EAC-BS : European Accreditation Council for Bariatric Surgery

Privacy Policy

Policy Updated: April 20, 2018

Contents

This EU Data Processing Addendum ("Addendum") supplements the On-line Application Agreement (the "Agreement") entered into by and between Members of Centres of Excellence (COE) programs or Surgeon of Excellence (SOE) ("Controller") and EAC-BS:European Accreditation Council for Bariatric Surgery Ltd ("Processor"). Any terms not defined in this Addendum shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall supersede and control.

1. Definitions

1.1 "Anonymous Data" means Personal Data that has been processed in such a manner that it can no longer be attributed to an identified or identifiable natural person without additional information unavailable to any third party other than Authorized Subcontractors.

1.2 "Authorized Employee" means an employee of Processor who has a need to know or otherwise access Personal Data to enable Processor to perform their obligations under this Addendum or the Agreement.

1.3 "Authorized Individual" means an Authorized Employee or Authorized Subcontractor.

1.4 "Authorized Subcontractor" means a third-party subcontractor, agent, reseller, or auditor who has a need to know or otherwise access Personal Data to enable Processor to perform its obligations under this Addendum or the Agreement, and who is either (1) listed in Exhibit C or (2) authorized by Controller to do so under Section 4.2 of this Addendum.

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

1.6 "Instruction" means a direction, either in writing, in textual form (e.g. by e-mail) or by using a software or online tool, issued by Controller to Processor and directing Processor to Process Personal Data.

1.7 "Personal Data" means any information relating to Data Subject which Processor Processes on behalf of Controller other than Anonymous Data, and includes Sensitive Personal Information.

1.8 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

1.9 "Privacy Shield Principles" means the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework.

1.10 "Process" or "Processing" means any operation or set of operations which is performed upon the Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction.

1.11 "Sensitive Personal Information" means a Data Subject's

(i) government-issued identification number (including social security number, driver's license number or state-issued identification number) or email address;

(ii) financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account;

(iii) genetic and biometric data or data concerning health; or

(iv) Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, sexual orientation or sexual activity, criminal convictions and offences (including commission of or proceedings for any offense committed or alleged to have been committed), or trade union membership.

1.12 "Services" shall have the meaning set forth in the Agreement.

1.13 "Standard Contractual Clauses" means the agreement executed by and between Controller and Processor and attached hereto as Exhibit B pursuant to the European Commission's decision (C(2010)593) of February 5, 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of protection.

1.14 "Supervisory Authority" means an independent public authority which is established by a member state of the European Union, Iceland, Liechtenstein, or Norway.

2. Processing of Data

2.1 The rights and obligations of the Controller with respect to this Processing are described herein. Controller shall, in its use of the Services, at all times Process Personal Data, and provide instructions for the Processing of Personal Data, in compliance with EU Directive 95/46/EC (the "Directive"), and, when effective, the General Data Protection Regulation (Regulation (EU) 2016/679) (the "GDPR" and together, "Data Protection Laws")). Controller shall ensure that its instructions comply with all laws, rules and regulations applicable in relation to the Personal Data, and that the Processing of Personal Data in accordance with Controller's instructions will not cause Processor to be in breach of the Data Protection Laws. Controller is solely responsible for the accuracy, quality, and legality of

(i) the Personal Data provided to Processor by or on behalf of Controller,

(ii) the means by which Controller acquired any such Personal Data, and

(iii) the instructions it provides to Processor regarding the Processing of such Personal Data. Controller shall not provide or make available to Processor any Personal Data in violation of the Agreement or otherwise inappropriate for the nature of the Services, and shall indemnify Processor from all claims and losses in connection therewith.

2.2 Processor shall Process Personal Data only

(i) for the purposes set forth in the Agreement,

(ii) in accordance with the terms and conditions set forth in this Addendum and any other documented instructions provided by Controller, and

(iii) in compliance with the Directive, and, when effective, the GDPR. Controller hereby instructs Processor to Process Personal Data for the following purposes as part of any Processing initiated by Controller in its use of the Services.

2.3 The subject matter, nature, purpose, and duration of this Processing, as well as the types of Personal Data collected and categories of Data Subjects, are described in Exhibit A to this Addendum.

2.4 Following completion of the Services, at Controller's choice, Processor shall return or delete the Personal Data, except as required to be retained by the laws of the European Union or European Union member states.

3. Authorized Employees

3.1 Processor shall take commercially reasonable steps to ensure the reliability and appropriate training of any Authorized Employee.

3.2 Processor shall ensure that all Authorized Employees are made aware of the confidential nature of Personal Data and have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement with Processor, any Personal Data except in accordance with their obligations in connection with the Services.

3.3 Processor shall take commercially reasonable steps to limit access to Personal Data to only Authorized Individuals.

4. Authorized Subcontractors

4.1 Controller acknowledges and agrees that Processor may (1) engage the Authorized Subcontractors listed in Exhibit C to this Addendum to access and Process Personal Data in connection with the Services and (2) from time to time engage additional third parties for the purpose of providing the Services, including without limitation the Processing of Personal Data.

4.2 Processor shall notify Controller before engaging any third party other than Authorized Subcontractors to access or participate in the Processing of Personal Data. At least ten (10) days before enabling any third party other than Authorized Subcontractors to access or participate in the Processing of Personal Data, Processor will notify Controller of that update via email. Controller may object to such an engagement in writing within ten (10) days of receipt of the aforementioned notice by Controller.

4.2.1 If Controller reasonably objects to an engagement in accordance with Section 4.2, Processor shall provide Controller with a written description of commercially reasonable alternative(s), if any, to such engagement, including without limitation modification to the Services. If Processor, in its sole discretion, cannot provide any such alternative(s), or if Controller does not agree to any such alternative(s) if provided, Processor may terminate this Addendum. Termination shall not relieve Controller of any fees owed to Processor under the Agreement.

4.2.2 If Controller does not object to the engagement of a third party in accordance with Section 4.2 within ten (10) days of notice by Processor, such third party will be deemed an Authorized Subcontractor for the purposes of this Addendum.

4.3 Processor shall ensure that all Authorized Subcontractors have executed confidentiality agreements that prevent them from disclosing or otherwise Processing, both during and after their engagement by Processor, any Personal Data both during and after their engagement with Processor.

4.4 Processor shall, by way of contract or other legal act under European Union or European Union member state law (including without limitation approved codes of conduct and standard contractual clauses), ensure that every Authorized Subcontractor is subject to obligations regarding the Processing of Personal Data that are no less protective than those to which the Processor is subject under this Addendum.

4.5 Processor shall be liable to Controller for the acts and omissions of Authorized Subcontractors to the same extent that Processor would itself be liable under this Addendum had it conducted such acts or omissions.

5. Security of Personal Data

5.1 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, Processor shall maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Processing Personal Data.

6. Transfers of Personal Data

6.1 Any transfer of Personal Data made subject to this Addendum from member states of the European Union, Iceland, Liechtenstein, Norway, Switzerland or the United Kingdom to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of these countries shall, to the extent such transfer is subject to such laws and regulations, be undertaken by Processor through one of the following mechanisms: (a) in accordance with the Swiss-U.S. and EU-U.S. Privacy Shield Framework and Principles issued by the U.S. Department of Commerce, both available at https://www.privacyshield.gov/EU-US-Framework (the "Privacy Shield Principles"), or (b) the Standard Contractual Clauses set forth in Exhibit B to this Addendum.

6.2 If transfers are made pursuant to 6.1(a), Processor self-certifies to, and complies with, the Swiss-U.S. and EU-U.S. Privacy Shield Frameworks, as administered by the U.S. Department of Commerce, and shall maintain such self-certification and compliance with respect to the Processing of Personal Data transferred from member states of the European Union, Iceland, Lichtenstein, Norway, Switzerland or the United Kingdom to any countries which do not ensure an adequate level of data protection within the meaning of the laws and regulations of the foregoing countries for the duration of the Agreement.

7. Rights of Data Subjects

7.1 Processor shall, to the extent permitted by law, promptly notify Controller upon receipt of a request by a Data Subject to exercise the Data Subject's right of: access, rectification, restriction of Processing, erasure, data portability, restriction or cessation of Processing, withdrawal of consent to Processing, and/or objection to being subject to Processing that constitutes automated decision- making (such requests individually and collectively "Data Subject Request(s)").

7.2 Processor shall, at the request of the Controller, and taking into account the nature of the Processing applicable to any Data Subject Request, apply appropriate technical and organizational measures to assist Controller in complying with Controller's obligation to respond to such Data Subject Request and/or in demonstrating such compliance, where possible, provided that

(i) Controller is itself unable to respond without Processor's assistance and

(ii) Processor is able to do so in accordance with all applicable laws, rules, and regulations. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor.

8. Actions and Access Requests

8.1 Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance where necessary for Controller to comply with its obligations under the GDPR to conduct a data protection impact assessment and/or to demonstrate such compliance, provided that Controller does not otherwise have access to the relevant information. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor.

8.2 Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance with respect to Controller's cooperation and/or prior consultation with any Supervisory Authority, where necessary and where required by the GDPR. Controller shall be responsible to the extent legally permitted for any costs and expenses arising from any such assistance by Processor.

8.3 Processor shall maintain records sufficient to demonstrate its compliance with its obligations under this Addendum, and retain such records for a period of three (3) years after the termination of the Agreement. Controller shall, with reasonable notice to Processor, have the right to review, audit and copy such records at Processor's offices during regular business hours.

8.4 Upon Controller's request and at Controller's choice, Processor shall, no more than once per calendar year make available for Controller's review copies of certifications or reports demonstrating Processor's compliance with prevailing data security standards applicable to the Processing of Controller's Personal Data.

8.5 In the event of a Personal Data Breach, Processor shall, without undue delay, inform Controller of the Personal Data Breach and take such steps as Processor in its sole discretion deems necessary and reasonable to remediate such violation (to the extent that remediation is within Processor's reasonable control).

8.6 In the event of a Personal Data Breach, Processor shall, taking into account the nature of the Processing and the information available to Processor, provide Controller with reasonable cooperation and assistance necessary for Controller to comply with its obligations under the GDPR with respect to notifying (i) the relevant Supervisory Authority and (ii) Data Subjects affected by such Personal Data Breach without undue delay.

8.7 The obligations described in Sections 8.5 and 8.6 shall not apply in the event that a Personal Data Breach results from the actions or omissions of Controller.

9. Return / Deletion of Personal Data.

9.1 Upon termination of these Terms, Processor, at the choice of Controller, shall

(i) return all Personal Data to Controller in a structured, commonly used and machine-readable format and delete existing copies and backups, or

(ii) destroy and delete all Personal Data and other materials containing Personal Data from Controller subject to Processing including all copies and backups. Processor shall certify accurate deletion upon Controller's request.

10. Limitation of Liability

10.1 The total liability of each of Controller and Processor (and their respective employees, directors, officers, affiliates, successors, and assigns), arising out of or related to this Addendum, whether in contract, tort, or other theory of liability, shall not, when taken together in the aggregate in accordance with the "Directive".

EXHIBIT A

Details of Processing

Nature and Purpose of Processing

The purpose of checking data quality and accreditation processes is to audit data outputs against clear, pre-defined criteria. It allows organizations to demonstrate that they are meeting and maintaining quality standards and allow data to be shared between different institutions with the assurance of consistency.

The data accreditation process is a systematic methodology incorporating standards and good practice appropriate to the field. Data quality can be reviewed internally with the achievement of standards then tested by an external audit.

Data accreditation can be thought of as a means to set a quality baseline for information systems, laying a firm foundation for further development.

The main Purposes of Processing are

- Online institution registration and company web site
- Patient health record, featuring data types extensibility
- Online review process support
- COE/SOE Inspection process support
- Statistics analysis infrastructure
- Anonymous studies, statistic and outcome reports.
- Study longitudinally the safety and efficacy of bariatric surgery
- Track key health changes following bariatric surgery

Personal data submitted on this website will be used for the purposes specified in this privacy policy or in relevant parts of the website.

We may use your personal information to:

(a) administer the website;

(b) improve your browsing experience by personalising the website;

(c) enable your use of the services available on the website;

(d) send statements and invoices to you, and collect payments from you;

(e) send you general (non-marketing) commercial communications;

(f) send you email notifications which you have specifically requested;

(g) send to you [our newsletter and other] marketing communications relating to our business [or the businesses of carefully-selected third parties] which we think may be of interest to you by post or, where you have specifically agreed to this, by email or similar technology (you can inform us at any time if you no longer require marketing communications);

(h) provide third parties with statistical information about our users - but this information will not be used to identify any individual user;

(i) deal with enquiries and complaints made by or about you relating to the website;

Where you submit personal information for publication on our website, we will publish and otherwise use that information in accordance with the license you grant to us.

We will not without your express consent provide your personal information to any third parties for the purpose of direct marketing.

Duration of Processing

Until the date the Services of the Agreement are completed, and Processing of Personal Data is no longer required.

Categories of Data Subjects

Medical Institutions
Surgeons
IBARTM Members
Patients
Auditors
Medical Researchers

Type of Personal Data

- Website Personal Data

We will collect, store, and use the following categories of data when you use our site:

Data we collect about you. If you consent to our use of cookies

If you visit our site, we will automatically collect certain technical information, for example, the type of device (and its unique device identifier) you use to access our site, the Internet protocol (IP) address used to connect your device to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system, mobile network information and platform.
We will automatically collect information about your visit to our site including the full Uniform Resource Locators (URL), clickstream to, through and from the Website (including date and time), pages you viewed, page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.

- Application Personal Data

You will provide us and we will collect, store, and use the following categories of data when you use our app:

The type of information collected depends on how you use the services of the Processor. Personal data is collected via account registration, online information forms, patient forms, submission forms, follow-up forms, event registration forms, over the phone, and/or by email. In most situations information requested will include patient data, such as patient demographics, pre-operative, intra-operative and outcome data. Physicians or other medical personnel may be asked to supply information regarding their institution of employment.

All patients should be asked to sign an informed consent form allowing their pre-operative, intra-operative and outcome data (excluding personal data such as name, surname, address, contact details e.t.c) to be included in the International Bariatric Registry (IBARTM) for the purpose of carrying out anonymous studies, statistic and outcome reports, as well as for the ongoing evaluation of the Institutions as a COE.

To ensure absolute accuracy, patients who decline to give their consent will be included in the registry only as a patient treated and will thus be included in the total number of cases managed at each Institution, purely as a statistic. However, a clear note of the patient's wish to remain anonymous and not be included in the registry should be indicated in the relevant databank check-box.

- IBARTM Member’s Personal Data

You will provide us and we will collect, store, and use the following categories of data for all IBARTM Members:

Name, Email address, Address, contact Phone numbers, Job function and employer details/institutional affiliation, Gender and nationality, Areas of scientific interest, Event Registration Information, Recruitment Information (e.g. CV, certificates, date of birth, performance assessments, reference letters etc.)

EXHIBIT B

Standard Contractual Clauses

For the purposes of Article 26(2) of Directive 95/46/EC1 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: **EAC-BS:European Accreditation Council for Bariatric Surgery Ltd**

Address: 11 Afroditis Avenue, P.C. 8522, Pafos, Cyprus

Tel.: +30 2810 232304; fax: +30 2810 234380; e-mail: info[at]eac-bs.com.

……

(the data exporter)

And

Name of the data importing organization: [Processor, Inc.]

Address: [insert]

Tel.: [insert]; fax: [insert]; e-mail: [insert]

Other information needed to identify the organization: [if needed; otherwise “not applicable”]

……

(the data importer)

each a “party”; together “the parties”, 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 t he personal data specified in Appendix 1.

Clause 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;

(b) 'the data exporter' means Controller;

(c) 'the data importer' means Processor;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor 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 his 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 organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 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 subprocessor shall be limited to its own processing operations under the Clauses.

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.

Clause 4

The data exporter agrees and warrants

Obligations of the data exporter:

(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 impo rter 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 Appendix 2 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 t he meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor 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 Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing 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 subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer und er the Clauses; and

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

Clause 5

The data importer agrees and warrants:

Obligations of the data importer:

(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 Appendix 2 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 subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 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 subprocessing, it has previously informed the data exporter and obtained its prior written consent; (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

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

Clause 6

Liability

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 subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

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 his subprocessor 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 of 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 subprocessor of its obligations in order to avoid its own liabilities.

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 subprocessor 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 subprocessor agrees that the data subject may issue a claim against the data subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

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.

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.

Clause 8

Cooperation with supervisory authorities

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

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, 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.

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

Clause 9

Governing Law

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

Clause 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 Clause.

Clause 11

Subprocessing

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 subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses2. Where the subprocessor 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 subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor 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 subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing 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.

4. The data exporter shall keep a list of subprocessing 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.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to th e 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.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or o f 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: Eva Panagopoulou

Position: Program Co-ordinator

Other information necessary in order for the contract to be binding (if any): [if needed; otherwise “not applicable”]

(stamp of organisation)

Signature…….

On behalf of the data importer:

Name (written out in full):

Position: (written out in full):

Address: (written out in full):

Other information necessary in order for the contract to be binding (if any): [if needed; otherwise “not applicable”]

(stamp of organisation)

Signature…….

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 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 Appendix.

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

Special categories of data (if appropriate)

Data importer

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

Special categories of data (if appropriate)

Data subjects

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

Special categories of data (if appropriate)

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):

Special categories of data (if appropriate)

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

Special categories of data (if appropriate)

DATA EXPORTER

Name: [Controller, Inc.]

Authorised Signature ……

DATA IMPORTER

Name[Processor, Inc.]

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix 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 Clauses 4(d) and 5(c) (or document/legislation attached):

Special categories of data (if appropriate)

EXHIBIT C

Authorized Subcontractors

Controller acknowledges and agrees that the following entities shall be deemed Authorized Subcontractors that may Process Personal

Data pursuant to this Addendum:

- IFSO
- EAC-BS Support Team: Software engineer(s) who applies the principles of software engineering to the design, development, maintenance, testing, and evaluation of computer software.
- Auditor/s
- IBAR users