关于 MindAccess IoT Value Plan 的特定条款

2019年3月

1. 范围

1.1. **范围**。本特定条款是 MindSphere 协议的组成部分。本特定条款仅在贵方使用 *MindAccess IoT Value Plan* 和相关服务允许第三方访问某些服务时适用，此等服务系第三方从贵方处获得的基于平台的服务的组成部分（该服务被称为**“OEM 服务”**）。贵方仅能在交易文件明确允许的前提下，允许用户访问作为贵方 OEM 服务部分的服务。从贵方处获得 OEM 服务的第三方被称为**“OEM 客户”**。

1.2. **定义。**本文件中大写术语以本特定条款或 MindSphere 协议赋予的含义为准。

2. OEM 服务的提供

2.1. **使用权**。在遵循本特定条款诸项限制性规定的前提下，我们授予贵方允许 OEM 客户及其用户在贵方账户下为每一个 OEM 客户设置的子租户下访问和使用 OEM 服务的权利，这是一项不可转让、不可再许可、有时限、可撤销的权利（每个子租户都是一个**“OEM 子账户”**）。访问 OEM 服务的 OEM 客户的用户也是贵方的用户。贵方提供的 OEM 服务可以是无偿的，也可以是有偿的。对于我们向贵方提供的旨在接受检测和评估的服务，或“预发布”版、“beta 测试”版或“预览”版服务，如贵方拟允许 OEM 客户访问，必须事先取得我方同意。

2.2. **账户的设置与管理**。贵方负责设置、管理和配置为 OEM 客户及其用户访问 OEM 服务所必需的 OEM 子账户。贵方应为每个 OEM 客户设置并维护一个单独的 OEM 子账户。贵方只能允许 OEM 客户及其用户访问其指定的 OEM 子账户。贵方应确保 OEM 子账户仅用于向相应 OEM 客户及其用户提供 OEM 服务。

2.3. **OEM 客户的内容。**与使用 OEM 服务相关的信息或数据（**“OEM 客户数据”**）的采集、存储、处理、修改、披露或以其他方式的使用，贵方应通知 OEM 客户且应获得他们的同意（如果法律要求）。输入、上传或存储于平台的 OEM 客户数据是贵方内容的组成部分。我方提供将贵方内容的某些部分迁移到替代技术或第三方账户的服务，在此范围内，若贵方 OEM 客户请求贵方允许其就 OEM 客户数据接收此项迁移服务时，贵方应予允许。

2.4. **支持。**贵方独自负责向贵方 OEM 客户及其用户提供支持，不得让贵方 OEM 客户或其用户使用我们就服务向贵方提供的支持。

2.5. **营销。**贵方在营销和广告活动中应确保贵方，而不是阿里云或西门子，被称作为 OEM 服务提供商，但贵方可表明 OEM 服务利用了平台和服务。

3. 贵方与 OEM 客户的关系

3.1. **贵方的角色。**贵方承认并同意：（i）关于访问和使用 OEM 服务的任何合同关系仅限于贵方和 OEM 客户之间；且（ii）阿里云仅向贵方提供服务，不因 OEM 客户和/或其用户访问或使用 OEM 服务而对其承担任何义务或责任。贵方无权在法律交易中代表阿里云或西门子，也不得以任何方式约束他们。就提供 OEM 服务而言，贵方是独立主体，独自负责与营销和提供 OEM 服务有关的所有经济机遇和风险。贵方自行确定提供 OEM 服务的收费价格，独自负责与 OEM 客户有关的所有账单开具和收费事宜。

3.2. **OEM 合同。**贵方向并非贵方关联方的 OEM 客户提供 OEM 服务必须与其签订书面合同（**“OEM 合同”**）。贵方应确保 OEM 合同符合 MindSphere 协议，且对阿里云的保护力度不低于 MindSphere 协议的规定。贵方所签的 OEM 合同至少应包含本特定条款附件所列诸条款的基本内容（“最低限度条款”）。贵方应始终负责 OEM 合同的可执行性和实际执行，并确保其符合有关法律法规。贵方应确保 OEM 客户及其用户遵守最低限度条款。贵方发现 OEM 客户或其用户有不遵守最低限度条款的行为，应立即将这方面的情况以及贵方对其采取的行动通知我们。

3.3. **数据。**在法律有要求的情形下，贵方应与 OEM 客户达成关于处理和保护其数据（包括个人数据）的适当协议。贵方和 OEM 客户之间的该等协议应允许阿里云和西门子及其分包商处理贵方、OEM 客户及其用户的任何数据（包括个人数据）。

3.4. **OEM 合同的变更**。如 MindSphere 协议的某项变更致使 OEM 合同也要做相应变动以保持一致性，贵方应立即对 OEM 合同做出相应变动。

4. 记录与审计

4.1. **记录。**贵方应详尽记录 OEM 客户及其用户的数量和身份，并将该记录与所有 OEM 合同妥善保存。

4.2. **审计。**我们有权委派审查员在给予合理提前通知的前提下在正常营业时间内对贵方进行审查，以确定贵方是否履行了作为 OEM 服务提供商应履行的合同义务。审查员须对阿里云和第三方承担保密义务，仅向我们提供关于贵方是否履行相应义务的信息。贵方应：（i）向审查员提供为此项审查所必需的所有文档；（ii）允许审查员进入贵方场所并配合审查员进行有关调查；以及（iii）采取商业意义上正常合理的一切行动协助审查员进行审查。我方承担审查费用，除非在审查中发现贵方有重大违规行为，在这种情形下，审查费用由贵方承担。

附件一最低限度条款

1. **主题事项；范围**

1.1. **合同方**。本**最低限度条款**是由【此处填写贵方公司的名称和地址】（“**我们**”；“**我方**”或“**我们的**”）和贵方或代表贵方接受本条款的主体（“**贵方**”或“**贵方的**”）之间所达成。

1.2. **主题事项**。我方使用西门子专有的基于云的开放性物联网操作系统 MindSphere（“**平台**”）。本条款适用于贵方访问和使用平台以及基于平台的诸项服务，该等服务是我方使用平台向贵方提供服务的一部分（统称“**服务**”）。

1.3. **合同关系。**关于访问和使用服务的任何合同关系仅限于贵方和我方。我方负责提供服务和相关支持。本条款不构成阿里云或西门子对贵方的任何义务。与服务有关的任何问题、投诉或索赔应发送到【此处填写贵方公司的名称和地址、电话号码和电子邮箱】。

1.4. **第三方受益人。**就本条款而言，阿里云和西门子系第三方受益人，有权代表我方并以阿里云或西门子自身的名义为阿里云或西门子的利益对贵方执行这些条款。而且，针对贵方的陈述、保证、赔偿和责任的所有限定同样适用于阿里云和西门子以保障其利益。

1.5. **定义**。本文件中某些大写术语，参见本条款第 8 条的规定；其他大写术语，也以本条款规定的含义为准。

2. **服务的提供**

2.1. **服务的访问与使用**。我方授予贵方通过贵方账户访问和使用服务的权利，这一权利是不可转让、不可再许可、有时限且可撤销的。

2.2. **贵方账户**。我方允许贵方使用我方向贵方提供的访问凭证通过相应账户访问和使用服务。该访问凭证仅对贵方指定的用户有效，且与其有效的电子邮箱相挂钩。一个访问凭证只对一个用户有效，且只能由一个用户使用。

2.3. **访问凭证**。贵方应确保贵方和所有用户：(i)谨慎保存访问凭证，防止他人擅自使用；(ii)只能通过贵方账户或我方允许的其他方式访问服务，不得用除此以外的任何方式；(iii)不得规避针对贵方账户、平台或与平台有关的主机、网络或账户的认证或安全措施，也不得对其进行披露；(iv)不得使用虚假身份或他人的访问凭证对贵方账户、平台或服务进行访问；和(v)任何凭证仅供被授予该凭证的人士使用。

3. **贵方义务**

3.1. **服务的使用。**贵方应始终遵守法律和可接受使用政策，可接受使用政策随附在本条款后或者贵方也可从【此处插入贵方链接】下载。

3.2. **更新。**对于我方或阿里云向贵方提供的作为服务组成部分的软件，贵方应始终保持更新，安装可供适用的更新和补丁。贵方自行负责贵方系统以及现场硬件和软件的安全。

3.3. **使用监测**。贵方承认：阿里云、西门子或代表阿里云的第三方有权为阿里云或西门子的内部业务需要而监测贵方在平台上对服务的使用情况（如用户数和存储容量）。西门子还可在汇总的基础上（且仅在此基础上）使用该信息改善西门子及其分包商的产品和服务。西门子、阿里云和我方有权在贵方使用服务可能违反法律法规的情形下出于报告目的而向第三方披露贵方的内容。

3.4. **高风险系统**。贵方承认并同意：尽管存在高风险系统运行有赖于某项服务正常运行的情形，但服务并不是为了用于高风险系统的运行或在高风险系统中运行而设计的。

4. **条款变更**

我们将通过提前通知的方式变更本条款，该等通知至少在本条款更新版本生效前【30】天告知贵方，且通知中将载明本条款更新版本生效的时间。

5. **数据隐私**

双方应遵守关于保护个人数据的法律法规。

6. **专有权利**

6.1. **平台和西门子服务中的专有权利**。对平台和阿里云提供并由我方将其作为服务组成部分加以利用的任何服务以及它们的任何部分和其改进所涉及的所有权利、所有权、利益和技术诀窍，以及它们所含的知识产权，完全属阿里云、西门子或其第三方业务伙伴和/或许可方所有。

6.2. **贵方内容中的权利**。贵方授予我方和我方业务伙伴（包括阿里云和西门子）为向贵方提供服务而使用、托管、存储、传输、展示、修改和复制贵方内容的权利，且该权利是全世界范围的、非排他性、可转让、可再许可且免许可费。

7. **遵守出口管控与制裁法律**

7.1. **出口与制裁法律。**贵方同意遵守一切有关的制裁（包括禁运）和出口（包括再出口）管控的法律法规，包括德意志联邦共和国、欧盟和美国（所有适用的）有关规定（统称“**出口与制裁法律**”）。

7.2. **贵方义务。**贵方有义务：(i)拒绝并阻止根据出口与制裁法律规定所禁止或受到制裁或需要许可的地点对服务的访问；(ii)持续性地对照相应的制裁名单核查用户；(iii)不得向制裁名单中列明的包括用户在内的任何个人或机构授予访问平台或服务的权利；以及（iv）确保贵方内容在有关国家/地区不属于管控数据或技术数据，举例来说，在欧盟或德国，相应等级为 AL = N，而在美国，相应等级为 ECCN = N 或 EAR99。

7.3. **信息要求**。在贵方有责任配合有关机构或我方进行出口管控或制裁方面的合规性核查情形下，贵方应按我方要求，立即向我方提供与特定目的地、最终用户和我方所提供服务特定用途有关的所有信息，包括关于贵方和用户的信息。

7.4. **履约保留权**。如有关国家或国际性的外贸或海关法规、禁运或其他制裁措施致使本条款无法履行，则我方不承担任何履行义务。贵方进一步承认我方有义务根据适用于我方的出口与制裁法律限制或暂停贵方和用户对服务的访问。

8. **定义**

8.1. “**阿里云**”是指阿里云计算有限公司，也包括其直接或间接拥有或控制的所有公司和其他法律实体、直接或间接拥有或控制其的所有公司和其他法律实体或与其处于同一实体控制下的所有公司和其他法律实体。此处“控制”是指直接或间接拥有的对某公司或其他实体作出或使其作出管理和决策的权力。

8.2. **“高风险系统”**是指在合理范围内可预见其故障有可能直接导致死亡、人身伤害或灾难性的财产损害因而需要加强安全功能（例如故障保护或容错性）的设备或系统。有必要配备高风险系统的领域包括但不限于关键性基础设施、直接性健康支持设备、航空器、火车、船舶、车辆导航或通信系统、空中交通管制、武器系统、核设施、发电厂、医疗系统和医疗设施、交通运输设施。

8.3. “**法律**”是指法律、法规、规定、规范和命令，包括但不限于针对特定行业或企业的规定，以及劳资委员会决策、数据隐私保护、通信、能源、IT 安全、出口管控、制裁和机密信息保护方面的法律法规。

8.4. “**西门子**”是指西门子股份公司（德国），也包括其直接或间接拥有或控制的所有公司和其他法律实体、直接或间接拥有或控制其的所有公司和其他法律实体或与其处于同一实体控制下的所有公司和其他法律实体。此处“控制”是指直接或间接拥有的对某公司或其他实体作出或使其作出管理和决策的权力。

8.5. “**用户**”是指贵方允许在贵方账户下访问和使用诸项服务的一方。

8.6. “**贵方内容**”是指贵方或在贵方账户下使用服务的用户在使用服务过程中输入、上传或存储于平台的任何信息、程序、软件、应用、任何形式的代码、脚本、库或数据。

阿里云

可接受使用政策

2019 年 3 月

本可接受使用政策（“**政策**”）规定了贵方在使用我方服务时必须遵守的条款。

1. 定义

大写术语以适用于服务的本条款所赋予的含义为准。

2. 禁止贵方非法地、有害地或冒犯性地使用内容

贵方不得为非法、有害或冒犯性目的而使用服务，也不得鼓励、促动、提供便利或指示他人为非法、有害或冒犯性目的而使用服务。贵方内容不得有任何非法、有害或冒犯性的部分。特别地，贵方对服务的使用、贵方内容以及贵方对贵方内容的使用不得：

(i) 违反任何法律或侵他人的权利；

(ii) 不得损害他人利益，也不得损害阿里云的运营或声誉，包括不得提供或传播欺诈性的产品、服务、方案或推广，也不得提供或传播快速赚钱骗局、庞氏骗局或传销骗局、网络钓鱼、网址欺骗或其他欺诈活动；

(iii) 输入、存储或发送引导用户访问外部网站或数据槽的超链接，包括贵方内容中所含的贵方没有取得相应授权的或非法的内嵌微件或其他访问工具；

(iv) 含有诽谤、淫秽、侮辱性、侵犯隐私或其他令人反感的成分；

(v) 将阿里云或其业务伙伴（包括西门子）置于责任负担下的情形。

3. 禁止违反使用限制

贵方不得：

(i) 向任何第三方全部或部分复制、出售、转售、许可、转移、转让、分许可、出租、租赁或以其他方式提供服务或平台（除非我方允许或法律有此规定）；

(ii) 编译、拆解、反编译、逆向工程或以其他方式变动、篡改、修复或试图发现服务或平台所含软件的源代码（除非我方同意或法律有此规定）；

(iii) 利用服务或平台的任何部分或在此基础上创制衍生作品；

(iv) 改动或清除服务或平台中对知识产权或品牌名称的提示或标记；以及

(v) 模仿阿里云网站或其他用户界面的界面外观，或模仿与阿里云有关的品牌展示、色彩组合、字体、平面设计、产品图标或其他要素；和

(vi) 将受限于某项许可的贵方内容上传到平台，且该许可规定，作为使用、访问和/或修改该内容的条件，阿里云提供的与贵方内容交互或与其托管于同一主机的阿里云或西门子业务伙伴的软件或服务应：(a)以源代码形式披露或传播；(b)许可接收者用来创制衍生作品；(c)无偿许可；(d)不得用于商业目的；或(e)受到任何方式的制约。

4. 禁止滥用

贵方不得：

(i) 以试图避免或规避某项服务使用限定与限制的方式使用该服务，例如规避访问和存储的限制或避免招致收费；

(ii) 访问或使用服务进行性能检测，研制竞争性产品或服务，或拷贝其特征或用户界面，或在业务流程外包、其他外包或分时服务运营中使用服务；

(iii) 干扰阿里云系统的正常运行，包括通过邮件“轰炸”、新闻“轰炸”、播放“攻击”或“泛洪”技术加重系统负荷，使其不堪重负；

(iv) 从事某种活动、修改或试图修改平台或服务从而对平台或服务性能造成负面影响。

5. 禁止违反安全规程

贵方不得以导致、允许、协助或提供便利对平台或服务安全构成威胁的行动的方式使用服务。特别地，贵方：

(i) 在访问服务前、使用过程中和传输贵方内容时，采取一切合理的预防措施，包括预防病毒、特洛伊木马或其他有可能损害软件的程序的措施，以保护贵方用来连接到和/或访问平台的贵方系统、现场硬件、软件或服务免受攻击；

(ii) 不得干扰或破坏服务或连接到平台的其他设备或网络的完整性或性能，特别是不得传输贵方内容中含有病毒、特洛伊木马或其他有可能损害软件的程序的部分；

(iii) 不得以有可能损害阿里云系统或其安全性或致使其丧失功能、造成过重负担、受到削弱或破坏的方式使用服务，也不得以有可能干扰平台的其他用户的方式使用服务；

(iv) 未经我方事先明示书面同意，不得对服务或平台进行任何渗透测试，也不得在服务或平台上进行任何渗透测试；和

(v) 不得将不符合行业标准安全政策（如密码保护、病毒防护、更新和补丁等级）的设备连接到服务。

6. 报告

贵方觉察到违反本政策的行为，应立即通知我方，并应我方要求向我方提供旨在阻止、减轻或纠正该违规行为的协助。