SIEMENS

MindSphere 数据隐私条款

2020 年 7 月

1. 目的、范围及术语

1.1. 本数据隐私条款（**"DPT"**）为贵方与我方之间的委托数据处理协议，且适用于我方作为处理者或子处理者为贵方提供的涉及个人数据处理的所有服务。

1.2. 本数据隐私条款描述了与本数据隐私条款制约的服务相关的我方与贵方与数据保护相关联的所有权利和义务。其他权利和义务应独家遵循 MindSphere 协议的其他部分的规定。

1.3. 如适用的数据保护法有此要求，则贵方应和所有的贵方的授权实体签订数据处理协议，且应与本数据隐私条款的规定保持一致并遵循适用的数据保护法的要求。贵方应确保（亦包括贵方的授权实体），我方与我方的子处理者能够作为本数据隐私条款中所述的处理者和子处理者提供处理服务。

1.4. 本数据隐私条款中的大写术语由本文件第 13 条给出定义或由 MindSphere 协议其他部分赋予含义。

2. 我方提供的处理服务详情

2.1. 我方所提供处理服务的详细信息见本数据隐私条款附件 1，包括处理的范围、性质和目的以及已处理个人数据类型及受影响数据主体的类别。

2.2. 我们将根据 MindSphere 协议的条款（包括本数据隐私条款之规定）或贵方允许的其他条款处理个人数据。

2.3. 我方有权为遵循法律和/或政府命令而披露或授权我们的子处理者披露个人数据。如有此类请求，我方或子处理者将（i）将该请求主体重新引导至贵方，以便向贵方直接请求数据，我方可提供贵方的基本联系信息，以及（ii）及时通知贵方并提供该请求副本，除非法律或政府命令禁止我方如此作为。

3. 指示权

3.1. 作为处理者，我方仅遵从贵方书面指示行事。MindSphere 协议（包括本数据隐私条款）是贵方对我方作为贵方处理者进行个人数据处理的完整及最终指示。

3.2. 任何附加或替换指示必须经由双方书面同意且可能产生额外费用。

3.3. 若我方认为某指示违反了适用的数据保护法，我方将通知贵方。但我方无义务对贵方的指示进行任何法律审查。

4. 技术及组织措施

我们将实施本数据隐私条款附件 2 所述的技术及组织措施。贵方在此确认，我方提供的安全等级对于我方代表贵方处理数据时产生的固有风险而言，是适当的。贵方理解并同意，技术的进步及发展决定着所采用的技术和组织措施。因此，在保证措施安全等级的前提下，我方有权采取适当的替代措施。

5. 数据处理保密义务

我方将确保在该数据隐私条款下，涉及个人数据处理的人员均承诺负有保密义务。

6. 子处理者

6.1. 贵方特此批准我方聘用子处理者。我方委托的子处理者的目前名单见 www.mindsphere.io/terms。

6.2. 我方有权随时撤换或新增子处理者。如适用的数据保护法规定我方聘用新增子处理者须取得贵方批准，则我方将依照以下程序取得贵方批准：(i)如我方需授权新增子处理者访问贵方个人数据，则将提前至少 20 天通知贵方，采用的方式是向作为贵方订单订购程序之组成部分而提供给我方或此后与贵方账户相挂钩的电子邮箱发送消息，或授予贵方访问上文第 6.1 条所指网站的权利，该网站列示了目前所有的子处理者，并告知贵方获取关于新增子处理者通知的方法；(ii)如贵方没有在上述 20 天期限内提出合理的反对意见并书面说明不予批准的理由，则视为贵方批准聘用该新增子处理者；(iii)如贵方在上述期限内提出合理的反对意见，则我方将在授权该新增子处理者访问贵方个人数据前做出合理的努力：(a) 建议变更贵方对服务的配置或使用，以避免贵方所反对的新增子处理者处理个人数据，或(b) 提出其他措施，以解决贵方反对意见涉及的问题；(iv)如我方提出的变更或措施不足以消除贵方不予批准的理由，贵方有权在我方对贵方的反对予以回应后提前 10 天通知我方终止受影响的服务。如贵方终止受影响的服务，则我方对于贵方就该服务预付的款额，将按剩余期间在整个订阅有效期所占的比例予以退还。如贵方没有在上述 10 天期限内终止受影响的服务，则视为贵方已批准聘用新增子处理者。

6.3. 我方有权紧急更换子处理者。该等情形下，如果适用的数据保护法有此要求，我方将及时向贵方通知该紧急更换事项，贵方接到通知后应按第 6.2 条规定的批准程序予以批准。

6.4 如委托任何子处理者，根据适用的数据保护法的要求，我方将与该子处理者签订一份协议，对子处理者规定适当的合同义务，且该义务的保护性不低于本数据隐私条款中的义务。我方对我方的子处理者的任何行为或疏忽负责，负责方式等同于我方自身在本条款下的行为和疏忽。

7. 传输给非欧洲经济区接收者

7.1. 如果从位于欧洲经济体、瑞士或英国的控制者处向非欧洲经济区接收者的传输控制者个人数据，我们将执行 www.mindsphere.io/terms 载明的子处理者名单上与相应子处理者相对应的传输保护措施。贵方应负责评估我方执行的这些传输保护措施是否足以使贵方或贵方的授权实体遵循了适用的数据保护法。

7.2. 如某项传输保护措施是基于欧盟示范合同，则适用下述规定：西门子股份公司与相应子处理者签订该欧盟示范合同。每份欧盟示范合同都应含有贵方和被授权实体同意加入该合同的权利。贵方特此同意（作为数据输出者）与现有子处理者加入欧盟示范合同，并同意：贵方将来依照第 6.2 条批准新增子处理者，即应视为贵方宣布同意与该新增子处理者加入欧盟示范合同。而且，贵方同意确保每一位贵方的授权实体（同样作为数据输出者）加入该欧盟示范合同。我方（同时代表相应子处理者）特此说明，贵方无需将贵方或贵方的授权实体宣布加入欧盟示范合同的事项通知我方。

7.3. 如某项传输保护措施是基于 BCR-P，则适用下述规定：对于依照本数据隐私条款处理的个人数据，我方将以合同方式约束相关子处理者遵守 BCR-P。

8. 修正与删除

8.1. 我方将自行决定：或者（i）通过服务功能为贵方提供修正或删除个人数据的能力，或（ii）按照贵方的指示修正或删除个人数据。若需贵方或贵方的授权实体支持，贵方应提供所有必要支持，并获得相应授权实体的支持，以便我方履行该义务。

8.2. MindSphere 协议终止后，我方将删除或匿名化存储于平台的贵方个人数据，除非我方依法被要求保留相关数据。贵方确认，贵方的部分个人数据将作为平台灾难恢复备份而被我方保留，直至根据我方政策将相关文件删除。

9. 个人数据外泄

如有任何个人数据外泄情形，我方将在发现后及时通知贵方。我方将（i）与贵方合理配合，对数据泄露事件展开调查；（ii）向贵方提供合理支持，帮助贵方履行适用的数据保护法（如适用）下的安全漏洞通告责任；以及（iii）启动相应的合理补救措施。

10. 进一步通知

10.1 我方将及时通知贵方以下信息：（i）根据本数据隐私条款处理的个人数据的数据主体的投诉或请求（如关于个人数据处理的更正、删除和限制）；或（ii）主管数据保护机构或法院下发的关于本数据隐私条款下关于个人数据处理的命令或请求。

10.2 基于贵方请求，我方在合理范围内支持贵方：(i)处理上文第 10.1 条描述的投诉、请求或指令（特别是履行贵方对请求行使数据主体的权利给予回应的义务），或 (ii)履行贵方作为适用的数据保护法下控制者的义务（例如实施数据保护影响评估的义务）。基于该种支持占用的时间和材料，贵方应给予相应的补偿。

11. 审计

11.1. 贵方有权依照下文第 11.2 至 11.5 条的规定，以适当方式每年对我方及我方子处理者就遵守本文件项下数据保护义务的情况进行审计（尤其是我方实施的技术和组织措施），除非根据适用的数据保护法有必要进行其他额外审计；此类审计仅限于与向贵方提供服务相关的信息及数据处理系统。

11.2. 我方及我方子处理者可以聘用（内部或外部）审计师进行审计，以验证我方是否履行本文件项下的数据保护义务，特别是是否符合数据隐私条款第 4 部分采取技术及组织措施的要求。每次审计都会形成审计报告（例如，“服务组织管理 1，II 类报告”及“服务组织管理 2，II 类报告”）。由我方或我方子处理者提供的管理标准和框架，将根据监管或认证机构针对所有适用的管理标准或框架制定的标准和规则进行审计。

11.3. 贵方同意由我方提供的审计报告及相应信息（并称为**“审计报告”**）应当首先用于解决贵方在该数据隐私条款下的审计权利。应贵方要求，我方应提供服务相关的审计报告。

11.4. 若贵方能够证明我方提供的审计报告不足以使贵方或授权实体遵守适用的数据保护法下适用的审计要求和义务，则贵方或相关授权实体应详细说明所需进一步的信息、文件或支持。我方应在合理期限内提供此类信息、文件、或支持，费用应由贵方承担。

11.5. 审计报告及审计期间提供的任何补充信息及文件均为保密信息，且仅可根据实质上等同于 MindSphere 协议中所规定的保

SIEMENS

密义务提供给授权实体。若审计与我方子处理者相关，则我方有权要求贵方及授权实体在发布贵方或授权实体可获得的审计报告及任何补充信息或文件之前直接与各子处理者签订保密协议。

12. 唯一联系人和责任

12.1 贵方是我方的唯一联系人，即使涉及到本数据隐私保护条款下的贵方的授权实体和用户的情形时亦是如此。

12.2 如本数据隐私条款或任何第 7 条中的传输保护措施（如欧盟示范合同）规定了控制者（包括除贵方外的其他控制者）对于我方和/或我方子处理者的权利，贵方应以自身的名义和/或代表其他控制者直接与我方联系，以便行使这些权利。如贵方就针对子处理者行使权利事宜与我方联系，贵方须授权我方代表贵方或相应控制者对该子处理者行事。我方有权拒绝除贵方外的其他控制者直接向我方提出的请求、指示或权利主张。

12.3 如本数据隐私条款或任何传输保护措施中包含了针对控制者的通知义务，我方将该等通知提供给贵方，即解除我方通知控制者的义务 。

12.4 在不损害数据标的的法定权利的情形下，MindSphere 协议中规定的责任限制应同样适用于我方以及我方的子处理者针对贵方和贵方授权实体在本数据隐私条款（和任何第 7 条规定的传输传输保护措施）下的责任（应共同作为整体计算）。

12.5 贵方应确保上述第 12.1 至 12.4 条包含的限制可由我方和我方的子处理者针对贵方授权实体进行实施。

13. 定义

13.1.“适用的数据保护法”指所有与此处个人数据处理相关的可适用的法律。

13.2. “授权实体”指（i）贵方的关联方，（ii）在 MindAccess IoT Value 特定条款中界定的贵方 OEM 客户，或（iii）其他通过贵方的指定账户有权访问和使用服务或雇佣有权访问和使用服务的用户的其它法律实体。

13.3. “对处理者有约束力的公司准则”或“BCR-P”指根据 General Data Protection Regulation (EU) 2016/679 第 47 条批准的对处理者有约束力的公司准则。

13.4.“控制者”指单独或与其它方共同决定个人数据处理目的及方法的自然人或法人。

13.5. “经认定的对个人数据充分保护国家”是指欧盟委员会认定的欧洲经济区范围外对个人数据给予充分保护的国家。

13.6.“数据主体”指已被识别的或可识别的自然人。

13.7. “**DPT**”指本数据隐私条款。

13.8. “EEA”是指欧洲经济区。

13.9. “欧盟示范合同”是指根据欧盟委员会 2010 年 2 月 5 日通过的 2010/87/EU 号决定或其后继文件确定的关于向第三国处理者传输个人数据的格式合同条款。

13.10. “紧急替换”是指子处理者的短期替换。这在以下情况下是十分必要的：（i）当遇到超出我方合理控制范围的事件时；（ii）为了持续提供服务（例如子处理者意外停止业务、突然停止向我方提供服务或违反与我方的合同义务）。

13.11. “个人数据”指与一位数据主体直接或间接相关的信息，包括但不限于，姓名、电子邮件地址、邮寄地址、身份证号、位置数据、在线识别或有关某人身体、生理、遗传、心理、经济、文化或和社会身份的一个或多个特定因素。基于本数据隐私条款之目的，个人数据是指仅包括贵方或任何授权实体输入的或通过使用本服务衍生的个人数据，即个人数据是贵方内容的一个子集，且适用于任何此处使用的数据保护法。

13.12. “个人数据外泄”指因违反安全规定导致本数据隐私条款下的被处理的个人数据被意外或非法销毁、丢失、更改、未经授权披露或访问。

13.13. “处理者”指代表一位控制者处理个人信息的自然人或法人，公共机关、机构或其他实体。

13.14. “处理”指无论通过自动化方式与否，任何根据个人数据或个人数据集进行的操作或一组操作。例如收集、记录、组织、结构、存储、改写或修改、检索、咨询、使用、通过传输披露、散播或以其他方式提供、校准或组合、限制、删除或销毁、访问、转移和清理。

13.15.“子处理者”指任何由我方根据本数据隐私条款为提供服务而聘用的有权访问个人数据的其它的处理者。

13.16.“特殊类别个人数据”指能显示出种族、民族、政治观点、宗教或哲学信仰，工会会员、社会保险措施、行政或刑事诉讼和制裁信息，或能够单独识别出某个自然人的基因数据、生物特征数据、健康数据或某个自然人的性生活或性取向的数据。

13.17.“传输保护措施”是指(i)(欧盟）2016/679 号文件《通用数据保护条例》第 45 条所指的对个人数据充分保护国家的认定，或 (ii)(欧盟）2016/679 号文件《通用数据保护条例》第 46 条规定的适当保护措施。

SIEMENS

13.18.“向非欧洲经济区接收者的传输”是指我方或我方任何子处理者(i)在欧洲经济区境外或经认定的对个人数据充分保护国家境外进行的个人数据处理；或(ii)从欧洲经济区境外或经认定的对个人数据充分保护国家境外进行的对个人数据的访问。

SIEMENS

数据隐私条款之附件 1

如果某个特定的服务有需要，双方可在订单内详述服务细节，或我方可在适用的交易文件中提供更多详细信息。

处理操作

我方与我方的子处理者将按以下方式处理个人数据：

- 提供服务
- 在与提供服务相关联的数据中心提供个人数据存储和备份（多租户架构）

数据主体

所处理的个人数据涉及以下数据主体类别：

数据主体包括雇员、承包商、业务伙伴或个人数据存储在平台上的其他个人。

数据类别

所处理的个人数据涉及以下个人数据类别：

所处理的与服务相关的个人数据类别由贵方、贵方的授权实体和用户决定。所处理的个人数据和内容中包含的个人数据可能包括：姓名、电话号码、电子邮件地址、时区、地址数据、系统访问/使用/授权数据、以及包含个人数据的系统日志文件或任何其他用户进入服务的专用数据。

（如果属于）特殊类别个人数据

服务没有处理特殊类别个人数据的意向，贵方与贵方的授权实体不得直接或间接向我方传输任何此类敏感个人数据。

SIEMENS

数据隐私条款之附件 2

某些服务可能受到不同或其它技术和组织安全措施的保护(TOMs)，如各订单或适用的交易文件中所述。在所有其他情况下，应适用我方和/或我方的子处理者实施的如下技术和组织安全措施(TOMs)。

除属于贵方责任范围内的下述技术和组织安全措施外，贵方应自行负责实施其他安全措施，例如在贵方场所或对资产执行现场准入和系统访问控制措施，或根据贵方具体要求配置服务。

1. 现场和环境安全

我们采取适当措施，防止未经授权的人士进入数据处理设备（即，数据库和应用服务器及相关硬件）。这应通过以下方式实现:

a) 建立安全区域；

b) 保护和限制访问路径；

c) 保护分散的数据处理设备和个人计算机；

d) 为员工和第三方建立访问授权，包括各自的文档；

e) 门禁卡规定；

f) 门禁卡限制；

g) 对托管个人数据的数据中心的所有访问都将进行记录、监控和追踪；

h) 对托管个人数据的数据中心通过受限制的访问控制和其他适当的安全措施进行安全保护；和

i) IT 区域和数据中心的配套设备的维护和检查只能由授权人员进行。

2. 访问控制（IT 系统和/或 IT 应用）

2.1 我们实施角色和职责的概念。

2.2 我们实施授权及认证架构，包括但不限于以下要素:

a) 实施基于角色的访问控制；

b) 账户创建、修改、删除的实施过程；

c) IT 系统和应用的访问受认证机制保障；

d) 根据 IT 系统或应用的特点和技术方案而采用适当的认证方法；

e) 访问 IT 系统和应用至少需要对特权帐户进行双重认证；

f) 记录、监控和追踪所有对个人数据的访问；

g) 实施 IT 系统和应用（包括允许或拒绝入站网络连接的防火墙）的入站网络连接的授权和日志记录措施；

h) 对 IT 系统、应用程序和网络服务的特权访问权应只授予需要其完成自身任务的个人（最低限度特权原则）；

i) 对 IT 系统和应用程序的特权访问权应由文件记录并保持最新；

j) 定期审查和更新对 IT 系统和应用程序的访问权限；

k) 实施密码政策，包括要求重新设定密码的复杂程度、密码的最短长度和足够期限后的有效期，不重复使用最近使用过的密码；

l) IT 系统及应用在技术上实施密码政策；

m) 员工和外部人员对 IT 系统和应用的访问权限在雇佣关系或合同终止后立即被移除；和

n) 使用最先进的安全认证证书。

2.3 IT 系统和应用程序在超过合理定义的闲置时间限制后自动锁定或终止。

2.4 我们将对云资产的特权访问限制为单个或特定范围的 IP 地址。

2.5 通过 bastion 主机对云资产进行特权访问。

2.6 我们维持 IT 系统的登入程序，以防止可疑的登入活动（例如，防止暴力破解和密码猜测攻击）。

3. 可用性控制

3.1 我们通过实施适当和先进的反恶意软件解决方案，保护系统和应用程序免受恶意软件的侵害。

3.2 我们为 IT 系统定义、记录及实施备份概念，包括下列技术及组织要素：

a) 备份存储介质受到保护，防止未经授权的访问和环境威胁（如高温、潮湿、火灾）；

b) 定义备份间隔；和

c) 根据 IT 系统或应用程序的临界性，定期对备份数据的恢复进行测试。

3.3 我们将备份存储在与生产系统所在位置不同的物理位置。

3.4 非生产环境中的 IT 系统和应用程序与生产环境中的 IT 系统和应用程序在逻辑上或物理上是分离的。

3.5 存储或处理个人数据的数据中心应受到保护而免于遭受自然灾害、物理攻击或事故。

3.6 IT 领域和数据中心的支持设备，如电缆、电力、电信设施、供水或空调系统，应受到保护而免于遭受干扰和未经授权的操控。

4. 运行安全

4.1 我们维持及实施一个定期检查及更新的信息安全架构。

4.2 我们会记录与安全有关的事件，例如用户管理活动（例如:建立、删除）、登入失败、IT 系统及应用系统的安全配置变更。

4.3 我们持续分析各自的 IT 系统和应用的反常、异常、危害指标和其他可疑活动的日志数据。

4.4 我们会定期扫描及 IT 系统及应用系统的安全漏洞。

4.5 我们为 IT 系统及应用系统实施及维护一个变更管理流程。

4.6 我们维护一个流程来更新和实施供应商对各自 IT 系统和应用程序的安全补丁和更新。

4.7 在处理或重用 IT 系统之前，我们将彻底地删除数据或物理性地销毁数据存储媒体。

SIEMENS

5. 传输控制

5.1 我们定期记录和更新网络拓扑及其安全需求。

5.2 我们会通过以下内容持续及有系统地监测 IT 系统、应用系统及相关网络范围，以发现恶意及异常的网络活动：

a) 防火墙（如有状态防火墙、应用程序防火墙）；

b) 代理服务器；

c) 入侵检测系统(IDS)和/或入侵预防系统(IPS)；

d) URL 过滤；和

e) 安全信息和事件管理(SIEM)系统。

5.3 我们使用最先进的加密连接来管理 IT 系统和应用程序。

5.4 我们通过最先进的网络协议，如 TLS，在传输过程中保护内容的完整性。

5.5 我们加密或使您能够加密通过公共网络传输的您的数据。

5.6 我们使用安全密钥管理系统（KMS）在云中存储密钥。

6. 安全事件

我们维持并实施事件处理流程，包括但不限于：

a) 安全违规记录；

b) 客户通知流程；和

c) 事件响应计划，以便在事件发生时处理以下事项：（i）角色、职责，以及在妥协情况下的沟通和联系策略；（ii）特定的事件响应程序；和（iii）所有关键系统部件的覆盖和响应。

7. 资产管理、系统获取、开发和维护

7.1 在开发及获取新的 IT 系统及应用系统之前，以及改善现有的 IT 系统及应用系统之前，我们会先确定及记录信息安全的要求。

7.2 我们建立了一个正式的流程来控制和执行已开发应用程序的更改。

7.3 我们计划并把安全测试纳入 IT 系统及应用系统的开发周期。

7.4 我们实施适当的安全补丁程序，包括：

a) 监测组件的潜在弱点(CVEs)；

b) 修复的优先级；

c) 修复的及时实施；和

d) 从可靠的来源下载补丁。

8. 人力资源安全

8.1 我们在人力资源安全方面采取了以下措施：

SIEMENS

a) 有权查阅个人数据的员工受保密义务的约束；和

b) 可接触个人数据的员工定期接受有关适用的数据保护法律法规的培训。

8.2 我们针对员工和外部供应商实施相应的离职或终止流程。