数据处理协议

本数据处理协议（“协议”）签约双方为 Siemens Product Lifecycle Management Software Inc.，也被称为 Siemens Industry Software（以下简称“SISW”），以及签名接受本协议条款及条件的客户（“客户”）。 SISW 保留通过其关联公司行使其在本协议下的任何权利并履行其在本协议下任何义务的权利。 因此，本协议下所用“SISW” 一词还可指由 Siemens Product Lifecycle Management Software Inc. 最终母公司直接或间接拥有或控制的关联公司，以及经 Siemens Product Lifecycle Management Software Inc. 授权发行 SISW 云服务（“云服务”）的个体。

客户应全权负责确定受处理影响的数据和个体类型，并应确保此类云服务方式处理的合法性。 客户也应负责利用云服务所提供之功能对个人数据进行任何更正、删除或拦截。 客户可利用云服务所提供之功能导出并删除其数据，包括个人数据。 在本数据处理协议终止后，客户应于 30 日内向 SISW 发送书面请求，要求客户数据可供客户下载。 在 SISW 所规定的用于响应此类请求的任何期限期满后，客户的任何剩余数据将可予以删除，将不再提供给客户。 SISW 和客户同意，在云服务范围内，客户发布指令的权利仅可通过利用云服务所提供之功能予以行使。 对于客户数据的附加指令，则要求 SISW 和客户签订一份独立的书面协议，包括一份有关客户执行此类指示所需支付任何额外费用的协议。 客户承诺，其将不会向云服务上传或于其中存储任何受保护的健康信息 (PHI)，除非 SISW 和客户已签订一份独立的书面协议，明确允许将 PHI 存储于云服务中。

在提供云服务时，就运行系统而言，SISW 应遵守本数据处理协议附件 A 下附录 2 中所规定的技术和组织措施。 与云服务相关的非运行系统可能会或可能不会遵守本数据处理协议附件 A 下附录 2 中所规定的技术和组织措施。 此外，SISW 可不时变更运行系统适用的技术和组织措施，前提是此类变更不会以任何重大方式对此类措施的保护级别产生不利影响。 SISW 将限制其人员在未经授权的情况下收集、处理或使用个人数据，并将仅雇用经明确指示遵守数据隐私保护要求的人员处理客户个人数据。

SISW 有权在云服务执行过程中雇佣辅助处理方。 如果辅助处理方对客户个人数据的访问无法予以拒绝，经客户要求，SISW 将提供有关此类辅助处理方和其各自所在地的列表，并于任何新辅助处理方获授权访问客户个人数据前，按照规定对此类列表进行更新。 如果客户对任何新辅助处理方提出合理异议，客户应将此类异议告知 SISW，且如果 SISW 坚持雇佣新辅助处理方，客户应有权以正当理由终止本数据处理协议。 如果任何此类辅助处理方的雇佣涉及个人数据的跨境传输，SISW 将尽力敦促此类辅助处理方就此类个人数据维持适当的数据保护水平。

SISW 将定期核验适用的技术和组织措施是否予以遵守，并在经客户合理要求时，向其确认适用的技术和组织措施已得到遵守。 如果客户有理由相信 SISW 所作确认有误，客户应有权经合理的事先通知，与 SISW 协商后安排审核，以确认技术和组织措施是否予以遵守。 此类审核的成本和费用应由客户承担。

SISW 和客户同意，针对从欧盟国家至非欧盟国家的客户个人数据的任何数据传输，如果欧盟认为此类非欧盟国家未达到充分的个人数据保护水平，此类传输将按照欧盟标准合约条款执行，相关条款详见附件 A，且已充分纳入本协议下。 如果本数据处理协议和标准合约条款存在冲突，则以标准合约条款为准。 标准合约条款将受数据输出方（定义见附件 A）所在欧盟成员国法律的支配。

附件 A
欧盟标准合约条款

根据《欧盟数据保护指令》(95/46/EC) 第 26(2) 条，就将个人数据传输至位于未能确保充分数据保护水平的第三方国家/地区的处理方，

以下双方

客户和/或其欧盟境内的关联公司

（以下简称“**数据输出方**”）

以及

Siemens Product Lifecycle Management Software Inc.，也称为 Siemens Industry Software，包括由 Siemens Product Lifecycle Management Software Inc. 最终母公司直接或间接拥有或控制的任何关联公司，以及经 Siemens Product Lifecycle Management Software Inc. 授权可以其名义处理数据的个体，

（以下简称“**数据输入方**”）

单称为“一方”，合称为“双方”，

已达成下述合约条款（“合约条款”），以就附录 1 下所述由数据输出方至数据输入方的个人数据传输，针对个人隐私和基本权利和自由的保护实施充分保障。

第 1 条 定义

根据合约条款规定：

(a) “个人资料”、“特殊的数据类型”、“处理/处理中”、“控制方”、“处理方”、“数据主体”及“监管当局”应具有欧洲议会和理事会于 1995 年 10 月 24 日颁布的有关个人数据处理相关个体的保护和此类数据自由传输的《欧盟数据保护指令》(95/46/EC) 下所载列的相同含义；

(b) “数据输出方”指传输个人数据的控制方；

(c) “数据输入方”指同意从数据输出方处接收按照数据输出方指示及本合约条款下规定进行传输后，以数据输出方的名义予以处理的个人数据的处理方，且其不受制于可确保《欧盟数据保护指令》(95/46/EC) 第 25(1) 条下所定义范围内充分保护的第三方国家/地区系统；

(d) “辅助处理方”指由数据输入方或其任何其他辅助处理方雇佣的任何处理方，其同意从数据输入方或其任何其他辅助处理方处接收个人数据，此类数据在按照数据输出方指示、本合约条款及书面分包合同条款进行传输后，仅计划用于以数据输出方的名义执行的处理活动；

(e) “适用的数据保护法”指就适用于数据输出方所在成员国的数据控制方的个人数据的处理而言，旨在保护个人基本权利和自由（尤其是隐私权）的法律；

(f) “技术和组织安全措施”指旨在保护个人数据以防意外或非法破坏或意外丢失、变更、擅自披露或访问的措施，尤其适用涉及网络数据传输的处理，以及抵制所有其他非法的处理形式。

第 2 条　传输细节

传输细节及尤其是特定情况下个人数据的特殊类型详载于附录 1 下，其构成了本合约条款不可分割的一部分。

第 3 条　第三方受益人条款

1. 数据主体可以第三方受益人的身份针对数据输出方强制执行本款、第 4(b) 至 (i) 款、第 5(a) 至 (e) 款和 (g) 至 (j) 款、第 6(1) 和 (2) 款、第 7 款、第 8(2) 款，以及第 9 至 12 款。

2. 数据主体可针对数据输入方强制执行本款、第 5(a) 至 (e) 和 (g) 款、第 6 款、第 7 款、第 8(2) 款及第 9 至 12 款，如果数据输出方已从事实意义上消失或已在法律意义上不存在，除非任何继任实体已以合同或法律实施途径承担了数据输出方的全部法律义务，即其将因此承担数据输出方的权利和义务，则在这一情况下，数据主体可针对此类实体强制执行上述条款。

3. 数据主体可针对辅助处理方强制执行本款、第 5(a) 至 (e) 和 (g) 款、第 6 款、第 7 款、第 8(2) 款及第 9 至 12 款，如果数据输出方和数据输入方已从事实意义上消失或已在法律意义上不存在或遭受破产，除非任何继任实体已以合同或法律实施途径承担了数据输出方的全部法律义务，即其将因此承担数据输出方的权利和义务，则在这一情况下，数据主体可针对此类实体强制执行上述条款。 辅助处理方的此类第三方责任应仅限于本合约条款下其自身的处理操作。

4. 双方接受以联盟或其他主体为代表的数据主体，前提是数据主体明确提出此类意愿且符合国家法律规定。

第 4 条　数据输出方的义务

数据输出方同意并保证：

(a) 个人数据的处理，包括传输本身，已经并将继续遵守适用的数据保护法下相关规定（并在适用时已告知数据输出方所在成员国的有关当局），并且不违反该成员国的有关规定；

(b) 其已指示并将在个人数据处理服务的整个期间指示数据输入方处理个人数据，此类数据仅以数据输出方的名义进行传输，且传输符合适用的数据保护法和本合约条款的规定；

(c) 数据输入方将就本协议附录 2 下的技术和组织安全措施提供充分保证；

(d) 在对适用的数据保护法规定进行评估后，此类安全措施可适当用于保护个人数据以防意外或非法破坏或意外丢失、变更、擅自披露或访问的措施，尤其适用涉及网络数据传输的处理，以及抵制所有其他非法的处理形式，且此类措施保证了一定的安全等级，在考虑到现有技术和实施成本的基础上，其可适当防御处理和待保护数据性质所带来的风险；

(e) 其将确保遵守安全措施的规定；

(f) 如果传输涉及到特殊的数据类型，数据主体已被告知或将被提前告知或在传输后尽快得知，其数据可能传输至未能提供《欧盟数据保护指令》(95/46/EC) 下所定义范围内充分保护的第三方国家/地区；

(g) 如果数据输出方决定继续传输或解除暂停，则根据第 5(b) 款和第 8(3) 款的规定，将来自数据输入方或任何辅助处理方的通知进一步告知数据保护监管当局；

(h) 经数据主体要求，向其提供本合约条款副本（附录 2 除外）、安全措施概述，以及按照本合约条款编制的任何有关辅助处理服务的合同副本，除非本合约条款或合同包含商业信息，则在这一情况下，可将此类商业信息予以删除；

(i) 对于辅助处理而言，处理活动由辅助处理方按照第 11 款进行，其应就个人数据和数据主体权利的保护提供与数据输入方在本合约条款下的同等保护水平；以及

(j) 其将确保遵守第 4(a) 至 (i) 款；

第 5 条　数据输入方的义务

数据输入方同意并保证：

(a) 仅以数据输出方的名义，且在遵守其指示和本合约条款的前提下对个人数据进行处理；如果数据输入方因任何原因而无法保证遵守此类规定，其同意立即告知数据输出方其无法遵守，则在这一情况下，数据输出方有权暂停数据传输和/或终止合同；

(b) 其无理由相信适用法律阻止其履行从数据输出方处收到的指示及其在合约下的义务，且如果法律变更可能对本合约条款下的保证和义务产生重大不利影响，其将在得知此类变更后及时将其告知数据输出方，则在这一情况下，数据输出方有权暂停数据传输和/或终止合同；

(c) 其在处理传输的个人数据前已执行了附录 2 下的技术和组织安全措施；

(d) 其将立即告知数据输出方以下事项：

(i) 任何要求执法当局披露个人数据的具有法律约束力的请求，除非另有禁止规定，例如，刑法下有关确保执法调查保密性的禁令；
(ii) 任何意外或未经授权的访问；以及
(iii) 直接从数据主体处收到的任何请求，且无需作出响应，除非其已经明确授权作出响应；

(e) 及时并妥善处理来自数据输出方的与传输的个人数据的处理相关的咨询，并采纳监管当局有关传输的个人数据的处理的建议；

(f) 经数据输出方要求，提交其数据处理设施，以将其用于本合约条款下对处理活动的审计，此类审计将由数据输出方或由独立成员组成且持有所需专业资质的检查机构进行，此类机构受保密义务约束，由数据输出方选定（适用时），且与监管当局达成一致；

(g) 经数据主体要求，向其提供本合约条款副本或任何现有的辅助处理合同，除非本合约条款或合同包含商业信息，则在这一情况下，可将此类商业信息予以删除，但附录 2 除外，其将在数据主体无法从数据输出方处获得副本的情况下由安全措施概述予以替代；

(h) 对于辅助处理而言，其已将相关情况提前告知数据输出方并取得了事先书面同意；

(i) 处理服务将由辅助处理方按照第 11 款执行；

(j) 及时将其在本合约条款下订立的任何辅助处理方协议的副本发至数据输出方。

第 6 条　法律责任

1. 双方同意，如果任何数据主体因任何一方或辅助处理方违反第 3 款或第 11 款下义务而遭受损失，其有权就所受损失从数据输出方处获得赔偿。

2. 如果由于数据输出方已从事实意义上消失或已在法律意义上不存在或已遭受破产，数据主体无法因数据输入方或其辅助处理方对其在第 3 款或第 11 款下的任何义务违反而针对数据输出方提起第 1 项下的赔偿诉求，数据输入方同意，数据主体可针对数据输入方提起诉求，犹如其为数据输出方，除非任何继任实体已以合同或法律实施途径承担了数据输出方的全部法律义务，则在这一情况下，数据主体可针对此类实体强制行使其权利。

   数据输入方不得鉴于辅助处理方违反了其义务而规避自身的责任。

3. 如果由于数据输出方和数据输入方均已从事实意义上消失或已在法律意义上不存在或已遭受破产，数据主体无法因辅助处理方对其在第 3 款或第 11 款下的任何义务违反而针对数据输出方或数据输入方提起第 1 和 2 项下的赔偿诉求，辅助处理方同意，数据主体可针对数据辅助处理方在本合约条款下自身的处理操作向其提起诉求，犹如其为数据输出方或数据输入方，除非任何继任实体已以合同或法律实施途径承担了数据输出方或数据输入方的全部法律义务，则在这一情况下，数据主体可针对此类实体强制行使其权利。 辅助处理方的法律责任应仅限于本合约条款下其自身的处理操作。

第 7 条　调解及管辖权

1. 数据输入方同意，如果数据主体行使其第三方受益人权利和/或就本合约条款下的损害寻求赔偿，数据输入方将接受数据主体的决策：

   (a) 将冲突提交至一位独立人士或（在适用时）监管当局进行调解；

   (b) 将冲突提交至数据输出方所在成员国的法院。

2. 双方同意，数据主体所作决策将不得对其根据国家或国际法律下其他条款而寻求救济的实体或程序权利造成影响。

第 8 条　与监管当局的合作

1. 数据输出方同意，如果监管当局要求，或适用的数据保护法下予以要求，其将向监管当局提交本协议副本。

2. 双方同意，监管当局有权就数据输入方或任何辅助处理方进行审计，此类审计具有适用的数据保护法下针对数据输出方所执行审计相同的范围和条件。

3. 如果存在适用于数据输入方或任何辅助处理方的法律，以阻止就数据输入方或任何辅助处理方执行第 2 项下的审计，数据输入方将立即告知数据输出方。 在此类情况下，数据输出方有权采取第 5(b) 款下载列的措施。

第 9 条　适用法律

本合约条款应受数据输出方所在成员国法律的支配。

第 10 条　合同变更

双方承诺不会对本合约条款进行变更或修改。 但本规定不得妨碍双方在必要情况下新增有关业务相关事宜的条款，前提是此类条款不与本合约条款冲突。

第 11 条　辅助处理

1. 未经数据输出方事先书面同意，数据输入方不得分包其在本合约条款下以数据输出方的名义执行的任何处理操作。 如果在取得数据输出方同意的情况下，数据输入方分包其在本合约条款下的义务，其仅能以与辅助处理方订立书面协议的方式进行转包，且本协议向辅助处理方施加了与本合约条款向数据输入方所施加的同等义务。 如果辅助处理方未能履行其在此类书面协议下的数据保护义务，数据输入方应就辅助处理方对此类协议下义务的履行向数据输出方负有全部责任。

2. 数据输入方和辅助处理方之间的事先书面合同也应载列一项如第 3 款下的第三方受益人条款，以将其适用于由于数据输出方或数据输入方已从事实意义上消失或已在法律意义上不存在或已遭受破产，且无继任实体以合同或法律实施途径承担了数据输出方或数据输入方的全部法律义务，数据主体无法针对数据输出方或数据输入方提起第 6 款第 1 项下的赔偿诉求的情况。 辅助处理方的此类第三方责任应仅限于本合约条款下其自身的处理操作。

3. 第 1 项下所载列合同中与辅助处理数据保护相关的条款应受数据输出方所在成员国法律的支配。

4. 数据输出方应，编制在本合约条款下签订的且由数据输入方按照第 5(j) 款的规定予以告知的辅助处理协议的列表，此类列表应至少于每年更新一次。 该列表应提交至数据输出方的数据保护监管当局。

第 12 条　个人数据处理服务终止后的义务

1. 双方同意，在数据处理服务提供终止后，数据输入方和辅助处理方应按照数据输出方的指示，向其归还所有传输的个人数据及相关副本，或应销毁所有个人数据并向数据输出方证明其确已销毁，除非数据输入方所适用法律阻止其归还或销毁全部或部分已传输个人数据。 在这一情况下，数据输入方保证，其将确保已传输个人数据的保密性，并将不再主动对其加以处理。

2. 数据输入方和辅助处理方保证，经数据输出方和/或监管当局要求，其将提交其数据处理设施，以将其用于第 1 项下的措施审计。

标准合约条款附录 1

数据输出方
数据输出方指（请简要说明与传输相关的活动）：

客户，系 SISW 所提供云服务的订购者，SISW 批准经客户授权的最终用户访问、修改、使用、删除、下载及以其他方式处理客户数据，此类数据可能包括本协议下所述的个人数据和用于云服务的相关文档。

数据输入方
数据输入方指（请简要说明与传输相关的活动）：

Siemens Product Lifecycle Management Software Inc.，其自身和/或通过辅助处理方提供云服务，其包括：维护云服务运行所基于的且位于美国和欧盟的计算基础架构；在基础架构中存储由客户上传至云服务的客户数据；监测云服务和基础设施的可用性和持续运行；以及维护本协议和云服务相关文档下所述基础架构的安全性。

数据主体
已传输个人数据涉及下述数据主体类型（请说明）：

除非数据输出方明确书面规定，数据主体可能包括经客户授权使用云服务的最终用户和个人数据存储于云服务中的客户的其他人士。

数据类型
已传输个人数据涉及下述数据类型（请说明）：

存储于云服务中的特定数据类型受限于客户的重要配置，但是，可能存储于云服务中的通用数据类型包括但不限于：姓名、邮箱地址、公司名称、电话、工作地点、国籍或公民身份，以及与云服务的访问和使用相关的信息。 根据客户的云服务配置，诸多其他数据类别可能存在于客户数据中。

特殊的数据类型（如适用）
已传输个人数据涉及下述特殊的数据类型（请说明）：

任何存储于云服务中的特殊数据类型将由双方在本协议中或订单中约定，或详载于待提供至客户的专业服务工作说明书中，以作为其云服务部署的一部分。

处理操作
已传输个人数据将受限于下述基本处理活动（请说明）：

可对个人数据执行下述处理：基于客户配置，作为云服务正常操作的一部分；通过存储和/或存档部署于由数据输出方维护的计算基础架构中，于单租户或多租户环境下进行处理；根据由经客户授权使用云服务的最终用户发至云服务的指示进行访问或传送；以及作为由数据输出方执行的云服务维护操作的一部分。

标准合约条款附录 2

部分云服务产品基于不同条款进行提供，且此类条款在适用时将详载于订单中。 否则，根据第 4(d) 和第 5(c) 款的规定，数据输入方将就存储于系统中的个人数据执行下述技术和组织措施。

关于数据输入方根据第 4(d) 和第 5(c) 款的规定执行的技术和组织安全措施的描述如下：

1. 物理访问控制。 未经授权人士将不得获得对处理和/或使用个人数据的数据处理系统所在房屋、建筑物或房间的物理访问。

   措施： 所有数据中心严格遵守强制适用于安保人员、监控器材、运动检测器、访问控制机制的安全程序及其他措施，以防止设备和数据中心设施不受损害。 仅授权代表有权访问数据中心设施内部系统和基础架构。 为确保适当的功能性，物理安全设备（例如：运动传感器、照相机等）将得到定期维护。 详细而言，下述物理安全措施将于所有数据中心执行：

   a. 一般情况下，建筑物通过访问控制系统（智能卡接入系统）予以保护。
   b. 授权证书，其包括一个电子访问卡（区分员工、供应商或承包商）和 PIN 码，将提供至授权人员，以确保获得对数据中心设施的物理访问。
   c. 对数据中心系统边界内的物理访问受电子访问控制系统的强制监管，该系统包括在建筑物和房间入口部署有读卡器和 PIN 码按键，且在建筑物和房间出口部署有读卡器。
   d. 根据安全级别，建筑物、个别区域及周边房屋会进一步采取其他保护措施。 此类措施包括特定访问配置、视频监控、防盗报警系统及生物识别访问控制系统。
   e. 访问权限将根据下述系统和数据访问控制措施在专用基础上授予授权人员。 该规定同样适用于访客访问。 前往 SISW 建筑物的来客和访客必须在接待处登记其姓名，且必须由 SISW 授权人员陪同。 SISW 和所有第三方数据中心提供商正在记录进入数据中心内部 SISW 私人区域的人员姓名和时间。
   f. SISW 员工和外部人员必须于所有 SISW 场所佩戴身份证件。

2. 系统访问控制。 用于提供云服务的数据处理系统必须防止未经授权的使用。

   措施：
   a. SISW 或其辅助处理方按照 NIST SP 800-53：第 4 版，访问控制 (AC) 及标识和认证 (IA) 要求对环境进行管理。
   b. 多个授权级别将适用对敏感系统访问权限的授予，包括此类用于存储和处理个人数据的系统。 相关流程将执行到位，以确保仅授权用户具有添加、删除或修改用户的适当权限。
   c. 所有 SISW 系统的访问用户所持有的独特用户名和密码必须达到最低复杂性标准。
   d. SISW 及其辅助处理方会将相关流程执行到位，以确保经请求的授权更改仅能按照准则执行（例如：未经授权则不会授予权限）。 如果 SISW 用户变更角色或离开公司，将执行一项撤销环境访问权限的流程。
   e. SISW 和辅助处理方已制定一项密码策略，旨在禁止密码共享、管理密码泄露、要求对所有使用密码进行定期变更，以及要求对预设密码进行变更。 分配的个性化用户 ID 用于认证。 所有密码必须达到最低复杂性标准，并以加密方式存储。 对于域名密码，系统强制要求每隔 60 日对达到最低复杂性标准的密码进行变更。 每台 SISW 电脑设置有密码保护屏幕保护程序。
   f. SISW 或其辅助处理方对下述帐户事件进行自动审核：创建、修改、启用、禁用及删除。 系统管理员将定期检查日志。
   g. SISW 及其辅助处理方的网络使用防火墙与公共网络隔离开来。
   h. SISW 及其辅助处理方在公司网络接入点针对电子邮件帐户部署有最新防病毒软件，并在所有文件服务器及所有工作站中同样部署有此类软件。
   i. SISW 及其辅助处理方实施安全补丁管理，以确保部署相关安全更新。
   j. 对 SISW 企业网络和关键基础架构的全远程访问受到强大的多因素认证保护。

3. 数据访问控制。 有权使用数据处理系统的人员将获得仅适用于其有权访问的个人数据的访问权限，且在处理、使用及存储过程中不得对个人数据进行未经授权的读取、复制、修改或删除。

措施：

a. 个人、保密或敏感信息访问权限仅在须知的情况下授予。 换言之，员工或外部第三方有权访问完成其工作所需的信息。 SISW 所使用授权概念记录了权限是如何指定的，及哪些权限予以指定。 所有个人、保密或其他方式下的敏感数据将根据 SISW 安全策略和标准予以保护。
b. 任何 SISW 云服务的所有运行服务器将于相关数据中心进行运行。 用于保护处理个人、保密或其他敏感信息的应用程序的安全措施将得到定期检查。 为此，SISW 还推行周期性外部审计，以确认此类措施得到适当方式的应用。
c. SISW 不允许向当前用于任何云服务的系统安装未经 SISW 批准的个人软件或其他软件。
d. 如果因底层数据存储介质故障而要求传输数据，自此类传输完成之后，存在故障的存储介质将被消磁（适用磁存储）或碎片处理（适用固态或光存储）。

4. 数据传输控制。 在传输过程中，不得在未经授权的情况下对个人数据进行读取、复制、修改或删除。

措施：

a. SISW 或其辅助处理方按照 NIST SP 800-53：第 4 版，系统和通信保护 (SC) 要求对基础架构和配置进行管理。 其包括部署于系统边界的基于网络的入侵防御系统 (NIPS) 和防火墙，以防止基础架构外部边界的恶意通信。 NIPS 和防火墙按照 DISA STIG 标准进行配置。 使用符合 FIPS 140-2 的加密模块在传输过程中对数据进行加密。
b. 如果数据载体以物理方式进行运输，SISW 将实施适当措施，以确保达到约定的服务级别（例如：加密及衬铅容器）。
c. 根据 SISW 的安全策略，经由 SISW 内部网络的个人数据传输受到与任何其他保密信息同等的保护。
d. 当数据在 SISW 和客户之间传输时，适用于已传输个人数据的保护措施详载于本协议或用于云服务的相关文档下。 该规定同样适用于物理和基于网络的数据传输。 客户应就来自 SISW 分界点（例如：托管云服务的数据中心的出站防火墙）的任何数据传输承担责任。

5. 数据输入控制。 云服务允许就个人数据是否已从用于提供云服务的基础架构予以访问、修改或删除，或此类操作人员的确定展开回溯性认定。

措施：

a. SISW 仅允许授权人员访问其工作过程中所需的个人数据。 SISW 执行一个日志系统，以确保 SISW 或其辅助处理方可在云服务支持的最大限度内输入、修改及删除或拦截个人数据。
b. 如果已经或可能发生未经授权的活动，审计跟踪可提供促进事件重建的充足信息。 每一操作系统事件日志记录包括事件类型、时间标识、事件来源、事件地点、事件结果及与事件相关的用户。

6. 作业控制。 个人数据将仅根据本协议条款和客户提供的任何相关指示进行处理。

措施：

a. SISW 将执行相关控制和流程，以确保遵守 SISW 和其客户、辅助处理方或其他服务提供商之间所订立的合同。
b. 客户数据将受到不低于 SISW 信息分类标准下适用于保密信息同等水平的保护。
c. 所有 SISW 员工和合作伙伴必须尊重所有敏感信息的保密性，包括 SISW 客户和合作伙伴的商业秘密，且这一规定具有合同性约束力。

7. 可用性控制。 个人数据将受到保护，以防意外或未经授权的损毁或损失。

措施：

a. SISW 采用备份流程和其他措施，以在必要时确保业务关键系统的快速恢复。
b. SISW 依赖于全球云服务提供商，以确保数据中心的电力供应。
c. SISW 已针对云服务制定应急计划及业务和灾难恢复策略。

8. 数据分离控制。 收集用于不同目的的个人数据可分开处理。

措施：

a. 在适用时，SISW 将利用所部署软件（例如：多租户或分离系统蓝图）的技术性能，以完成客户和任何其他客户个人数据之间的数据分离。
b. SISW 针对每一客户维护专用实例（具有逻辑或物理分离）。
c. 客户（包括其关联公司）仅有权访问其自身的客户实例。

9. 数据完整性控制。 确保处理活动过程中个人数据是完好、完整及最新的：

措施： SISW 在多个层面实施防御策略，以防未经授权的修改。 其指代上述控制和措施章节所述的控制措施。防火墙配置将形成分离公共和私人访问的多个网络段。 每一防火墙规则集将具有特定的访问控制，以指明不同网络段之间允许的通信。

a. 安全监控中心： 自动化入侵检测软件将配合使用其他安全预防和取证软件和流程，以就任何安全突发事件进行预告、调查，并在需要时发出通知并协助补救。
b. 杀毒软件：所有系统将具有最新防病毒配置，以防病毒、蠕虫、木马及其他形式的恶意软件。
c. 备份和恢复：所有系统均达到数据和配置备份快照的基础水平。 在适用时，SISW 及其辅助处理方也将运行具有高可用性配置的客户实例，其将确保数据存储于两个相互间具有充分距离的独立数据中心。
d. 定期外部审计用以验证安全措施。 SISW 及其辅助处理方将定期进行外部审计，以检测上述安全措施。