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

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

Clause 9

Use of sub-processors

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

b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[2] 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

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

shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

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

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

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

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

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

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

Clause 13

Supervision

a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

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

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

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([3]);

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

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

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

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

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

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

Clause 15

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

15.1 Notification

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

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

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.

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

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

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

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

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

15.2 Review of legality and data minimisation

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

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

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

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

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

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

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

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

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

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

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

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

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

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the Governing Law outlined in Section 14 of the Data Protection Addendum.

Clause 18

Choice of forum and jurisdiction

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

2) The Parties agree that those shall be the courts identified in Section 14 of the Data Protection Addendum.

3) 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.

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

EXHIBIT B

UK Addendum to EU SCCs

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

The Parties	Exporter (who sends the Restricted Transfer)	Importer (who receives the Restricted Transfer)
Parties' details	See Annex I below	See Annex I below
Key Contact	See Annex I below	See Annex I below

Table 2: Selected SCCs, Modules and Selected Clauses

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

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1	NO	N/A	N/A	N/A	N/A	N/A

2	YES	See Exhibit A above	See Exhibit A above	See Exhibit A above	See Exhibit A above	See Exhibit A above
3	NO	N/A	N/A	N/A	N/A	N/A
4	NO	N/A	N/A	N/A	N/A	N/A

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: See Annex 1 below
Annex 1B: Description of Transfer: See Annex 1 below
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex 2 below
Annex III: List of Sub processors (Modules 2 and 3 only): See Annex 3 below

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 ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

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

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

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

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

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

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

Hierarchy

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

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

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

Incorporation of and changes to the EU SCCs

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

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

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

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

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

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

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

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

    b. In Clause 2, delete the words:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

m. Clause 17 is replaced with:

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

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

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

    b. reflects changes to UK Data Protection Laws;

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

19. If the ICO issues a revised Approved Addendum under Section 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.


SECURE
CODE
WARRIOR

ANNEX I

A. LIST OF PARTIES

	Data exporter	Data importer
Name	The entity identified as “customer” in the DPA or governing agreement.	“Secure Code Warrior” as identified in the DPA or governing agreement.
Address	The customer’s address associated with its Secure Code Warrior account or as otherwise specified in the governing agreement	The address for Secure Code Warrior specified in the governing agreement.
Contact person’s name, position and contact details	The customer’s contact details associated with its Secure Code Warrior account or as otherwise specified in the governing agreement	The contact details for Secure Code Warrior specified in the governing agreement.
Activities relevant to the data transferred under these Clauses:	Performance of the services pursuant to the governing agreement.	Performance of the services pursuant to the governing agreement.
Role:	Controller	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Categories of data subjects are specified in Section 2.3 of the DPA.

Categories of personal data transferred

The personal data is described in Section 2.3 of the DPA. For more information refer to Secure Code Warrior’s privacy policy:

https://www.securecodewarrior.com/trust/privacy-policy

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

N/A

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

Continuous basis depending on the use of the services by the customer.

Nature of the processing

The nature of the processing is described in Section 2.3 of the DPA.

Purpose(s) of the data transfer and further processing

To provide the services outlined in the governing agreement.

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

Secure Code Warrior will process customer data for the duration of the governing agreement, unless otherwise agreed upon in writing, and in accordance with Secure Code Warrior's privacy policy (https://www.securecodewarrior.com/trust/privacy-policy)

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

The sub-processors will process customer data as necessary to perform the services pursuant to the governing agreement and for the duration of that agreement unless otherwise agreed in writing.

C. COMPETENT SUPERVISORY AUTHORITY

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

The data exporter's competent supervisory authority will be determined in accordance with the GDPR/UK GDPR.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES

Secure Code Warrior commits to the continuous maintenance of technical and organisational measures (TOMs) designed to safeguard information security and ensure the protection of personal data.
The below list of TOMs comply with the ISO/IEC 27001 and 27701 standards and SOC 2 framework.

We may periodically update its TOMs to address new security challenges, regulatory requirements or technological advancements. Any changes will be designed to enhance or maintain existing levels of security and data protection.

- **Encryption of data at rest and in transit:** Personal data is encrypted using industry-standard protocols to protect it from unauthorised access during storage and transmission.
- **Pseudonymization**: Personal data transformed to prevent identification without additional information that is kept separate and secure.
- **Access control:** Only authorised personnel have access to personal data, based on the principle of least privilege.
- **Multi-factor authentication (MFA)**: Employees are required to use more than one form of authentication to verify their identity, significantly reducing the risk of unauthorised access.
- **Security audits and vulnerability assessments:** Conducted periodically to identify and remediate potential security threats.
- **Data backup and recovery:** Robust data backup and disaster recovery procedures to ensure the availability and integrity of personal data in the event of a disaster or data loss incident.
- **Network security:** Firewalls, intrusion detection/prevention systems (IDPS), and other network security measures help protect against unauthorised access and cyber threats.
- **Secure development practices:** Secure coding guidelines, regular code reviews and security testing are part of the software development lifecycle.
- **Data protection policies:** Comprehensive data protection policies and procedures aligned with the EU/EEA GDPR are regularly socialised, reviewed and updated.
- **Data processing agreements:** Contracts with third parties who process personal data include clauses that require them to adhere to data protection standards and provisions equivalent to those agreed with the data controller.

- **Employee training and awareness:** Regular training sessions for employees on data protection best practices, security awareness, and the importance of protecting personal data are regularly conducted every quarter.
- **Incident response plan:** An incident response plan is in place to quickly and effectively respond to data breaches or security incidents.
- **Data Protection Impact Assessments (DPIAs):** As required by data protection regulation, DPIAs are conducted for processing activities that pose a high risk to the rights and freedoms of individuals. Data processing activities that do not meet the regulatory threshold are also subject to other types of risk assessments to ensure data protection principles and obligations have been sufficiently considered and addressed.
- **Supplier and third-party management:** Due diligence exercises are established to assess and monitor the data protection practices of suppliers and third parties that handle personal data.
- **Compliance monitoring and reporting:** Mechanisms established to monitor compliance with data protection laws and regulations, as well as reporting to relevant stakeholders and authorities as necessary.

Further details regarding our information security program is available at https://www.securecodewarrior.com/trust

ANNEX III

LIST OF SUB-PROCESSORS

An up-to-date list of sub-processors used for the provision of the services is maintained at https://www.securecodewarrior.com/trust/sub-processors

Sub-processor and data processing location	Purpose	Personal data processed	Contact and privacy policy
Secure Code Warrior group entities • Australia • EU/EEA • United Kingdom • USA	Product support, maintenance and delivery	• Phone number (trial users only) • Email address • Name (first and last) • Device information (browser type, device identifier and IP address) • Professional information (employer, team name, role, job title) • Location information (country/region and geo-location derived from IP address) • Platform performance metrics and assessment data	privacy@securecodewarrior.com https://www.securecodewarrior.com/trust/privacy-policy

Amazon Web Services (AWS) • EU/EEA • USA	Cloud storage host for our website, platform and infrastructure, and email notification service provider	• Personal data collected by AWS • Email address • Name (first and last) • Device information (browser type, device identifier and IP address) • Location information (country/region and IP geo-location)	**Amazon Web Services, Inc:** Attn: AWS Legal 410 Terry Avenue North Seattle WA 98109-5210, USA **Amazon Web Services EMEA SARL:** 38 Avenue John F. Kennedy L-1855 Luxembourg aws-EU-privacy@amazon.com https://aws.amazon.com/privacy/
Datadog • USA	Application log management, monitoring and alerting	• Email address • User ID • Device information (browser type, device identifier and IP address) • Location information (country/region and IP geo-location)	Datadog, Inc. 620 8th Avenue Floor 45 New York NY 10018, USA privacy@datadoghq.com https://www.datadoghq.com/legal/privacy/
EverAfter • EU/EEA • Israel • USA	Customer onboarding and ongoing success	• Email address • Name (first and last) • Device information (browser type, device identifier and IP address)	https://www.everafter.ai/legal/privacy EverAfter AI Ltd. Yigal Alon 82 Tel Aviv Israel 6789124 privacy@everafter.ai
MongoDB • EU/EEA • USA	Cloud database storage and management	• Email address • Name (first and last) • Device information (browser type, device identifier and IP address) • Professional information (employer, team name, role, job title)	Attn: Legal Department MongoDB, Inc. 1633 Broadway 38th Floor New York NY 10019, USA privacy@mongodb.com https://www.mongodb.com/leg

		• Location information (country/region and IP geo-location) • Assessment information (challenge stats/results) • Preferred language	al/privacy-policy
Salesforce • Australia • EU/EEA • United Kingdom • USA	Platform usage insights, metrics and visualisations	• Email address • Name (first and last) • Professional information (employer, team name, role, job title) • Assessment information (challenge stats/results)	https://www.salesforce.com/privacy/overview/ 415 Mission Street, 3rd Floor San Francisco CA 94105, USA privacy@salesforce.com
Usersnap • EU/EEA	Customer bug reports	• Email address • Device information (browser type, device identifier and IP address)	Energiestrasse 1 A-4020 Linz Austria contact@usersnap.com https://usersnap.com/privacy-policy
Zendesk • USA	Customer support	• Email address • Device information (browser type, device identifier and IP address)	Attn: Privacy Team 989 Market Street San Francisco, CA 94103, USA privacy@zendesk.com https://www.zendesk.co.uk/company/agreements-and-terms/privacy-notice