隐私和数据保护附录
2020 年 10 月 1 日

本附录适用于以下规定的情形。如果本附录与合同文件在本附录所涵盖的主题方面存在不一致或冲突，则应以要求对本附录约束的任何个人数据或其他 GE 信息进行更高级别保护的条款为准。本附录中的要求是对合同文件下 GE 与供应商之间任何保密义务的补充。GE 或负责保护本附录所约束的任何个人数据或其他 GE 信息的适用 GE 关联公司可以强制执行本附录的条款。如果供应商关联公司以自己的名义直接根据合同文件提供商品、服务和/或可交付成果，而在这种情况下，供应商对本附录中条款的同意也代表该供应商关联公司附属机构给出，且供应商保证该供应商关联公司具有如此为之的权力和权限，则本附录同样适用。本附录中所使用的“供应商”应理解为供应商和供应商关联公司的统称。

第 I 节 - 定义

以下定义和解释规则适用于本附录。措词“包括”、“含”、“如”、“例如”或任何类似表达后的任何词语仅供说明之用。

(i) ***合同文件***是指约束供应商向 GE 提供货物、服务和/或可交付成果的相关协议、合同、工作说明书、任务订单、采购订单或其他文件。

(ii) ***受控数据***是具有法律或法规所禁止的分发和/或处理要求的技术或政府信息，包括但不限于受控非机密信息和许可证所需出口受控数据，该数据由 GE 提供给第三方或由第三方为配合履行合同文件而创建。

(iii) ***数据的有益使用***即以合法方式使用数据以从中获取利润、优势或享受。

(iv) ***数据管控者***是指单独或与他人共同决定处理个人数据的目的和方式的自然人或法人、公共主管当局、专门机构或其他机构。

(v) ***数据处理者***是指代表数据管控者处理个人数据的自然人或法人、公共主管当局、专门机构或其他机构。

(vi) ***数据主体***是指已识别或可识别的自然人。

(vii) ***GE*** 是指通用电气公司或与供应商签订合同文件的 GE 关联公司方。

(viii) ***GE 关联公司***是指无论当前存在还是随后在合同文件期限内被创建或收购，均直接或间接控制 GE、受 GE 控制或与 GE 共同受控的任何实体。

(ix) ***GE 机密信息***是由 GE 创建、收集或修改，披露或使用不当时可能会对 GE 造成损害，且根据合同文件向供应商提供且如此注明的信息。GE 机密信息包括但不限于来自任何司法管辖区的高度机密个人数据、受控或敏感个人数据。

(x) ***GE 高度机密信息***即 GE 在合同文件中标识为“高度机密”，或 GE 在披露时标识为“受限”、“高度机密”或类似字样的 GE 机密信息。

(xi) ***GE 信息系统***是指由 GE 管理的任何系统和/或计算机，其中包括笔记本电脑和网络设备。

(xii) ***移动设备***是指运行移动操作系统的平板电脑、智能手机或类似设备。笔记本电脑不视为移动设备。

(xiii) ***综合隐私法***是指定义并承认各方为数据管控者和数据处理者（或以例如 GDPR 或 LGPD 等其他名称应用类似概念）的综合性国家隐私法。

(xiv) ***个人数据***是指与处于或来自适用法律所定义之任何司法管辖区的已识别或可识别的自然人（数据主体）相关的任何信息，该信息结合合同文件进行处理。在法律要求的情况下，法人是数据主体。个人数据至少是 GE 机密信息。

(xv) ***处理***是指对 GE 机密信息执行任何操作或一组操作（无论是否通过自动方式），包括但不限于收集、记录、组织、存储、改编或改变、检索、访问、咨询、使用、通过传输、传播或以其他方式提供来披露、对齐或组合、封锁、擦除或销毁。

(xvi) ***安全事故***是指 GE 机密信息被遗失、窃取、不当更改、不当销毁、用于合同文件或本附录不允许的目的、或被合同文件或本附录所规定的供应商人员之外的任何人访问的任何事故。

(xvii) ***敏感个人数据***是一类被认为特别敏感的个人数据，包含医疗记录和其他个人健康信息，其中包括：如《1996 年美国健康保险便携性法案》所定义，并受该法案约束的受保护健康信息 (PHI)（适用时）；个人银行帐户和支付卡信息以及其他财务帐户信息；客户银行帐户和支付卡信息；国别标识；根据适用法律规定的特殊类别数据（例如种族或民族、政治观点、宗教或哲学信仰、工会会员资格、基因和生物特征数据、家庭生活和性取向）。在某些司法管辖区，“敏感个人信息或数据”是一个已有定义的术语。在任何应用此类管辖定义的法律或法规适用的情况下，本附录中所定义的“敏感个人数据”一词旨在包括但不限于属于此类管辖定义的所有数据或信息。

(xviii) ***供应商***是按照合同文件向 GE 提供货物、服务和/或可交付成果的实体。供应商也可能被称为第三方。

(xix) ***供应商信息系统***是指按照合同文件用于处理、存储、传输和/或访问 GE 机密信息的任何供应商系统和/或计算机，包括笔记本电脑和网络设备。

(xx) ***供应商人员***是指按照合同文件提供服务和/或可交付成果的所有个人或实体，包括供应商的员工、经批准的关联公司和第三方（例如供应商、承包商、分包商和代理商），以及他们任何一者直接或间接雇用、聘用或聘请的任何人员。

(xxi) ***受信任第三方网络连接***是以与标准 GE 办公室相同的方式连接到 GE 内部网络的第三方网络的物理隔离段。

第 II 节 – 信息安全要求。*凡是供应商和/或供应商人员处理 GE 机密信息，有权访问与合同文件相关的 GE 信息系统，或向 GE 提供某些服务时，第 II 节适用。唯一的例外情况为，供应商处理的 GE 机密信息仅限于个人数据，且就本附录而言，GE 和供应商都是独立的数据管控者；在这种情况下，只有第I 节和第III(B)(2) 节的条款适用于供应商处理的个人数据。为澄清起见，第 II 节应适用于供应商/数据管控者处理的任何非个人 GE 机密信息，例如技术或业务财务信息。第 II 节中使用且未在本附录中定义的大写术语应具有本附录引用的《GE 第三方信息安全要求》中赋予它们的含义。*

A 部分：安全管控措施

供应商应遵循适用于供应商根据合同文件所提供之服务、产品和/或可交付成果的《GE 第三方信息安全要求》（可在 http://www.gesupplier.com/html/GEPolicies.htm），但前提是供应商将：

1. 处理 GE 机密信息，包括托管应用程序或提供云计算机平台；
2. 有权访问 GE 信息系统或受信任第三方网络连接；
3. 为 GE 开发软件；
4. 提供数据中心设施服务；
5. 支持 GE 所定义的一项或多项关键业务功能；
6. 提供高可用性要求，即第三方的服务/应用程序具有 GE 所定义的高可用性要求；
7. 利用虚拟化，负责管理虚拟机映像和/或虚拟机监控程序，并处理 GE 高度机密信息、机密信息、受控数据或敏感个人数据；并/或
8. 提供包含可执行二进制代码的产品。

B 部分：安全事故

1. 一旦供应商或其分处理商遭遇任何安全事故，则供应商应毫无拖延地且在不迟于发现该安全事故后的 72 小时内通知 GE，而如果适用法律有所要求，则应在较之更短的时间内通知 GE。供应商应通过 security@ge.com 向 GE 的网络事故响应团队报告安全事故。供应商应与 GE 合作调查安全事件，并向 GE 提供安全事故的详细描述、安全事故所涉及的数据类型、每个受影响人员的身份，以及一旦可以收集或以其他方式获得，GE 便会合理要求获取的任何其他信息。

2. 除非法律禁止，否则供应商应在向任何第三方发布或传达之前，向 GE 提供与安全事件相关的任何通告内容的合理通告以及评论和批准该内容的机会，只是 GE 无权否决安全通告中为遵循适用法律而必须包含的内容。
3. 如果 GE 选择就安全事故而发送安全通告，则供应商应根据安全通告，在适用法律或法规允许的情况下提供与该安全通告的内容和分发有关的合理且及时的信息。
4. 除经批准的安全通告之外，除非执法使然或法律另有要求，否则供应商在未经 GE 法律部门明确书面授权时不得向任何第三方发表任何有关 GE 卷入安全事故的公开声明。

C 部分：GE 审核权

1. GE 保留在提前 30 天通知的情况下对供应商是否遵守本附录中的要求进行审核的权利，包括但不限于：(i) 审核供应商的适用政策、流程和程序；(ii) 审核供应商最近漏洞评估及随附补救计划的结果；以及 (iii) 在供应商物理安全措施和供应商信息系统的常规工作时间进行现场评估。如果供应商的漏洞评估未达到或超过 GE 应用程序安全要求，GE 保留进行应用程序漏洞评估的权利。只要供应商处理 GE 机密信息，则此权利便应在合同文件终止或到期后继续有效。
2. 以合同文件的保密条款为准，GE 或其代表可以审查、审核、监控、拦截、访问和披露供应商提供的任何在 GE 信息系统上或在访问 GE 网络的 GE 移动设备上处理或存储的信息。

D 部分：追加监管要求

如果供应商处理受追加监管要求约束的 GE 机密信息，或以受追加监管要求约束的方式处理该信息，则供应商同意与 GE 合作，以确保 GE 遵守此类要求。此类合作可能包括但不限于执行适用法律要求的追加协议（例如欧盟标准合同条款、美国受保护健康信息协议）、遵守追加安全要求、完成适用于供应商的监管备案以及参与监管审核。

E 部分：供应商人员

供应商负责确保所有供应商人员均遵守本附录。在向任何供应商人员提供对任何 GE 机密信息的访问权限之前，供应商必须要求他们担负遵守合同文件和本附录中适用要求的义务。供应商应采取合理措施确，以保此类供应商人员持续遵守要求。未经 GE 事先书面同意，供应商不得指派任何第三方参与提供合同文件规定的服务和/或可交付成果。在获得此类同意的情况下，此类第三方的变更均必须获得 GE 的事先书面批准。供应商必须向 GE 提供一份分处理商名单，且供应商有义务持续更新该名单。

F 部分：数据的有益使用

GE 数据的有益使用仅由 GE 定义。供应商对 GE 数据的使用严格限定为本附录下明确同意的或 GE 以书面形式另行授权的用途。

G 部分：GE 机密信息的返还和终止

供应商应在合同文件终止后三十 (30) 天内，或在 GE 提出要求的情况下则应在合同文件的期限内，停止对 GE 机密信息的一切处理，并将 GE 机密信息的所有副本返还 GE。GE 可以自行决定要求供应商使用商定的方法销毁 GE 机密信息的所有副本，从而确保此类 GE 机密信息不可恢复，并证明此类销毁，以代替副本返还。只有在法律要求或合同文件和/或适用的监管或行业标准要求时，供应商可以在本节上述规定的期限过后继续保留 GE 机密信息，但前提是：(i) 供应商在合同文件终止或到期之前向 GE 通知义务，包括此类保留的具体原因；(ii) 供应商对此类副本设有书面保留期和安全删除程序，备份副本仅保留到其法律要求的保留期结束；(iii) 在该保留期之后，所有副本和备份副本均以无法恢复的方式删除；(iv) 供应商不会对非保留或删除相关副本所需的 GE 机密信息进行处理；(v) 供应商继续遵守本附录中与任何此类保留的 GE 机密信息有关的所有要求，直到这些信息被安全地删除。

不论合同文件因何种原因终止或到期，均不会免除供应商根据合同文件和本附录的条款继续保护 GE 机密信息的义务。

第 III 节 - 隐私和数据保护

A 部分. 隐私和数据保护 - 总则。 ***凡是供应商和/或其供应商人员处理与合同文件相关的个人数据时，本节 A 部分适用，但就本附录而言，GE 和供应商都是本附录或适用隐私法所定义的数据管控者，且唯一的 GE 机密信息供应商流程是个人数据时除外；在这种情况下，仅第 I 节和第 III(B)(2) 节的条款适用。***

1. **处理。**供应商自身应，且应确保其所有供应商人员应：
   (a) 仅按照 GE 在合同文件中以及不时发出的指示处理个人数据。如果供应商认为有任何 GE 指示违反合同文件或适用法律的条款，除非适用法律禁止如此为之，否则供应商必须在执行此类指示之前毫不迟疑地通知 GE。
   (b) 依据所有适用于本附录所约束之个人数据相关供应商活动的法律，公正合法地处理所有个人数据；且
   (c) 仅在 GE 已为直接收集提供事先书面批准的情况下（包括在合同文件中明确提供时），直接收集个人数据，并在此类直接收集已获得 GE 批准的情况下，遵守适用的数据隐私法律和法规，包括关于通知、同意、访问和纠正/删除的条款；直接从数据主体收集此类信息时将提供的任何通知以及将使用的任何同意语言均需事先获得 GE 的书面批准。

2. **国际传输和托管地点**。在 (i) 将个人数据从合同文件中确定的托管司法管辖区传输到另一个托管司法管辖区，或 (ii) 提供从合同文件中确定的托管管辖区以外的任何位置对此类个人数据的远程访问之前，供应商必须获得 GE 的批准；在 GE 给予批准的情况下，此类批准以可能执行追加协议为条件，以促进遵守适用法律。
3. **查询**。除非法律禁止，否则供应商应立即通知 GE，并仅根据 GE 就第三方为披露个人数据或关于供应商处理个人数据的信息所提任何请求而给出的指示采取行动。
4. **保密**和信息安全如果供应商处理处理与合同文件相关的个人数据，则供应商应遵守上述第 II 节的条款。供应商应将个人数据的披露权或访问权限定至其如下供应商人员：对于该合同文件为合法业务须知者；以及已就合同文件和本附录的要求（例如保密要求）接受过适当培训和指导者。
5. **供应商个人数据。**GE 可以要求供应商提供某些个人数据（例如供应商代表的姓名、地址、电话号码和电子邮件地址）以促进合同文件的履行，GE 及其承包商可以将此类数据存储在位置合适且可供其人员在世界各地访问的数据库中，并将其用于与履行合同文件相关的必要目的，包括但不限于供应商支付管理。GE 将在法律意义上成为该数据的数据管控者，并同意使用合理的技术和组织措施，以确保按照适用的数据保护法处理此类信息。供应商可以通过书面请求获取供应商个人信息的副本，或通过书面通知向 GE 提交更新和更正。GE 将始终遵守在其网站上发布的隐私政策。在供应商要求 GE 提供个人数据以履行供应商合同义务的情况下，本段的条款具有互惠性。

B 部分. – 综合隐私和数据保护司法管辖区。 ***只要供应商和/或供应商人员处理与合同文件有关的个人数据属于综合隐私法的适用范围，则本节 B 部分适用。除本附录的其他适用各节外，为遵守适用的综合隐私法的要求，供应商进一步同意如下条款（如果它们与本附录的其他条款发生冲突，则以前者为准）。***

1. 如果供应商是适用综合隐私法所定义的与合同文件相关的数据处理者：

   a. 供应商应协助 GE 履行 GE 在适用法律下应尽的义务，包括：
      i. 准备隐私影响评估（必要时）；
      ii. 响应数据主体访问请求；以及
      iii. 向数据保护机构和数据主体发出任何必要的违规通知。

b. 供应商应在最多十 (10) 天内向 GE 提供响应数据主体访问请求所需的信息或数据。
c. 如果供应商直接收到任何数据主体访问请求，或如果数据主体联系供应商询问有关为 GE 处理个人数据的任何问题，除非适用法律要求，否则供应商不得回应此类访问请求，而应立即以书面形式向 GE 通知该请求，并应将数据主体引导到 GE。
d. 必要时，供应商应协助 GE 获取数据保护机构的处理批准。
e. 供应商应根据 GE 的选择，在合同文件终止时返还或销毁个人数据（适用法律要求的除外）。
f. 一经要求，供应商应向 GE 提供证明供应商遵守适用法律所需的所有信息。
g. 如果 GE 和所有处理个人数据的供应商均处于欧盟 (EU)、欧洲经济区 (EEA)、英国、瑞士或综合隐私法适用的任何其他司法管辖区，或供应商处理发生在欧盟、欧洲经济区和/或英国或瑞士之外，且相关的国际传输受《欧盟标准合同条款》或其他公认传输机制（例如充分性、《供应商 BCR-处理者》或《欧盟/瑞士-美国隐私护盾》）以外的传输机制的约束，则数据主体的已处理个人数据的类别和此类已处理个人数据的类型可能涉及以下内容：

数据主体的类别
员工；学员；申请人；合同工和临时工；主管和在雇佣关系中与 GE 共享其个人信息的其他人员；供应商；分销商和代理商；顾客；潜在客户；以及客户（对于 GE Healthcare，客户可能包括患者）。

个人数据的类型
识别数据（名字、姓氏、地址、电子邮件地址、日期和其他识别信息）；职业识别数据（简历、职业地位、学历、奖项、职位描述、层级定位、绩效水平）；财务和经济信息（银行详细信息、工资）；系统日志数据；可能包含在业务相关通信和互动、内部系统和日志数据中的其他个人数据；以及敏感个人数据，包括有关种族或民族血统、政治观点、宗教或哲学信仰、工会会员资格、性生活、健康或医疗记录和犯罪记录的信息。

2. 如果 GE 和供应商都是与合同文件相关的综合隐私法所定义的独立数据管控者：

a. GE 和供应商在处理此类个人数据时均应遵守各自在适用综合隐私法下的义务，并应按照各自作为数据控制者的义务处理此类个人数据，其中包括以下要求：

i. 根据适用的综合隐私法，公正且合法地处理个人数据；
ii. 根据适用的综合隐私法，为其处理建立法律基础；
iii. 在向数据主体提供有关其处理个人数据的目的和法律依据的明确且充分的信息，以及适用的综合隐私法要求的任何其他此类信息时，已遵守适用的综合隐私法；

b. 供应商应仅在合同文件中规定的向 GE 提供商品、服务和/或可交付成果所需的范围和期限内处理个人数据，且不得出于任何其他目的或以任何其他方式处理个人数据，除非根据适用的综合隐私法要求如此为之。

c. 作为个人数据的数据管控者，GE 和供应商确认以下各项：

i. 他们已实施适当的技术和组织措施，以确保安全级别与供应商处理个人数据的风险相适应；
ii. 除了遵守本附录条款下适用的任何信息安全审核要求之外（例如，如果供应商处理个人数据以外的 GE 机密信息），供应商还应根据双方商定的条件与 GE 合作完成 GE 信息安全调查问卷或类似审查；
iii. 供应商遵守个人数据国际传输相关适用综合隐私法的要求；
iv. 供应商应与 GE 合作，以确保 GE 遵守适用于供应商处理个人数据的综合隐私法的任何追加要求（例如，《欧盟控制者标准合同条款》或等效条款，其中供应商为数据进口者）；
v. 供应商就个人数据的保留和安全删除遵守适用的综合隐私法。

d. 作为个人数据的数据管控者，GE 和供应商应在发现任何涉及本附录适用范围内个人数据处理的安全事故后立即通知对方。供应商应通过 security@ge.com 向 GE 的网络事故响应团队报告安全事故。供应商仍旧负责承担与供应商担任数据管控者角色时发生的此类安全事故的调查和所需通知（例如向数据主体）相关的任何费用。除经批准的安全通告之外，除非执法使然或法律另有要求，否则供应商在未经 GE 法律部门明确书面授权时不得向任何第三方发表任何有关 GE 卷入安全事故的公开声明。

e. 作为个人数据管控者，GE 和供应商进一步同意合作，以协助彼此履行各自在适用综合隐私法下的义务，包括：

i. 准备隐私影响评估（必要时）；
ii. 获取数据保护机构的处理批准（必要时）；
iii. 响应数据主体访问请求，并以其他方式满足数据主体权利；
iv. 向数据保护机构和数据主体发出任何必要的违规通知。