ATTACHMENT E: TERMS FOR SUPPLIERS PROCESSING DATA SUBJECT TO DATA PROTECTION REGULATIONS

If the Purchase Order is issued for services that require Supplier to process data subject to data protection regulations, Supplier agrees it will comply with the terms and conditions included in this Attachment E.

E.1. BACKGROUND AND PURPOSES

E.1.1. Certain services provided by Service Provider involve the processing of personal data about the MFA's employees, patients or affiliates.

E.1.2. The processing of personal data by the MFA is subject to various data protection and privacy legal, regulatory, and contractual requirements (collectively "**Applicable Data Protection Requirements**"), including without limitation under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("**EU General Data Protection Regulation**"); Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009; the Standard Contractual Clauses set out by the EU Commission Decision of 5 February 2010 (2010/87/EU) and the EU Commission Decision of 27 December 2004 (2004/915/EC) (collectively, the "**EU Standard Contractual Clauses**"); and any applicable European Union or Member State law relating to data protection or the privacy of individuals.

E.1.3. Pursuant to its obligations under Applicable Data Protection Requirements, the MFA is required to impose data protection obligations upon Service Providers that process personal data that originates from within the European Economic Area or is otherwise subject to Applicable Data Protection Requirements ("**Flowdown Requirements**").

E.2. General

E.2.1 In the event of any conflict or inconsistency between the terms of the Standard Purchase Order Terms and Conditions, the following order of precedence shall govern, from highest to lowest: (i) this Attachment E, (ii) Attachment C (if applicable), and (iii) the Standard Purchase Order Terms and Conditions.

E.3. Data Protection

E.3.1 For the purposes of this Clause 3, the terms, "**controller**", "**data subject**", "**personal data**", "**personal data breach**", "**processor**" and "**process**" will have the meaning given to them by the EU General Data Protection Regulation. "**EEA**" means the European Economic Area, Switzerland and, after the United Kingdom ("UK") leaves the European Union, the UK. "**C-to-P Transfer Clauses**" means the EU Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries approved by European Commission Decision of February 5, 2010, as included in Schedule 1 to this Attachment E.

E.3.2 For the purposes of providing the services to the MFA, Service Provider may have access to, or be provided with personal data that is subject to Applicable Data Protection Requirements ("**European Personal Data**") and in relation to which the MFA is subject to certain obligations. This Clause 3 assists the MFA in complying with its obligations when providing or allowing access to European Personal Data by Service Provider.

E.3.3 The subject-matter of the data processing is the provision of the services, and the processing will be carried out for the duration of the Purchase Order. Appendix 1 of Schedule 1 of this Attachment E sets out the nature and purpose of the processing, the types of European Personal Data Service Provider processes on the MFA's behalf and the categories of data subjects whose personal data is processed.

E.3.4 Each Party undertakes to comply with all Applicable Data Protection Requirements applicable to it and will not knowingly cause the other to breach Applicable Data Protection Requirements.

E.3.5 The MFA will be the controller and Service Provider will be the processor regarding the European Personal Data processed by Service Provider on the MFA's behalf under the Purchase Order.

E.3.6 Service Provider will, and will ensure that any of its employees or agents will, only process European Personal Data in accordance with the Purchase Order, this Attachment E, and documented instructions received from the MFA. If Service Provider is legally required by European Union or European Member State law to process European Personal Data otherwise than as instructed by the MFA, it will notify the MFA before such processing occurs, unless the law requiring such processing prohibits Service Provider from notifying the MFA on an important ground of public interest, in which case it will notify the MFA as soon as that law permits it to do so.

E.3.7 Service Provider will implement appropriate technical and organizational security measures to ensure a level of security appropriate to the risks that are presented by the processing and the nature of the European Personal Data to be protected, and at minimum in compliance with Appendix 2 of Schedule 1 of this Attachment E. If Service Provider receives notice regarding any violation of Applicable Data Protection Requirements, has reason to believe such notice will be received or has reason to believe that the security of any records containing European Personal Data that Service Provider maintains has been breached or potentially breached, Service Provider shall immediately provide notice and additional requested information to the MFA regarding such notice or knowledge.

E.3.8 Service Provider will ensure that its personnel who have access to European Personal Data are both (1) informed of the confidential nature of the European Personal Data and obliged to keep such European Personal Data confidential including, if applicable, as set forth in Attachment C; and (2) aware of Service Provider's duties and their personal duties and obligations under the Purchase Order and this Attachment E.

E.3.9 Service Provider will use commercially reasonable efforts to: (1) assist the MFA with the fulfillment of the MFA's obligation to respond to requests for exercising the data subject's rights as set out in Applicable Data Protection Requirements; (2) assist the MFA in ensuring compliance with Applicable Data Protection Requirements, including obligations to investigate, remediate and provide information to regulators or data subjects about personal data breaches without undue delay, to carry out privacy impact assessments and to consult with regulators regarding processing which is the subject of a privacy impact assessment; (3) make available all information necessary to demonstrate compliance with Applicable Data Protection Requirements; (4) allow for and contribute to audits including, if applicable, as set forth in Section C.12 of Attachment C, including inspections and information requests, conducted by the MFA or an auditor mandated by the MFA. Service Provider will promptly notify the MFA about any instruction from the MFA that, in its opinion, infringes Applicable Data Protection Requirements.

E.3.10 Upon termination, cancellation, expiration or other conclusion of the Purchase Order, Service Provider shall return to the MFA or, if return is not feasible, destroy all European Personal Data in whatever form or medium that Service Provider received from or created on behalf of the MFA. This provision shall also apply to all European Personal Data that is in the possession of subcontractors or agents of Service Provider. In such case, Service Provider shall retain no copies of such information, including any compilations derived from and allowing identification of European Personal Data. Unless otherwise requested in writing by the MFA, Service Provider shall complete such return or destruction as promptly as possible, but not more than thirty (30) days after the effective date of the conclusion of this Agreement. Service Provider agrees to return or destroy such European Personal Data within seven (7) days of a request in writing by the MFA. Within the thirty (30) day period following termination or written request, Service Provider shall certify in writing to the MFA that such return or destruction has been completed. Written confirmation of the destruction of data in Service Providers possession or on Service Provider computer systems should include standards used for the destruction; such standards should meet National Institute of Standards, Guidelines for Media Sanitization, see http://csrc.nist.gov/. If Service Provider believes that the return or destruction of European Personal Data is not feasible, Service Provider shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction is not feasible, Service Provider shall extend the protections of this Attachment E to European Personal Data received from or created on behalf of the MFA, and limit further uses and disclosures of such European Personal Data, for so long as Service Provider maintains the European Personal Data.

E.3.11 Service Provider will not subcontract any of its processing operations under the Purchase Order unless (1) it has obtained the prior written consent of the MFA to do so; and (2) the subcontractor is subject to a written agreement which imposes the same obligations on that subcontractor as are imposed on Service Provider under the Purchase Order and this Attachment E. Service

Provider will remain fully liable to the MFA for any subcontractors' processing of European Personal Data under the Purchase Order and this Attachment E.

E.3.12 To the extent that the provision of the services under the Purchase Order involves the transfer of European Personal Data outside the EEA (either directly or via onward transfer) to any country or recipient which has not been recognised by the European Commission as offering an adequate level of protection for personal data transferred to it from the EEA, Service Provider agrees:

E.3.12.a. to comply with the C-to-P Transfer Clauses whereby the MFA will be regarded as the data exporter and Service Provider will be regarded as the data importer; or

E.3.12.b. that where Service Provider has provided the MFA with a current and valid Privacy Shield certification it warrants that it will maintain an active and valid certification with the EU-U.S. Privacy Shield Framework ("**Privacy Shield**"), and will process the European Personal Data in accordance with both that certification and the Privacy Shield Principles.

E.3.13 To the extent that any sub-processor engaged by Service Provider in accordance with Clause E.3.11 is located in a country outside the EEA which has not been recognised by the European Commission as offering an adequate level of protection for Personal Data transferred to it from the EEA, Service Provider will assist the MFA to adduce an adequate level of protection for the Personal Data as required by Applicable Data Protection Requirements by entering into the C-to-P Transfer Clauses with the sub-contractor on the MFA's behalf whereby the sub-processor will be regarded as the data importer and Service Provider will act as agent for the MFA as the data exporter. For the purposes of this Clause E.3.13, the MFA hereby appoints Service Provider as its agent to enter into the C-to-P Transfer Clauses with the sub-processor on the MFA's behalf.

E.3.14 For the purposes of the C-to-P Transfer Clauses, the following additional provisions shall apply:

E.3.14.a. The acceptance of the Terms and Conditions of this Purchase Order shall be considered as acceptance of the C-to-P Transfer Clauses;

E.3.14.b. Service Provider agrees to observe the terms of the C-to-P Transfer Clauses without modification;

E.3.14.c. the governing law in clause 9 of the C-to-P Transfer Clauses shall be the law of the MFA (as Data Exporter) unless the MFA is located outside the EEA in which case the governing law is the EEA Member State from which the data is transferred;

E.3.14.d. if so required by the laws or regulatory procedures of any jurisdiction, the Parties shall execute or re-execute the C-to-P Transfer Clauses as separate documents setting out the proposed transfers of Personal Data in such manner as may be required; and

E.3.14.e. in the event of inconsistencies between the provisions of the C-to-P Transfer Clauses and the Purchase Order as regards the services provided under the Purchase Order, the C-to-P Transfer Clauses shall take precedence. The terms of the Purchase Order or this Attachment E shall not vary the C-to-P Transfer Clauses in any way.

E.3.15 In the event that the C-to-P Transfer Clauses or Privacy Shield are amended, replaced or repealed by the European Commission or under Applicable Data Protection Requirements, the Parties shall work together in good faith to enter into any updated version of the C-to-P Transfer Clauses or negotiate in good faith a solution to enable a transfer of European Personal Data to be conducted in compliance with Applicable Data Protection Requirements.

E.3.16 The MFA shall be entitled, at no cost to itself, to suspend, or require Service Provider to suspend, any transfers of European Personal Data which do not comply or which cease to comply with the provisions of Clauses E.3.12 to E.3.15.

E.3.17 Service Provider agrees to indemnify and keep indemnified and defend at its own expense the MFA against all costs, claims, damages or expenses incurred by the MFA or for which the MFA may become liable due to any failure by Service Provider or its employees, agents or subcontractors to comply with any of its obligations under this Clause E.3.

E.3.18 Each party shall perform its obligations under this Clause E.3 at its own cost.

Schedule 1 to Attachment E: Standard Contractual Clauses (processors)

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 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 his behalf after the transfer in accordance with his 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 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 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.

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
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 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 the 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 under the Clauses; and

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

Clause 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 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 deposit 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 Clauses. 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 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.
2. The data importer and the subprocessor 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.

APPENDIX 1 TO SCHEDULE 1 (THE STANDARD CONTRACTUAL CLAUSES) OF ATTACHMENT E

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):

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

Data subjects

The European Personal Data concerns the following categories of data subjects (please specify):

Categories of data

The European Personal Data concerns the following categories of data (please specify):

Special categories of data (if appropriate)

The European Personal Data concerns the following special categories of data (please specify):

Processing operations

The European Personal Data will be subject to the following basic processing activities (please specify):

Duration

The European Personal Data will be processed by Service Provider for the duration of the services provided under the Purchase Order.

APPENDIX 2 TO SCHEDULE 1(THE STANDARD CONTRACTUAL CLAUSES) OF ATTACHMENT E

This Appendix shall contain a description of the technical and organisational security measures implemented by the data importer or Service Provider in accordance with Clauses 4(d) and 5(c), if applicable (or document/legislation attached):

1. Safeguard Standard for European Personal Data. Service Provider agrees that it will protect the European Personal Data it receives from or on behalf of GW according to commercially acceptable standards and no less rigorously than it protects its own confidential information. The following sources provide some generally recognized industry standards for the protection of confidential information. These sources are not intended to be comprehensive or exhaustive of all possible generally recognized industry standards:

a. Center for Internet Security - see http://www.cisecurity.org

b. Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org/

c. National Institute for Standards and Technology - see http://csrc.nist.gov

d. ISO/IEC 27000-series - see http://www.iso27001security.com/

2. Maintenance of the Security of Electronic Information. Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity, and availability of all electronically maintained or transmitted European Personal Data received from, or on behalf of, GW.

2.1 Network Security. Service Provider agrees at all times to maintain network security that, at a minimum, includes: network firewall provisioning, intrusion detection, and regular (at least annual) third party vulnerability assessments. Likewise, Service Provider agrees to maintain network security that conforms to generally recognized industry standards (as described in Clause 1 of this Appendix) and best practices that Service Provider then applies to its own network.

2.2 Application and System Security. Service Provider agrees at all times to provide, maintain and support its software release and subsequent updates, upgrades, and bug fixes such that the software is, and remains secure from those vulnerabilities using applicable and recognized industry practices or standards including:

a. The Open Web Application Security Project's (OWASP) "Top Ten Project" - see http://www.owasp.org;

b. The CWE/SANS Top 25 Programming Errors – see http://cwe.mitre.org/top25/ or http://www.sans.org/top25-programming-errors/; or

c. Other generally recognized and comparable industry practices or standards.

Additionally, Service Provider agrees to maintain a secure processing environment, includes but is not limited to the timely application of patches, fixes and updates to operating systems and applications as provided by Service Provider or open source support.

2.3 Data Security. Service Provider agrees to use administrative, technical, and physical measures that conform to generally recognized industry standards and best practices (as described in Clause 1 of this Appendix) and which are at least as secure as those that Service Provider applies to protect its own processing environment and confidential information.

2.4 Data Storage. Service Provider agrees that all European Personal Data will be stored, processed, and maintained solely on designated target servers. Additionally Service Provider agrees that no European Personal Data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that device or storage medium is in use as part of the Service Provider's designated backup and recovery processes and encrypted in accordance with Subsection 2.6 regarding data encryption. Service Provider agrees not to store European Personal Data outside of the EEA or United States without prior written consent from GW.

2.5 Data Transmission. Service Provider agrees that any and all electronic transmission or exchange of system and application data with GW and/or any other third parties when such third-party exchanges have been approved in writing by GW shall take place via secure means (using HTTPS or SFTP or equivalent) and solely in accordance with Subsection 2.7 regarding data re-use.

2.6 Data Encryption. Service Provider agrees to store all Regulated Information and any backup of that information as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Service Provider further agrees that any and all European Personal Data, as defined herein or under applicable legislation or regulations, stored on any portable or laptop computing device or any portable storage medium is likewise encrypted.

2.7 Data Re-Use; Protection of European Personal Data. Service Provider agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the Purchase Order and this Attachment E. European Personal Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Service Provider. Service Provider further agrees that no European Personal Data of any kind shall be transmitted, exchanged, or otherwise passed to other subcontractorsor interested parties except on a case-by-case basis as specifically agreed to in writing by GW.

2.8 Malicious Code. Service Provider represents and warrants that in performance of its services, Service Provider will not knowingly introduce into GW's systems any viruses, Trojan horses, worms, time bombs, locks, backdoors, counters, timers, spyware or other malware or any other computer programming devises that may damage GW's systems or data or prevent GW from operation or use of its systems, data or the like.