This Data Processing Addendum (“**Addendum**”) forms part of the written agreement entered into by and between Checkmarx Ltd. and/or an affiliate of Checkmarx Ltd. (collectively “**Checkmarx**”) and a Checkmarx customer (the “**Customer**”, and each of Checkmarx and Customer a “**Party**” and collectively the “**Parties**”) which incorporates this Addendum by reference (“**Services Agreement**”). The purpose of this Addendum is to reflect the Parties’ agreement with regard to the processing of Customer Personal Data in accordance with the requirements of Data Protection Legislation.

RECITALS

(A) The Customer and Checkmarx have entered into a Services Agreement that may require Checkmarx to process personal data on behalf of the Customer.

(B) This Addendum sets out the additional terms, requirements and conditions on which Checkmarx will process personal data when providing Services to the Customer.

1. DEFINITIONS AND INTERPRETATION

1.1 The following definitions shall apply:

Business Day means a business day in Israel when banks in Tel Aviv are open for business.

Customer Personal Data means any Customer personal data which Checkmarx processes, receives or otherwise has access to as a result of or in connection with the provision of the services under the Services Agreement.

Data Protection Legislation means all applicable data protection and privacy legislation in force from time to time including the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"), the Privacy and Electronic Communications Directive 2002/58/EC and any other applicable European Union or other legislation relating to personal data.

SCC means the European Commission's Standard Contractual Clauses for the transfer of Personal Data from the European Union to processors established in third countries, as set out in the Annex to Commission Decision 2010/87/EU a copy of which comprises Schedule 2.

Services Agreement has the meaning given to it above.

Services means the processing operations to be carried out in the performance of the Services Agreement as set forth thereto.

Term has the meaning given to it in Clause 10.1.

1.2 All data protection terms used in this Addendum, including 'personal data', 'process', 'controller', 'processor', 'data subject', 'personal data breach' and 'supervisory authority' shall have the meaning ascribed to them in the GDPR.

1.3 Interpretations and defined terms set forth in the Services Agreement apply to the interpretation of this Addendum.

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

1.5 A reference to "writing" or "written" includes email.

1.6 In the case of conflict or ambiguity between:

1.6.1 any of the provisions of this Addendum and the provisions of the Services Agreement, the provisions of this Addendum shall prevail; and

1.6.2 any of the provisions of this Addendum and any executed SCC, the provisions of the executed SCC will prevail.

2. PERSONAL DATA AND PROCESSING PURPOSES

2.1 Each Party shall comply with its respective obligations under the Data Protection Legislation in relation to all Customer Personal Data that may be processed in the performance and operation of this Addendum.

2.2 The Parties agree and acknowledge that the processing operations to be carried out in the performance of this Addendum conform to the description set out in Schedule 1 to this Addendum.

2.3 With respect to the Parties' respective rights and obligations under this Addendum, if at any time Checkmarx processes Customer Personal Data then the Parties agree that Customer is the controller and that Checkmarx is the processor.

2.4 The Customer retains control of the Customer Personal Data and remains responsible for its compliance obligations under applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Checkmarx. The Customer's instructions shall comply with the Data Protection Legislation.

2.5 The Customer shall have sole responsibility for the accuracy, quality and legality of Customer Personal Data provided to Checkmarx.

2.6 Checkmarx shall only process Customer Personal Data:

2.6.1 as needed to provide the Services;

2.6.2 in accordance with the documented instructions that it has received from Customer, including with regard to any transfers of personal data to third countries or international organisations; and

2.6.3 as needed to comply with applicable law (in which case, Checkmarx shall provide prior notice to the Customer of such legal requirement, unless that law prohibits such disclosure on important grounds of public interest).

3. SECURITY AND PERSONNEL

3.1 Checkmarx shall ensure that persons authorised to process Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3.2 Checkmarx shall ensure the security of the Customer Personal Data that it processes in accordance with the requirements of the GDPR, in particular:

3.2.1 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, Checkmarx shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(i) the pseudonymisation and encryption of Customer Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing;

(iii) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3.2.2 in assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Customer Personal Data transmitted, stored or otherwise processed; and

3.3 Checkmarx shall take steps to ensure that any natural person acting under the authority of Checkmarx who has access to personal data does not process them except on instructions from the Customer, unless he or she is required to do so by EU or EU Member State law.

4. CHECKMARX ASSISTANCE RELATING TO ANY CUSTOMER PERSONAL DATA

4.1 Checkmarx shall provide reasonable assistance to the Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights.

4.2 Checkmarx shall notify the Customer within four (4) Business Days if it receives a request from a data subject to exercise any of their rights under Data Protection Legislation.

4.3 Checkmarx shall provide reasonable assistance to the Customer, taking into account the nature of processing and the information available to Checkmarx, to ensure the Customer's compliance with its obligations in respect of the security of processing of Customer Personal Data, conducting data protection impact assessments and prior consultations with supervisory authorities.

4.4 Checkmarx shall immediately inform the Customer if, in its opinion, an instruction infringes the Data Protection Legislation.

5. PERSONAL DATA BREACHES

5.1 Checkmarx shall without undue delay notify the Customer if it becomes aware of a personal data breach relating to any Customer Personal Data and shall provide reasonable assistance to the Customer in responding thereto and any notification requirements which arise as a result thereof.

5.2 Checkmarx will cover all reasonable expenses associated with the performance of its obligations set out in Clause 5.1 unless the personal data breach arose from the Customer's specific instructions, negligence, wilful default or breach of this Addendum in which case (without prejudice to Checkmarx's other rights and remedies hereunder) the Customer will cover all expenses associated therewith.

6. SUB-PROCESSORS

6.1 Customer hereby grants to Checkmarx a general written authorisation for Checkmarx to use sub-processors for the provision of the Services, provided that Checkmarx shall ensure that:

6.1.1 it engages such sub-processors by written agreement and the terms of each written agreement must be consistent with the material terms of this Addendum, as if the sub-processor were Checkmarx;

6.1.2 where the sub-processor fails to fulfil its obligations under such written agreement, Checkmarx remains fully liable to the Customer for the sub-processor's performance of its agreement obligations;

6.1.3 the sub-processor complies with its obligations under the Data Protection Legislation relating to any Customer Personal Data and has sufficient organisational and technical measures in place to guarantee the protection of Customer Personal Data against unauthorised or unlawful processing; and

6.1.4 it will notify the Customer of any intended changes concerning the addition or replacement of a sub-processor thereby giving the Customer the opportunity to object to the addition or replacement within fourteen (14) days of the notification.

6.2 Those sub-processors approved as at the commencement of this Agreement are located at https://info.checkmarx.com/hubfs/Legal/List%20of%20Checkmarx%20Sub-processors%202020-08-19-1.pdf.

7. CROSS-BORDER TRANSFERS OF PERSONAL DATA

7.1 Checkmarx shall not transfer or otherwise process Customer Personal Data outside the European Economic Area ("**EEA**") or to or in a third country which does not provide adequate protection for personal data without obtaining the Customer's prior written consent.

7.2 If any Customer Personal Data transferred between the Customer and Checkmarx requires execution of SCC in order to comply with the Data Protection Legislation (where the Customer is the entity exporting Customer Personal Data to Checkmarx outside the EEA), the parties will complete all relevant details in, and execute, the SCC contained in Schedule 2, and take all other actions required to legitimise the transfer.

7.3 The Customer hereby consents to the transfer of Customer Personal Data to Checkmarx and Checkmarx sub-processors which are located outside the EEA subject to Checkmarx's compliance with Clause 7.5.

7.4 Where such consent is granted, Checkmarx may only transfer or otherwise process Customer Personal Data outside the EEA to a territory which does not provide adequate protection for personal data if adequate safeguards are put in place to protect Customer Personal Data.

7.5 If the Customer consents to appointment by Checkmarx of a sub-processor located outside the EEA (apart from in a third country which has been assessed by the European Commission and/or the relevant UK authority following the UK’s exit from the EU, as providing adequate protection for personal data) in compliance with the provisions of Clause 6, then the Customer authorises Checkmarx to enter into SCC with the sub-processor on its behalf wherein the Customer shall be regarded as the “data exporter” and the sub-processor as the “data importer”. Checkmarx will make the executed SCC available to the Customer on request.

8. RECORDS AND AUDITS

8.1 Checkmarx shall maintain all records required by Article 30(2) of the GDPR, and (to the extent they are applicable to Checkmarx's activities for Customer) Checkmarx shall make them available to Customer upon written request. The records relating to any Customer Personal Data shall contain the following information:

8.1.1 the name and contact details of the Customer and, where applicable, the joint controller, the Customer's representative and the data protection officer;

8.1.2 the categories of processing carried out on behalf of the Customer;

8.1.3 where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation, including where applicable, the documentation of any suitable safeguards required by the GDPR Article 49(1)(second sub-paragraph);

8.1.4 where possible, a general description of the technical and organisational security measures.

8.2 In relation to its processing of Customer Personal Data Checkmarx shall during the Term provide the Customer with information reasonably necessary to demonstrate compliance with the obligations laid down in the GDPR, and shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer provided that:

8.2.1 The Customer gives at least thirty (30) days' prior written notice to conduct such audit or inspection;

8.2.2 the auditor is subject to binding obligations of confidentiality; and

8.2.3 the audit or inspection is undertaken so as to cause minimal disruption to Checkmarx's business and other customers.

8.3 Upon the Customer’s written request, Checkmarx shall delete or return all Customer Personal Data to the Customer following the end of the Term, and shall delete all existing copies unless applicable EU member state law requires storage of Customer Personal Data.

9. CUSTOMER WARRANTY

9.1 The Customer warrants that it:

9.1.1 shall comply with all requirements and obligations of applicable Data Protection Laws;

9.1.2 shall have sole responsibility for the accuracy, quality and legality of Customer Personal Data; and

9.1.3 is entitled to disclose the Customer Personal Data to Checkmarx so that Checkmarx may process the Customer Personal Data in accordance with the Addendum on Customer's behalf.

9.2 The Customer shall at all times both during and after the Term fully indemnify and hold Checkmarx harmless from all claims and all direct, indirect or consequential losses and liabilities (including loss of profits, loss of business, depletion of goodwill and similar losses, including attorney's fees) awarded against, or incurred or paid by, Checkmarx as a result of or in connection with any actual or alleged breach by or on behalf of the Customer of any of the warranties set out in Clause 9.1.

10. TERM AND TERMINATION

10.1 This Addendum shall commence on the effective date of the Service Agreement.

10.2 This Addendum will remain in full force and effect until the earlier of the following dates (subject to Clause 10.2):

10.2.1 the termination of the Services Agreement; or

10.2.2 Checkmarx ceases to retain any Customer Personal Data related to the Services Agreement in its possession or control.

10.3 Any provision of this Addendum that expressly or by implication comes into or continues in force on or after termination of the Services Agreement in order to protect Customer Personal Data will remain in full force and effect.

10.4 If a change in any Data Protection Legislation prevents either Party from fulfilling all or part of its Services Agreement obligations, the Parties will suspend the processing of Customer Personal Data until that processing complies with the new requirements. If the Parties are unable to bring the Customer Personal Data processing into compliance with the Data Protection Legislation within sixty (60) days, either Party may terminate the Services Agreement on written notice to the other Party. Notwithstanding anything to the contrary in the Services Agreement, if the Services Agreement is terminated pursuant to this clause, all amounts that would have otherwise become due and payable after the effective date of such termination shall become due and payable on the effective date of such termination of the Services Agreement. Furthermore, Customer shall not be entitled to a refund of any amounts already paid under the Services Agreement.

11. SEVERANCE

If any provision or part-provision of this Addendum is or becomes invalid, illegal or unenforceable it shall be deemed deleted but that shall not affect the validity and enforceability of the rest of this Addendum.

12. NOTICE

12.1 Any notice or other communication given to a Party under or in connection with this Addendum must be in writing and delivered to:

12.1.1 for the Customer:

Attention:
Address: As set forth in the Services Agreement

12.1.2 for Checkmarx:

Attention: Chief Financial Officer
Address: As set forth in the Services Agreement

12.2 Clause 12.1 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

13. LIMITATION OF LIABILITY

Each Party’s and all of its Affiliates’ liability, taken together in the aggregate, arising out of or related to this Addendum, whether in contract, tort or under any other theory of liability, is subject to the ‘Limitation of Liability’ section of the Services Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that party and all of its Affiliates under the Agreement and this Addendum together.

SCHEDULE 1

Scope of the Data Processing

Description of processing activities:

1. Subject matter

The subject matter of the processing is as set out in the applicable Services Agreement.

2. Duration of the processing

For the purpose of providing the Services to Customer: during the term of the Services Agreement. For other specified purposes: as reasonably determined by Checkmarx.

3. Nature and purpose of the processing

The nature and purpose of the processing are:

- for Checkmarx to perform its obligations pursuant to the Services Agreement;
- for delivery and provision of the Services to the Customer;
- for customer support and technical troubleshooting;
- to communicate with the Customer and its end users; and
- to comply with law, including law enforcement requests.

4. Categories of Personal Data

Name, phone number, postal address, email address, position, transactions, usage details (incl. e.g. URLs visited, events triggered on defined actions such as page loads, clicks, logins and purchases), IP addresses, cookies, analytics data.

5. Categories of data subjects

Current, former and potential employees and subcontractors of the Customer and other authorized users of the Services.

6. Sub-Processors

The current list of sub-processors are set out in Schedule 3.

SCHEDULE 2

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: ....

address: ....

tel: ....

fax: ....

e-mail: ....

Other information needed to identify the organisation ....

(**the data exporter**)

Name of the data importing organisation: ....

address: ....

tel: ....

fax: ....

e-mail: ....

Other information needed to identify the organisation ....

(**the data importer**)

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Annex A.

1. Definitions

For the purposes of the Clauses:

(a) **personal data**, **special categories of data**, **process/processing**, **controller**, **processor**, **data subject** and **supervisory authority** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1);

(b) **the data exporter** means the controller who transfers the personal data;

(c) **the data importer** means the processor who agrees to receive from the data exporter personal data intended for processing on its behalf after the transfer in accordance with its instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) **the sub-processor** means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with its instructions, the terms of the Clauses and the terms of the written subcontract;

(e) **the applicable data protection law** means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) **technical and organisational security measures** means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

2. Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Annex A which forms an integral part of the Clauses.

3. Third-party beneficiary clause

3.1 The data subject can enforce against the data exporter this clause 3, clause 4(b) to clause 4(i), clause 5(a) to clause 5(e) and clause 5(g) to clause 5(j), clause 6.1 and clause 6.2, clause 7, clause 8.2 and clause 9 to clause 12 as third-party beneficiary.

3.2 The data subject can enforce against the data importer this clause 3.2, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2 and clause 9 to clause 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3.3 The data subject can enforce against the sub-processor this clause 3.3, clause 5(a) to clause 5(e) and clause 5(g), clause 6, clause 7, clause 8.2, and clause 9 to clause 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

3.4 The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

4. Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Annex B to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to clause 5(b) and clause 8.3 to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Annex B and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subjects as the data importer under the Clauses; and

(j) that it will ensure compliance with clause 4(a) to clause 4(i).

5. Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Annex B before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

ii. any accidental or unauthorised access; and

iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Annex B which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with clause 11; and

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

6. Liability

6.1 The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in clause 3 or in clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

6.2 If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or its sub-processor of any of their obligations referred to in clause 3 or in clause 11 because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

6.3 If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in clause 3 or in clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

7. Mediation and jurisdiction

7.1 The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

7.2 The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

8. Cooperation with supervisory authorities

8.1 The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

8.2 The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

8.3 The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in clause 5(b).

9. Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely ....

10. Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

11. Sub-processing

11.1 The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

11.2 The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

11.3 The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely ....

11.4 The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

12. Obligation after the termination of personal data processing services

12.1 The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

12.2 The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full): ....

Position: ....

Address: ....

Other information necessary in order for the contract to be binding (if any): ....

Signature ....

(Stamp of organisation)

On behalf of the data importer:

Name (written out in full): ....

Position: ....

Address: ....

Other information necessary in order for the contract to be binding (if any): ....

Signature ....

(Stamp of organisation)

Annex A.

to the Standard Contractual Clauses

This Annex forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex A.

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer): ....

Data importer

The data importer is (please specify briefly your activities relevant to the transfer): ....

Data subjects

The personal data transferred concern the following categories of data subjects (please specify) ....

Categories of data

The personal data transferred concern the following categories of data (please specify) ....

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify) ....

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify) ....

DATA EXPORTER DATA IMPORTER

Name:...

Authorised signature:.........................

Annex B.

to the Standard Contractual Clauses

This Annex B forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with clause 4(d) and clause 5(c) (or documents/legislation attached):

....
....