PRIVACY AND DATA PROTECTION APPENDIX
1 Oct 2020

This Appendix applies in the circumstances set out below. In the event of 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 any Personal Data or other GE information governed by this Appendix 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 responsible for the protection of any of the Personal Data or other GE information governed by this Appendix may enforce the terms of this Appendix. This Appendix is also applicable when a Supplier affiliate is providing goods, services and/or deliverables under the Contract Document directly, in its own name, in which event Supplier's agreement to the terms of this Appendix is also given on behalf of such Supplier affiliate; and Supplier warrants that it has the power and authority to do so. As used herein, "Supplier" shall mean Supplier and Supplier affiliate, collectively.

SECTION I – DEFINITIONS

The following definitions and rules of interpretation apply in this Appendix. Any words following the terms "including," "include," "e.g.,", "for example" or any similar expression are for illustration purposes only.

(i) ***Contract Document*** means the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of goods, services and/or deliverables by Supplier to GE.

(ii) ***Controlled Data*** is technical or government information with distribution and/or handling requirements proscribed by law or regulation, including but not limited to controlled unclassified information and license required export-controlled data, which is provided by GE to the Third Party or created by the Third Party in connection with performance of the Contract Document.

(iii) ***Beneficial Use of Data*** is the use of data in a lawful manner to gain profit, advantage or enjoyment from it.

(iv) ***Data Controller*** means the natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data.

(v) ***Data Processor*** means the natural or legal person, public authority, agency or other body, which processes personal data on behalf of the data controller.

(vi) ***Data Subject*** means an identified or identifiable natural person.

(vii) ***GE*** means the General Electric Company or a GE Affiliate party to the Contract Document with Supplier.

(viii) ***GE Affiliate*** means any entity that is directly or indirectly in control of, controlled by, or under common control with GE, whether now existing, or subsequently created or acquired during the term of the Contract Document.

(ix) ***GE Confidential Information*** is information created, collected, or modified by GE that would pose a risk of causing harm to GE if disclosed or used improperly, and is provided and identified as such to the Supplier under the Contract Document. GE Confidential Information includes but is not limited to Highly Confidential, Personal Data from any jurisdiction, Controlled, or Sensitive Personal Data.

(x) ***GE Highly Confidential Information*** is GE Confidential Information that GE identifies as "highly confidential" in the Contract Document, or that GE identifies as "Restricted," "Highly Confidential," or similar at the time of disclosure.

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

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

(xiii) ***Omnibus Privacy Law*** means a comprehensive national privacy law that defines and recognizes parties as Data Controllers and Data Processors (or applies similar concepts with different names, for instance the GDPR or LGPD).

(xiv) ***Personal Data*** means any information related to an identified or identifiable natural person (Data Subject) in or from any jurisdiction, as defined under applicable laws, which is Processed in connection with the Contract Document. Legal entities are Data Subjects where required by law. Personal Data is, at a minimum, GE Confidential Information.

(xv) ***Process(ing)*** means to perform any operation or set of operations upon GE Confidential Information, 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.

(xvi) ***Security Incident*** means any event in which GE Confidential Information 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.

(xvii) ***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 and Portability Act of 1996 where applicable; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special categories of data under applicable law (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, home life and sexual orientation). In some jurisdictions "Sensitive Personal Information or Data" is a defined term. Where any law or regulations applying such jurisdictional definition apply, the term 'Sensitive Personal Data' as defined herein is intended to include, without limitation, all data or information falling within such jurisdictional definition.

(xviii) ***Supplier*** is the entity providing goods, services and/or deliverables to GE pursuant to the Contract Document. Supplier may also be referred to as Third Party.

(xix) ***Supplier Information System(s)*** means any Supplier system(s) and/or computer(s) used to Process, store, transmit and/or access GE Confidential Information pursuant to the Contract Document, which includes laptops and network devices.

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

(xxi) ***Trusted Third Party Network Connection*** is a physically isolated segment of the Third-Party network connected to GE internal network in a manner identical to a standard GE office.

SECTION II – INFORMATION SECURITY REQUIREMENTS*. This Section II applies whenever a Supplier and/or Supplier Personnel Processes GE Confidential Information, has access to a GE Information System in connection with the Contract Document, or provides certain services to GE. The only exception is where the GE Confidential Information a Supplier Processes is limited to Personal Data, and where for purposes of this Appendix, both GE and Supplier are independent Data Controllers; in such circumstances, only the provisions of Section I and Section III(B)(2) shall apply to the Personal Data Processed by the Supplier. For the purposes of clarification, this Section II shall apply to any non-personal GE Confidential Information Processed by the Supplier/Data Controller, such as technical or business financial information. Capitalized terms used in this Section II and not defined in this Appendix shall have the meaning given to them in the GE Third Party Information Security Requirements referenced herein.*

Part A: Security Controls

Supplier shall comply with the GE Third Party Information Security Requirements (available at http://www.gesupplier.com/html/GEPolicies.htm), as applicable to the service, products and/or deliverables provided by the Supplier under the Contract Document, if Supplier will

1. process GE Confidential Information, including hosting applications or providing a cloud computer platform,
2. have access to a GE Information System or a Trusted Third-Party Network Connection,
3. develop software for GE,
4. provide data center facility services,
5. support one or multiple critical business functions as defined by GE,
6. provide high availability requirements or the Third Party's service/application has high availability requirements as defined by GE,
7. leverage virtualization, is responsible for the management of the virtual machine image and/or hypervisor, and Processes GE Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data, and/or,
8. provide a product that includes executable binary code.

Part B: Security Incidents

1. Supplier shall notify GE without undue delay and no later than within 72 hours after discovery, or sooner if required by applicable law, of any Security Incident experienced by Supplier or its sub-processors. Supplier shall report Security Incidents to GE's Cyber Incident Response Team at security@ge.com. Supplier shall cooperate with GE in its investigation of a Security 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.

2. Unless prohibited by law, Supplier shall provide GE reasonable notice of, and the opportunity to comment on and approve, the content of any notice related to a Security Incident 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 to comply with applicable law.
3. 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.
4. Other than approved Security Notices, or to law enforcement or as otherwise required by law, Supplier may not make 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 C: GE Audit Rights

1. 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 the 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 Application 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 Confidential Information.
2. 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 D: Additional Regulatory Requirements

In the event Supplier Processes GE Confidential Information 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), compliance with additional security requirements, completion of regulatory filings applicable to Supplier, and participation in regulatory audits.

Part E: Supplier Personnel

Supplier is responsible for compliance with this Appendix by all Supplier Personnel. Prior to providing access to any GE Confidential Information to any Supplier Personnel, Supplier must obligate them to comply with applicable requirements of the Contract Document and this Appendix. Supplier shall take reasonable steps to ensure continuing compliance by such Supplier Personnel. Supplier may not appoint any third party engaged in providing services and/or deliverables under the Contract Document without the prior written consent of GE. Where such consent has been given, any change of such third party requires GE's prior written approval. Supplier must provide a list of sub-processors to GE and the supplier has a continuing obligation to update this list.

Part F: Beneficial Use of Data

Beneficial use of GE data is defined solely by GE. Supplier's uses of GE data are strictly limited to uses which are explicitly agreed to hereunder, or otherwise authorized in writing by GE.

Part G: Return of GE Confidential Information and Termination

Supplier shall, within thirty (30) days of termination of the Contract Document, or if requested during the term of the Contract Document, cease all Processing of GE Confidential Information and return to GE all copies of GE Confidential Information. In lieu of returning copies, GE may, at its sole discretion, require Supplier to destroy all copies of GE Confidential Information, using agreed upon methods to ensure such GE Confidential Information is not recoverable, and certify to such destruction. Supplier may continue to retain GE Confidential Information beyond the period prescribed in this section above only when required by law, or in accordance with the Contract Document and/or applicable regulatory or industry standards, 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 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 Confidential Information 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 Confidential Information until the same is securely deleted. Termination or

expiration of the Contract Document for any reason shall not relieve the Supplier from obligations to continue to protect GE Confidential Information in accordance with the terms of the Contract Document and this Appendix.

SECTION III – PRIVACY & DATA PROTECTION

Part A. Privacy & Data Protection - General Provisions. ***This Part A applies whenever a Supplier and/or its Supplier Personnel Process Personal Data in connection with the Contract Document, except where, for purposes of this Appendix, both GE and Supplier are Data Controllers, as defined by this Appendix or applicable privacy law, and the only GE Confidential Information Supplier Processes is Personal Data; in such circumstance, only the provisions of Section I and Section III(B)(2) shall apply.***

1. **Processing**. Supplier shall, and shall ensure that all of its Supplier Personnel shall:
   (a) Only Process Personal Data on, and in compliance with, GE's written instructions in a Contract Document and as issued from time to time. Where Supplier believes that any GE instruction violates the terms of the Contract Document or applicable law, unless prohibited from doing so by applicable law, Supplier must inform GE without delay before performing such instruction.
   (b) Process all Personal Data fairly and lawfully and in accordance with all laws applicable to Supplier's activities concerning Personal Data governed by this Appendix; and
   (c) only collect Personal Data directly where GE has provided prior written approval for such direct collection (including where expressly provided in the Contract Document), and, where such direct collection has been approved by GE, comply with applicable data privacy laws and regulations, including provisions concerning notice, consent, access and correction/deletion; any notices to be provided and any consent language to be used when collecting such information directly from a Data Subject are subject to GE's prior and written approval.

2. **International Transfers & Hosting Locations**. Supplier must receive approval from GE prior to (i) moving Personal Data from the hosting jurisdictions identified in the Contract Document to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than such hosting jurisdictions identified in the Contract Document; where GE approves, such approval may be conditioned on execution of additional agreements to facilitate compliance with applicable law.

3. **Inquiries**. 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 Personal Data or for information concerning Supplier's Processing of Personal Data.

4. **Confidentiality & Information Security**. Supplier shall comply with Section II above if Supplier Processes Personal Data in connection with the Contract Document. Supplier shall limit disclosure of or access to Personal Data to its Supplier Personnel who have legitimate business need-to-know relating to this Contract Document, and who have received proper training and instruction as to the requirements of the Contract Document (such as confidentiality requirements) and this Appendix.

5. **Supplier Personal Data.** GE may require Supplier to provide certain Personal Data 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 Data 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. Where the Supplier requires Personal Data from GE to satisfy performance of the Supplier's contractual obligations the terms of this paragraph are reciprocal.

Part B. – Omnibus Privacy & Data Protection Jurisdictions. ***This Part B applies whenever Processing of Personal Data by Supplier and/or Supplier Personnel in connection with the Contract Document falls within the scope of an Omnibus Privacy Law. In addition to the other applicable sections of this Appendix, to comply with the requirements of applicable Omnibus Privacy Laws, Supplier agrees to the following provisions (which shall prevail in the event of conflict with the other provisions of this Appendix).***

1. Where Supplier is a Data Processor, as defined by the applicable Omnibus Privacy Law, in connection with the Contract Document:

   a. Supplier shall assist GE in the fulfilment of GE's obligations under applicable law including
      i. preparation of Privacy Impact Assessments (where required);
      ii. response to Data Subject access requests; and

iii. any required breach notification to Data Protection Authorities and Data Subjects.

b. Supplier shall provide GE with the required information or data to respond to a Data Subject access request within at most ten (10) days.
c. If Supplier receives any Data Subject access requests directly or if Supplier is contacted by a Data Subject with inquiries regarding any Processing of Personal Data for GE, Supplier shall not respond to such access request unless required by applicable law, shall promptly notify GE of the request in writing, and shall direct Data Subject to GE.
d. Supplier shall assist GE in obtaining approval for Processing from Data Protection Authorities where required.
e. Supplier shall, at GE's election, either return or destroy Personal Data at the termination of the Contract Document (except as required by applicable law).
f. Upon request, Supplier shall provide GE with all information necessary to demonstrate Supplier's compliance with applicable law.
g. Where both GE and all Supplier Processing of Personal Data are located within the European Union (EU), European Economic Area (EEA), United Kingdom, Switzerland, or any other jurisdiction in which an Omnibus Privacy Law applies, or Supplier Processing occurs outside the EU, EEA and/or United Kingdom or Switzerland and related international transfers are subject to a transfer mechanism other than the EU Standard Contractual Clauses or other recognized transfer mechanism (e.g. adequacy, Supplier BCR-Processor or EU/Swiss-US Privacy Shield), the categories of Data Subjects' Personal Data Processed and the types of such Personal Data Processed may concern the following:

Categories of Data Subjects
Employees; trainees; applicants; contract and temporary workers; directors and others whose personal information is shared with GE in the context of an employment relationship; suppliers; distributors and agents; customers; prospects; and clients (which in the case of GE Healthcare may include patients)

Types of Personal Data
Identification data (name, surname, address, email address, date and other identifying information); professional identification data (CV, professional status, education, awards, job description, hierarchical positioning, performance levels);financial and economic information (bank details, salary); system log data; other personal data that may be contained in business related communications and interactions, internal systems and log data; and sensitive personal data including information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life, health or medical records and criminal records

2. Where both GE and Supplier are independent Data Controllers, as defined by an Omnibus Privacy Law in connection with the Contract Document:

   a. Both GE and Supplier shall comply with their respective obligations under applicable Omnibus Privacy Law in Processing such Personal Data, and shall Process such Personal Data in accordance with their respective obligations as Data Controller, which include the requirements to:
      i. Process Personal Data fairly and lawfully in accordance with the applicable Omnibus Privacy Law
      ii. Establish a legal basis under the applicable Omnibus Privacy Law for its Processing
      iii. Have complied with the applicable Omnibus Privacy Law in providing Data Subjects with clear and sufficient information about the purposes and legal basis for which it will Process Personal Data, and any other such information required by the applicable Omnibus Privacy Law

   b. Supplier shall Process Personal Data solely to the extent and duration necessary to provide the goods, services and/or deliverables to GE set out in the Contract Document, and shall not Process Personal Data for any other purpose or in any other manner unless required to do so under the applicable Omnibus Privacy Law.

   c. As Data Controller of Personal Data, GE and the Supplier affirm the following:
      i. They have implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk of Supplier's Processing of Personal Data
      ii. In addition to complying with any information security audit requirements applicable under the provisions of this appendix (for example, where GE Confidential information other than Personal Data is Processed by the Supplier), Supplier shall cooperate with GE in completing GE information security questionnaires or similar reviews on mutually agreed terms
      iii. Supplier complies with requirements of applicable Omnibus Privacy Laws regarding international transfers of Personal Data

iv. Supplier shall cooperate with GE for GE's compliance with any additional requirements of Omnibus Privacy Laws applicable to Supplier's Processing of Personal Data, (e.g. EU Standard Contractual Clauses for Controllers or equivalent, where Supplier is data importer)

v. Supplier complies with applicable Omnibus Privacy Law with respect to retention and secure deletion of Personal Data

d. As Data Controllers of Personal Data, GE and Supplier shall notify one another without undue delay after becoming aware of any Security Incident involving the Processing of Personal Data that falls within the scope of this Appendix. Supplier shall report Security Incidents to GE's Cyber Incident Response Team at security@ge.com. Supplier remains responsible for any costs associated with the investigation and required notices (e.g. to Data Subjects) of such Security Incidents which occur where Supplier has assumed a Data Controller role. Other than approved Security Notices, or to law enforcement or as otherwise required by law, Supplier may not make any public statements concerning GE's involvement with a Security Incident to any third-party without explicit written authorization of GE's Legal Department.

e. As Controllers of Personal Data, GE and Supplier further agree to cooperate to assist one another in the fulfillment of their respective obligations under applicable Omnibus Privacy Laws including:

i. Preparation of Privacy Impact Assessments (where required);

ii. Obtaining approval for Processing from Data Protection Authorities (where required);

iii. Responses to Data Subject access requests and other satisfaction of Data Subject rights

iv. Any required breach notification to Data Protection Authorities and Data Subjects