

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

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: General Electric Company on behalf of itself and its Affiliates and Subsidiaries located within the territory of Switzerland and the European Economic Area (EEA) member states, including such Affiliates and Entities that may be added during the term of this Agreement.

Address: 3135 Easton Turnpike, Fairfield, Connecticut, U.S.A.

Tel:.....e-mail:

.....
(the data **exporter**)

And

Name of the data importing organisation: [VENDOR NAME] on behalf of itself and its Affiliates and Subsidiaries.

Address: [VENDOR ADDRESS]

Tel: [VENDOR TELEPHONE]e-mail: [VENDOR EMAIL]

.....
(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 the 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 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 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 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 and which will be identified by the data exporter in the the Statement of Work that is executed engaging the data importer for a particular matter. The Member State may include one or more of the following for a particular engagement, namely the territory of Switzerland and the European Economic Area (EEA) member states.

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, namely located within the territory of Switzerland and the European Economic Area (EEA) member states.
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.

Clause 13

Additional terms to address subprocessing obligations imposed on the data exporter by Clause 11 of the standard contractual clauses for the transfer of personal data to processors established in third countries under Commission Decision 2010/87/EU ("SCC")

The data importer acknowledges that certain personal data transferred by the data exporter to it may originate from other third-party controllers, and have been transferred to the data exporter for processing under the terms of another set of SCC. In that scenario, the parties agree the data exporter acts as a "data importer" and data importer acts as a "subprocessor". The additional terms below ("**Additional Terms**") are intended to meet the requirement to subcontract data importer obligations under the SCC 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 SCC.

1. For the purposes of these Additional Terms, Section 1 ("Definitions") of the Clauses apply except for the definition of data exporter which is amended as follows:

"the data exporter" means the third-party controller from whom the personal data originates.
2. For the purposes of these Additional Terms, the "subprocessor" will be the legal entity identified as "data importer" in the heading of the Clauses, and the "data importer" will be the legal entity identified as "data exporter" in the heading of the Clauses.
3. The subprocessor agrees to comply with all obligations under Section 5 (Obligations of the data importer) above.
4. The subprocessor agrees that data subjects will be able to bring action against it in 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.
5. The provisions relating to data protection aspects of these Additional Terms shall be governed by the law of the Member State in which the data exporter is established.
6. Appendices 1 and 2 to the Clauses remain applicable to these Additional Terms.

On behalf of the data exporter:

Name (written out in full): _____

Position: _____

Address: 3135 Easton Turnpike, Fairfield, CT, U.S.A.

Signature:

On behalf of the data importer:

Name (written out in full): _____

Position: _____

Address: _____

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):

.....
.....
.....
.....

Data importer

The data importer is (please specify briefly 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

Name:.....

Authorised Signature

DATA IMPORTER

Name:.....

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):

This Appendix governs whenever a Supplier Processes GE Data or has access to a GE Information System in connection with the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of services and/or deliverables by Supplier to GE (Contract Document). In the event of any inconsistency or conflict between this Appendix and the Contract Document with respect to a subject covered by this Appendix, the provision requiring the higher level of protection for GE Data shall prevail. The requirements in this Appendix are in addition to any confidentiality obligations between GE and the Supplier under the Contract Document. GE or the applicable GE Affiliate owning any of the GE Data being accessed pursuant to the Contract Document may enforce the terms of this Appendix.

Part A: Definitions

Any words following the terms "including," "include," "e.g.," "for example" or any similar expression are for illustration purposes only.

(i) *Controlled Data* is technical or government information with distribution and/or handling requirements proscribed by law, including but not limited to controlled unclassified information and license required export controlled data. Controlled Data shall be subject to the controls below for GE Restricted Data.

(ii) *GE* means the General Electric Company or a General Electric Company affiliate signing the Contract Document with Supplier.

(iii) *GE Data* is any GE Confidential Information as defined in the Contract Document Processed in connection with performance of the Contract Document. Personal Data, Sensitive Personal Data, Controlled Data and GE Restricted Data are GE Data.

(iv) *GE Information System(s)* means any systems and/or computers managed by GE, which includes laptops and network devices.

(v) *GE Restricted Data* is information that GE identifies as 'restricted data' in the Contract Document, or that GE identifies as "Restricted," "Highly Confidential," or similar at the time of disclosure.

(vi) *Highly Privileged Accounts, or HPAs*, are accounts with system level administrative or super-user access to devices, applications or databases, administration of accounts and passwords on a system, or ability to override system or application controls.

(vii) *Mobile Devices* means tablets, smartphones and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

(viii) *Personal Data* includes any information that relates to an identified or identifiable natural person (Data Subject), as defined under applicable law. Legal entities are Data Subjects where required by law.

(ix) *Process(ing)* means to perform any operation or set of operations upon GE Data, whether or not by automatic means, including but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying.

(x) *Security Incident* is any event in which GE Data is or is suspected to have been lost, stolen, improperly altered, improperly destroyed, used for a purpose not permitted under the Contract

Document or this Appendix, or accessed by any person other than Supplier Personnel pursuant to the Contract Document or this Appendix.

(xi) *Security Notices* are any written communications, notices, filings, press releases, or reports related to any Security Incident.

(xii) *Sensitive Personal Data* is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information (PHI), as defined in and subject to the U.S. Health Insurance Portability and Accountability Act of 1996; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special data categories of data under applicable data protection law (such as race, nationality, political opinions, trade union membership, home life, and sexual orientation). Sensitive Personal Data shall be subject to the controls specified below for GE Restricted Data.

(xiii) *Supplier* is the entity that is providing goods or services to GE pursuant to the Contract Document.

(xiv) *Supplier Information System(s)* means any Supplier systems and/or computers used to Process GE Data pursuant to the Contract Document, which includes laptops and network devices.

(xv) *Supplier Personnel* means all persons or entities providing services and/or deliverables under the Contract Document, including Supplier's employees, permitted affiliates, suppliers, contractors, subcontractors and agents, as well as anyone directly or indirectly employed or retained by any of them.

Parts B-E and H-J apply to all Suppliers that Process any GE Data.

Part B: Collecting, Processing and Sharing GE Data

Supplier shall implement appropriate organizational, technical, and physical measures and controls to ensure the security and confidentiality of GE Data and to prevent accidental, unauthorized or unlawful destruction, alteration, unauthorized disclosure or access, modification or loss; misuse; or unlawful Processing of GE Data. Supplier is responsible for compliance with this Appendix by all Supplier Personnel.

Organizational security controls:

1. Supplier and Supplier Personnel shall Process GE Data, and access and use GE Information Systems, only on a need-to-know basis and to the extent necessary to perform services under the Contract Document or as otherwise instructed by GE in writing.
2. Prior to providing access to any GE Data to any Supplier Personnel, Supplier must obligate them to comply with the applicable requirements of the Contract Document and this Appendix. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier Personnel.
3. Supplier must maintain and comply with written information security policies and procedures consistent with the requirements of this Appendix.
4. Supplier Personnel with access to GE Data must participate in appropriate information security awareness training prior to obtaining access to GE Data and annually thereafter.
5. Supplier shall maintain a current inventory of all hardware and software used to Process GE Data.
6. Supplier must ensure each account through which GE Data may be accessed is attributable to a single individual with a unique ID (not shared) and each account must require authentication (e.g., password) prior to accessing GE Data.
7. Supplier shall undertake reasonable measures to terminate Supplier Personnel's physical and logical access to GE Data no later than the date of separation or transfer to a role no longer requiring access to GE Data. Supplier shall notify GE of any separation or transfer of Supplier Personnel with GE SSO credentials no later than the day of that event.

8. GE Data shall not be Processed on personal accounts (e.g., individual email or cloud services accounts) or on personally-owned computers, devices or media.
9. Unless prohibited by law, Supplier shall notify GE promptly and act only upon GE's instruction concerning any request by a third party for disclosure of GE Data or for information concerning Supplier's Processing of GE Data, as well as any request received from an individual concerning his/her Personal Data.

Technical security controls on Supplier Information Systems:

10. Supplier must use strong passwords, including requirements for minimum password length, lockout, expiration period, complexity, encryption, changing of default passwords, and usage of temporary passwords. User account credentials (e.g., login ID, password) must not be shared.
11. Supplier Information Systems must have security controls that can detect and prevent attacks by use of network layer firewalls and intrusion detection/prevention systems (IDS/IPS) in a risk based manner, client and server-side antivirus programs that include up-to-date antivirus definitions, and installation into production of all critical patches or security updates within thirty (30) days from the release of any such updates or patches. Supplier must implement documented change management procedures that provide a consistent approach for controlling, implementing and documenting changes (including emergency changes) for Supplier Information Systems that includes appropriate segregation of duties.
12. Unless otherwise expressly agreed in the Contract Document, development and testing environments must be physically and/or logically separated from production environments and must not contain GE Data. Production changes must be approved by the Supplier's appropriate system owner, and include appropriate segregation of duties.
13. Any back-up media containing GE Data stored at Supplier's site must be kept in a secure location with restricted physical access and be encrypted if technically feasible. If off-site media storage is used, Supplier must have a media check-in/check-out process with locked storage for transportation.
14. An inactivity lock must be implemented on workstations when left unattended and a password or PIN must be required to enable access. Network layer security devices must allow only authorized connections, and rule sets must be reviewed.
15. Mobile Devices used to Process GE Data (including emails) must have centrally-managed security controls, including required passcode, minimum passcode length, inactivity lock, and a process in place to immediately remotely wipe lost or stolen devices.

Physical security controls shall include the following on all Supplier facilities where GE Data may be Processed:

16. Access to all Supplier locations where GE Data is Processed must be limited to Supplier Personnel and authorized visitors. Reception areas must be manned or have other means to control physical access.
17. Visitors at Supplier locations where GE Data is Processed must be required to sign a visitors register and wear an identification badge. For data centers or similar facilities, visitors must be escorted or observed at all times.
18. Documents that contain GE Data must be kept secured (e.g. locked office or file cabinet) when not in use.

Part C: Security Incidents

1. Security Incidents on Suppliers Information Systems must be logged and reviewed quarterly, secured, and maintained for a minimum of twelve (12) months.
2. Supplier must implement an up-to-date incident management plan designed to promptly identify, prevent, investigate, and mitigate any Security Incidents and must perform any required recovery actions to remedy the impact.

3. Supplier shall notify GE within seventy-two (72) hours after discovery, or shorter if required by applicable law, of any Security Incident experienced by Supplier. Supplier shall report Security Incidents to GE's Cyber Incident Response Team at gecirt@ge.com or 1-800-4GE-CIRT, or at such contact information communicated to Supplier from time to time. Supplier shall cooperate with GE in its investigation of an incident, and provide GE a detailed description of the Security Incident, the type of data that was the subject of the Security Incident, the identity of each affected person, and any other information GE reasonably requests, as soon as such information can be collected or otherwise becomes available.
4. If requested by GE, and at GE's direction, Supplier shall send Security Notices regarding a Security Incident. Unless prohibited by law, Supplier shall provide GE reasonable notice of, and the opportunity to comment on and approve, the content of such Security Notices prior to publication or communication to any third party, except GE shall not have the right to reject content in a Security Notice that must be included in order to comply with applicable law. Should GE elect to send a Security Notice regarding a Security Incident, Supplier shall provide reasonable and timely information relating to the content and distribution of that Security Notice as permitted by applicable law or regulation pursuant to the Security Notice.
5. Other than approved Security Notices, or to law enforcement or as otherwise required by law, Supplier may not make or permit any public statements concerning GE's involvement with a Security Incident to any third-party without explicit written authorization of GE's Legal Department.

Part D: Audits

Supplier responsibilities:

1. Supplier must conduct periodic security risk assessments of Supplier Information Systems to identify critical information assets, assess threats, and determine potential vulnerabilities.
2. Upon request, Supplier must provide GE an executive summary of any audits and assessments conducted on Supplier Information Systems, including the scope of the audit and/or assessment and any vulnerabilities and corrective actions.
3. Supplier must use commercially reasonable efforts to remediate within thirty (30) days any items rated as high or critical (or similar rating) in any audits or assessments of Supplier Information Systems.
4. Supplier agrees to cooperate fully with GE or its designee during audits (below) and shall provide access to facilities, appropriate resources, and supporting documentation and complete security assessment questionnaires as requested.

GE audit rights:

5. GE reserves the right to conduct an audit, upon 30 days advance notice, of Supplier's compliance with the requirements in this Appendix, including but not limited to: (i) review of Supplier's applicable policies, processes, and procedures, (ii) review of the results of Supplier's most recent vulnerability assessment and accompanying remediation plans, and (iii) on-site assessments during regular business hours of Supplier's physical security arrangements and Supplier Information Systems. GE reserves the right to conduct an Applications Vulnerability Assessment if Supplier's vulnerability assessments do not meet or exceed GE application security requirements. This right shall survive termination or expiration of the Contract Document so long as Supplier Processes GE Data.
6. Subject to the confidentiality provisions of the Contract Document, GE or its representative may review, audit, monitor, intercept, access and, disclose any information provided by Supplier that is Processed or stored on GE Information Systems or on GE Mobile Devices accessing the GE network.

Part E: Regulatory Requirements

In the event Supplier Processes GE Data that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Supplier agrees to cooperate with GE for GE's compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g., EU Standard Contractual Clauses, U.S. Protected Health Information Agreement), implementation of additional security controls required by applicable law, completion of regulatory filings applicable to Supplier, and participation in regulatory audits, subject to the terms of Part D above.

Part F applies to any Supplier that Processes Personal Data (including Sensitive Personal Data)

Part F: Personal Data

1. Supplier shall comply with all laws applicable to Supplier's activities concerning Personal Data governed by this Appendix, including those concerning notice and consent, onward transfer to a third party, and international transfer, and shall act only on GE's written instruction concerning any such transfers. Supplier must receive approval from GE prior to (i) moving Personal Data from its GE-approved hosting jurisdiction to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than the hosting jurisdiction or other GE-approved jurisdiction.
2. Any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) containing Personal Data must be encrypted at rest. Encryption also must be employed when transferring Personal Data over public networks/Internet. Supplier must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.
3. Unless and except to the extent expressly provided in the Contract Document, Supplier must seek and obtain GE's prior written approval regarding the scope of any Personal Data to be collected directly by Supplier, as well as any notices to be provided and any consent language to be used when collecting such information from a Data Subject. In the case of Personal Data collected directly from Data Subjects by Supplier, Supplier shall comply with applicable data privacy laws and regulations, including those concerning notice, consent, access and correction/deletion.

Part G applies to Suppliers that Process Sensitive Personal Data, Controlled Data, and/or GE Restricted Data. The requirements of this Part G are in addition to requirements of Parts A through F above. References to GE Restricted Data in this Part G shall be deemed to also refer to Sensitive Personal Data and/or Controlled Data as the context requires.

Part G: Protecting GE Restricted Data, Controlled Data, and Sensitive Personal Data

1. Supplier must have a formal information security program with clearly defined information security roles, responsibilities and accountability.
2. Supplier must perform or have an independent third party perform vulnerability assessments on Supplier Information Systems annually and remediate as required in Part D.3.
3. Any Supplier Personnel accessing Supplier's internal or hosted network remotely must be authenticated using two-factor authentication method and such transmissions must be encrypted at a level consistent with industry standards.
4. Supplier must implement a device hardening and configuration standard.
5. Supplier must implement appropriate data loss prevention (DLP) controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of GE Restricted Data from Supplier Information Systems.
6. Supplier must implement processes to support the secure creation, modification, and deletion of HPAs. Supplier must review and update HPA access rights quarterly. HPA usage must be reviewed weekly. All HPA access must be established using encrypted mechanisms (e.g., secure shell).

7. Supplier must dispose of paper records containing GE Restricted Data, and remove GE Restricted Data from Supplier Information Systems, in an auditable manner that ensures that the GE Restricted Data may not be accessed or readable.
8. Encryption must be implemented in the following instances: (i) any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) containing GE Restricted Data must be encrypted at rest; (ii) where technically feasible, GE Restricted Data must be stored in encrypted form, except where encryption is mandatory in such cases as set forth above; and/or (iii) transferring GE Restricted Data over public networks (such as the Internet).
9. Where encryption is required, Supplier must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.
10. Supplier Information Systems consisting of servers and/or network equipment used to store or access GE Restricted Data must be kept in a secure room with enhanced logical and physical access control, and located on the interior of the building with no windows unless safeguards are in place to prevent shattering and unauthorized entry.
11. Physical access must be monitored, recorded and controlled with physical access rights reviewed annually. Physical access logs detailing access must be stored for six (6) months unless prohibited by local law. If not staffed 24x7, alarms and entry point security cameras must be installed for off-hours access monitoring with recordings retained for at least thirty (30) days.
12. Supplier must receive approval from GE prior to moving GE Restricted Data from its GE-approved physical location or jurisdiction to a different physical location or jurisdiction.

Unless otherwise provided for in the Contract Document, Part H applies to any Supplier Information System(s) (i) that Processes GE Restricted Data, Controlled Data, and/or Sensitive Personal Data, and/or (ii) where an outage of the Supplier Information System(s), as identified in the Contract Document, is likely to significantly adversely impact GE or overall GE operations, financial position, regulatory compliance, and/or reputation.

Part H: Disaster Recovery

Unless a disaster recovery (DR) program is otherwise set forth in more detail elsewhere in the Contract Document, Supplier must maintain a DR program for all Supplier Information Systems and facilities used to provide services under the Contract Document to GE. The DR program must be designed to ensure that Supplier has a methodology by which a system can continue to function through an operational interruption or disaster. The DR program shall include the following elements:

1. Supplier's operational procedures must verify the successful completion of backups and the backup media must be tested regularly (at minimum semi-annually) to ensure it will operate in the event of an emergency.
2. For rooms containing Supplier Information Systems consisting of servers and/or network equipment used to provide services to GE, controls must be implemented to mitigate the risk of power failures, and environmental conditions.
3. DR plans must be implemented for all Supplier Information Systems and facilities that are used to provide services to GE.
4. Supplier must conduct full scale DR tests annually for Supplier Information Systems that are used to provide services to GE to ensure that such Supplier Information Systems can be recovered in a manner that meets the contractual service levels specified in the Contract Document. DR results must be documented and provided to GE upon request.

Part I: Termination

1. Supplier shall within 30 (thirty) days of termination of the Contract Document, or if requested during the term of the Contract Document, cease all Processing of GE Data and return to GE all copies of GE Data. In lieu of returning copies, GE may, at its sole discretion, require Supplier to destroy all copies of GE Data, using agreed upon methods to ensure such GE Data is not recoverable, and certify to such destruction.

2. Supplier may continue to retain GE Data beyond the period prescribed in Part I.1 where required by law, provided that (i) Supplier notifies GE prior to the Contract Document's termination or expiration of the obligation, including the specific reasons for such retention; (ii) Supplier has a documented retention period and secure deletion procedure for such copies, with back-up copies retained no longer than 6 (six) months from the date on which they were captured, and legally required copies retained only to the end of their legally required retention period; (iii) following such period, all copies and back-up copies are deleted in such a manner that they are not recoverable; (iv) Supplier performs no Processing of GE Data other than that necessitated by retaining or deleting the relevant copies; and (v) Supplier continues to comply with all the requirements of this Appendix in relation to any such retained GE Data until the same is securely deleted.
3. Termination or expiration of the Contract Document, for any reason, shall not relieve the Supplier from obligations to continue to protect GE Data against the impermissible disclosure in accordance with the terms of the Contract Document and this Appendix.

Part J: Miscellaneous

GE may require Supplier to provide certain personal information such as the name, address, telephone number, and e-mail address of Supplier's representatives to facilitate the performance of the Contract Document, and GE and its contractors may store such data in databases located and accessible globally by their personnel and use it for necessary purposes in connection with the performance of the Contract Document, including but not limited to Supplier payment administration. GE will be the Controller of this data for legal purposes, and agrees to use reasonable technical and organizational measures to ensure that such information is processed in conformity with applicable data protection laws. Supplier may obtain a copy of the Supplier personal information by written request, or submit updates and corrections by written notice to GE. GE will comply at all times with the privacy policy posted on its web site.

DATA EXPORTER

Name: _____

Authorised Signature:

DATA IMPORTER

Name: _____

Authorised Signature: