

## IBM MaaS360 (SaaS)

本“服务描述”描述 IBM 向客户提供的 Cloud Service。客户表示公司、公司授权用户和 Cloud Service 接收方。提供适用的“报价”和“权利证明”(PoE) 作为独立的交易文档。

### 1. Cloud Service

MaaS360 是一种易于使用的云平台，具有以端到端方式管理目前使用 iOS、Android、Windows 和 Blackberry 操作系统的移动设备所需的全部基本功能。以下是 Cloud Service 产品的简要描述：

#### 1.1 IBM MaaS360 Mobile Device Management (SaaS) 和 IBM MaaS360 Mobile Device Management (SaaS) Step up for existing customers

核心移动设备管理 (MDM) 功能包括设备注册、配置、安全策略管理和设备操作，例如，发送消息、定位、锁定和擦除。高级 MDM 功能包括自动化合规性规则、自带设备 (BYOD) 隐私设置以及 Mobility Intelligence 仪表板和报告。

#### 1.2 IBM MaaS360 Mobile Application Management (SaaS) 和 IBM MaaS360 Mobile Application Management (SaaS) Step up for existing customers

MaaS360 Mobile Application Management 能够添加应用程序，并向 MaaS360 管理的受支持设备分发这些应用程序。这包括 MaaS360 App Catalog (设备上的应用程序)，供用户查看、安装以及提醒更新的受管应用程序。

#### 1.3 IBM MaaS360 Mobile Application Security (SaaS) 和 IBM MaaS360 Mobile Application Security (SaaS) Step up for existing customers

MaaS360 Mobile Application Security 为开发期间使用 WorkPlace SDK 的企业应用程序提供额外的数据保护，或者对于 iOS 应用程序提供以下功能：上传应用程序 (.ipa)、配置概要信息和签署证书，以实现自动集成。Mobile Application Security 将应用程序与 Productivity Suite 集成。这支持单点登录、通过 Mobile Enterprise Gateway 的内部网访问以及数据安全设置实施。

#### 1.4 IBM MaaS360 Gateway for Apps (SaaS) 和 IBM MaaS360 Gateway for Apps (SaaS) Step up for existing customers

MaaS360 Gateway for Apps 为企业网络之外的用户提供内部应用程序资源的无缝访问路径，无需完整的设备 VPN 连接。

#### 1.5 IBM MaaS360 Mobile Content Management (SaaS) 和 IBM MaaS360 Mobile Content Management (SaaS) Step up for existing customers

MaaS360 Mobile Content Management 支持管理员向 IBM MaaS360 Mobile Device Management 管理的受支持设备添加和分发文档。其中包含 IBM MaaS360 Doc Catalogue，这是一种设备上的使用密码保护的容器，为用户提供一种安全且简单的方式来访问、查看和共享文档。包括无缝访问分布式内容和存储库，例如，SharePoint、Box 和 Google Drive。可以通过 MaaS360 Gateway for Documents 访问私有 SharePoint 和 Windows 文件。通过 MaaS360 管理的文档可使用数据丢失保护 (DLP) 策略选项（例如，需要认证、限制复制粘贴功能，以及阻止在其他应用程序中打开或共享）进行版本控制、审计和保护。

#### 1.6 IBM MaaS360 Mobile Document Sync (SaaS) 和 IBM MaaS360 Mobile Document Sync (SaaS) Step up for existing customers

MaaS360 Mobile Document Sync 使用户能够同步各个受管移动设备上的用户内容。管理员可以确保对于不同设备上的用户内容实施策略，例如，限制剪切/复制/粘贴，以及阻止在其他应用程序中打开或共享内容。内容安全地存储在云和设备上，只能通过 MaaS360 Doc Catalogue 进行访问。

## 1.7 IBM MaaS360 Mobile Document Editor (SaaS) 和 IBM MaaS360 Mobile Document Editor (SaaS) Step up for existing customers

MaaS360 Mobile Document Editor 是一种强大的办公套件，支持用户随时随地处理业务文档。MaaS360 Mobile Document Editor 支持：

- 创建和编辑 .DOC、.PPT 和 .XLS 文件。
- 幻灯片的演示模式
- 能够方便地处理电子邮件附件以及来自 MaaS360 for iOS 的其他文件。

## 1.8 IBM MaaS360 Gateway for Documents (SaaS) 和 IBM MaaS360 Gateway for Documents (SaaS) Step up for existing customers

利用 MaaS360 Gateway for Documents，企业可以使用 MaaS360 Mobile Content Management 为企业网络之外的设备额外提供对内部 Connections 站点、SharePoint 站点、Windows 文件共享以及其他文件存储的无缝访问，无需完整的设备 VPN 连接。要使用 MaaS360 Gateway for Documents，还需要购买 MaaS360 Mobile Content Management。支持 iOS 5.0 和 Android 4.0 或更高版本。

## 1.9 IBM MaaS360 Email Management (SaaS) 和 IBM MaaS360 Email Management (SaaS) Step up for existing customers

MaaS360 Email Management 包含支持 Microsoft Exchange ActiveSync 和 Lotus Traveler 的重要功能。

- Exchange ActiveSync: 支持移动设备通过 ActiveSync 协议连接到 Microsoft Exchange。包含核心移动设备管理功能，例如配置设备；创建、实施 ActiveSync 策略（验证码，阻止或允许访问电子邮件）；执行设备操作，例如，锁定和擦除；以及设备属性的详细报告。
- Lotus Traveler: 支持移动设备通过 Lotus Traveler 协议连接到 IBM Lotus Notes®。包含以下功能：配置设备；阻止或允许设备；实施验证码策略；擦除设备以及生成有关设备属性的详细报告。

## 1.10 IBM MaaS360 Secure Mobile Browser (SaaS) 和 IBM MaaS360 Secure Mobile Browser (SaaS) Step up for existing customers

MaaS360 Browser 是功能齐全的 Web 浏览器，通过定义网站过滤和安全策略，允许对企业内部网站点的访问，实施内容合规策略，确保用户只访问根据一系列内容类别（例如，社交网络、明确规定的站点或恶意站点）批准的 Web 内容。功能包括通过应用程序策略或黑名单（与 MobileFirst Protect Devices 组合使用时），禁用本机和第三方 Web 浏览器。它支持 Web 站点的白名单例外；限制 Cookies；限制复制、粘贴和打印功能；以及启用自我服务方式。

## 1.11 IBM MaaS360 Gateway for Browser (SaaS) 和 IBM MaaS360 Gateway for Browser (SaaS) Step up for existing customers

MaaS360 Gateway for Browser 允许受支持的设备访问经过批准的内部 Web 站点，而无需完整的设备 VPN 连接。

## 1.12 IBM MaaS360 for BlackBerry (SaaS) 和 IBM MaaS360 for BlackBerry (SaaS) Step up for existing customers

通过使用 BlackBerry API，为 BlackBerry Enterprise Server (BES) 连接的移动设备提供支持。功能包括远程操作，例如，发送消息，重置验证码，指定 BES 策略和擦除，以及有关设备属性的详细报告。需要安装 MaaS360 Cloud Extender。仅可用于通过 BES 5.0 使用 MaaS360 查看或管理的设备。

## 1.13 IBM MaaS360 Mobile Expense Management (SaaS) 和 IBM MaaS360 Mobile Expense Management (SaaS) Step up for existing customers

MaaS360 Mobile Expense Management 支持管理员创建数据使用策略，并将这些策略分配给 MaaS360 管理的受支持设备，在设备、组或全局级别分配这些策略，针对网络和漫游数据使用配置警报阈值和消息传递。

#### **1.14 IBM MaaS360 Management Suite (SaaS) 和 IBM MaaS360 Management Suite (SaaS) Step up for existing IBM MaaS360 customers**

产品套件/捆绑产品，包括 MaaS360 Mobile Device Management、MaaS360 Mobile Application Management、MaaS360 Content Service 和 MaaS360 Mobile Expense Management。

#### **1.15 IBM MaaS360 Productivity Suite (SaaS) 和 IBM MaaS360 Productivity Suite (SaaS) Step up for existing customers**

产品套件/捆绑产品，包括 MaaS360 Secure Mobile Mail、MaaS360 Mobile Application Management、MaaS360 Mobile Application Security、MaaS360 Content Service 和 MaaS360 Secure Mobile Browser。

#### **1.16 IBM MaaS360 Secure Mobile Mail (SaaS) 和 IBM MaaS360 Secure Mobile Mail (SaaS) Step up for existing customers**

MaaS360 Secure Mobile Mail 提供单独的办公生产力应用程序，以供用户访问和管理电子邮件、日历和联系人，并且通过限制将内容转发或移动到其他应用程序，实施认证，限制剪切/复制/粘贴，锁定电子邮件附件以仅供查看，从而控制电子邮件和附件，避免数据泄露。

#### **1.17 IBM MaaS360 Gateway Suite (SaaS) 和 IBM MaaS360 Gateway Suite (SaaS) Step up for existing customers**

MaaS360 Gateway Suite 允许 iOS 和 Android 上受支持的应用程序无缝地与企业内部网络中的资源进行通信。

#### **1.18 IBM MaaS360 Content Suite (SaaS) 和 IBM MaaS360 Content Suite (SaaS) Step up for existing customers**

产品套件/捆绑产品，包括 MaaS360 Mobile Content Management、MaaS360 Mobile Document Editor 和 MaaS360 Mobile Document Sync。

#### **1.19 IBM MaaS360 Mobile Threat Management (SaaS)**

MaaS360 Mobile Threat Management 通过移动恶意软件检测和高级越狱/root 检测，提供增强的移动安全性。利用 MaaS360 Mobile Threat Management，客户能够围绕着检测到的恶意软件和其他安全漏洞设置和管理合规性策略。

#### **1.20 IBM MaaS360 Content Service (SaaS)**

MaaS360 Content Service (SaaS) 支持用户将应用程序包和文档上传到 MaaS360 Content Distribution 系统。

IBM MaaS360 为每位客户提供 1GB 的存储空间。IBM MaaS360 还为每台设备每年提供 6 GB 的带宽利用率，作为共享带宽池使用。整个带宽池在所有设备间共享。无论产品捆绑软件或行项目的购买量为多少，基本存储空间和带宽分配都不会增加。如果客户所需的数量超过了提供的基本数量，那么其应该购买额外的存储空间和/或带宽。

#### **1.21 IBM MaaS360 Content Service Storage (SaaS)**

MaaS360 Content Service Storage (SaaS) 支持用户购买可用于 MaaS360 Content Service (SaaS) 的数据存储总量。

#### **1.22 IBM MaaS360 Content Service Bandwidth (SaaS)**

MaaS360 Content Service Bandwidth (SaaS) 支持用户购买可用于 MaaS360 Content Service (SaaS) 的带宽总量。

#### **1.23 IBM MaaS360 Professional (SaaS)**

为中小型企业提供一种快速、简便的方式，远程配置智能手机和平板电脑、执行安全策略、推送应用程序和文档以及保护企业和个人设备的数据。客户可以为您的业务快速、轻松和实惠地获取合适的移动性管理功能。

## 1.24 IBM MaaS360 Laptop Management (SaaS)

为客户提供基于 OS X 和 Windows PC 的设备以及智能手机和平板电脑上的注册、配置、管理和报告的能力。组织可以在同一 MaaS360 管理控制台中企业和员工持有的设备间保持安全策略和概要信息一致。

### 1.24.1 Windows

MaaS360 Laptop Management (SaaS) for Windows-based PCs 提供了针对硬件、操作系统和软件信息的无线注册和库存管理报告功能。端点安全性报告模块为客户提供的应用程序（诸如防病毒、备份/恢复、数据加密和个人防火墙以及缺少的操作系统补丁等）提供交互式报告和数据分析功能。数据保护模块为安全服务（包括数据加密、防数据泄漏、备份/恢复及其他集成应用程序）提供交互式报告和分析功能。支持 Windows XP SP3、Windows Vista、Windows 7、Windows 8+ 和 Windows 8+ Pro（包括 32 位和 64 位，如果适用）。

设备操作包括：

- 向设备发送消息
- 锁定设备
- 定位设备（需要 MaaS360 Laptop Location）
- 停止/启动/重新启动服务
- 关闭/重新启动
- 擦除硬盘驱动器
- 配置补丁设置
- 分发软件

### 1.24.2 MAC 操作系统 X

MaaS360 Laptop Management (SaaS) for Mac OS X 提供了针对硬件、操作系统和软件信息的无线注册和库存管理报告功能。端点安全性报告模块为客户提供的应用程序（诸如防病毒、备份/恢复、数据加密和个人防火墙以及缺少的操作系统补丁等）提供交互式报告和数据分析功能。数据保护模块为数据安全服务（包括数据加密）提供交互式报告和分析功能。配置管理模块为多项设备和用户设置提供远程管理，包括密码、电子邮件、VPN 和 Wi-Fi。支持 Mac OS X V10.7.3 或更高版本。

设备操作包括：

- 锁定设备
- 擦除硬盘驱动器
- 更改设备策略

## 1.25 IBM MaaS360 Laptop Location (SaaS)

MaaS360 Laptop Location (SaaS) 支持对所支持的笔记本电脑和平板电脑进行定位。MaaS360 可报告 Wi-Fi 或 IP 地址坐标位置，并将该数据转换为容易识别的地址。设备在线时，可检索其当前位置。MaaS360 会存储一段时间内报告的位置，因此可查看位置历史记录。需要 MaaS360 Laptop Management (SaaS) for Windows。支持 Windows XP SP3、Windows Vista、Windows 7、Windows 8+ 和 Windows 8+ Pro（包括 32 位和 64 位，如果适用）。

## 1.26 IBM MaaS360 Laptop Lifecycle Management (SaaS)

提供 MaaS360 Laptop Management (SaaS) 服务产品的功能并添加以下功能：

- 允许客户将程序包上传至 MaaS360 Content Service (SaaS) 平台并安排向 MaaS360 Laptop Management (SaaS) service for Microsoft Windows 管理的设备分发有效内容。客户可以控制各方面的分配情况，包括设备、组或全局级别的安装指示信息和目标定位。客户负责创建所有封装和安装文件。IBM 不提供创建安装程序包支持。

## 1.27 IBM MaaS360 Laptop Security (SaaS)

为组织提供在同一管理控制台中企业和员工持有的设备间保持安全策略和概要信息一致的能力。

## 1.28 IBM MaaS360 Essentials Suite (SaaS)

此套件支持客户查看和控制进入客户组织的移动设备和应用程序。此套件于单一界面为企业提供移动设备、应用程序和费用管理。

## 1.29 IBM MaaS360 Deluxe Suite (SaaS)

此套件包含 MaaS360 Essentials Suite 的所有功能，并添加一个单独的高安全性办公生产力应用程序，便于用户访问和管理他们的电子邮件、日程表、联系人以及交谈记录。

## 1.30 IBM MaaS360 Premier Suite (SaaS)

此套件包含 MaaS360 Deluxe Suite 的所有功能，并添加移动应用程序安全性、安全的移动浏览器、网关以及移动内容管理功能。

## 1.31 IBM MaaS360 Enterprise Suite (SaaS)

此套件包含 MaaS360 Premier Suite 的所有功能，并添加移动威胁管理、文档编辑器以及文档同步功能。

## 2. 安全描述

此 Cloud Service 遵循 <http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp> 中提供的针对 IBM SaaS 的 IBM 数据安全和隐私原则，以及本部分中提供的任何其他条款。对于 IBM 数据安全策略所做的任何更改都不会降低 Cloud Service 的安全性。

该 Cloud Service 已经过美国-欧盟安全港认证。

## 3. 服务标准协议

IBM 按照 PoE 中的规定为 IBM SaaS 提供了以下可用性服务级别协议 (SLA)。本 SLA 不是一项保证，也不适用于支持软件。本 SLA 仅提供给客户，且只能应用于生产环境。

### 3.1 可用性积分

客户必须在首次发现事件影响 Cloud Service 可用性的 24 小时内，通过 IBM 技术支持帮助中心记录 1 级严重性支持凭单。客户必须为 IBM 的任何问题诊断和解决提供合理帮助。

必须在约定的月份结束后的三个工作日内提交支持凭单，对未能满足 SLA 提出索赔。针对有效 SLA 索赔的赔偿将基于 Cloud Service 的生产系统处理不可用的时间段（“停机时间”），以针对 Cloud Service 的将来发票的贷记金额的形式支付。停机时间从客户报告停机事件开始计算，到 Cloud Service 复原为止，其中不包括有关以下方面的时间：计划或宣布的维护停运；IBM 可控范围之外的停机原因；客户或第三方的内容或技术、设计或指令问题；不受支持的系统配置和平台或其他由客户引起的错误；或客户导致的安全事件或客户安全测试。IBM 会根据每个约定的月份内累积的可用 Cloud Service 适用最高的赔偿，如下表中所示。对任何“约定的月份”给与的赔偿总额不应超过年度 Cloud Service 费用的十二分之一 (1/12) 的百分之十。

### 3.2 服务级别

约定的月份内的 Cloud Service 的可用性

一个合同月期间的可用性	可用性积分 (受索赔的“约定的月份”的每月订购费用* 的百分比)
低于 99.8%	2%
低于 98.8%	5%
低于 95.0%	10%

\* 如果 Cloud Service 是从 IBM 业务合作伙伴处购买的，那么每月订购费用将基于受索赔的“约定的月份”期间有效的 Cloud Service 当时目录价格进行计算，适用折扣费率为 50%。IBM 将直接向客户应用折扣。

可用性以百分比表示，计算如下：一个合同月中的总分钟数减合同月总停机时间，除以该合同月的总分钟数。

示例：约定的月份内停机时间总计 425 分钟

30 天的“约定的月份”内总计 43,200 分钟 - 425 分钟停机时间 = 42,775 分钟 <hr/> 总时间 43,200 分钟	= 2% 可用性积分，在约定的月份内实现 99.0% 的可用性
---	---------------------------------

## 4. 技术支持

针对 Cloud Service 的技术支持通过聊天、电话和电子邮件提供。

IBM 将提供《IBM 软件即服务支持手册》，其中提供了技术支持联系信息以及其他信息和流程。

严重性	严重性定义
1	中断或阻止客户所有员工执行正常业务运营的服务问题。 由对正常业务运营带来灾难性影响的服务引发的问题。
2	中断或阻止客户大部分员工执行正常业务运营的服务问题。 由对正常业务运营造成重大影响的服务引发的问题。
3	中断或阻止客户少部分员工执行正常业务运营的服务问题。 由对正常业务运营带来严重影响的服务引发的问题。
4	中断或阻止客户个别员工执行正常业务运营的服务问题。 由对正常业务运营造成轻微影响的服务引发的问题。

## 5. 权利和计费信息

### 5.1 收费标准

Cloud Service 根据交易文档中指定的收费标准提供：

- a. **授权用户** - 获取 Cloud Service 时所采用的一种计量单位。客户必须为每位唯一的“授权用户”取得单独且专有的权利，使其能够以任何方式，通过任何途径直接或间接地（例如：通过多路复用程序、设备或应用程序服务器）访问 Cloud Service。必须获取足够的权利，以涵盖客户的 PoE 或交易文档中所指定的评估期间给予 Cloud Service 访问权的“授权用户”的数量。
- b. **千兆字节** - 获取 Cloud Service 时所采用的一种计量单位。千兆字节定义为 2 的 30 次方个字节的数（1,073,741,824 字节）。必须获取足够的权利，以涵盖客户的 PoE 或交易文档中所指定的评估期间由 Cloud Service 处理的千兆字节数据总数。
- c. **受管客户端设备** - 获取 Cloud Service 时所采用的一种计量单位。“客户端设备”指单个用户计算设备或特殊用途的传感器或遥测设备，该设备向另一个通过称作服务器或由服务器管理的计算机系统，请求执行一系列命令、过程或应用程序或接收执行的结果，或向其提供数据。多个客户端设备可以共享对一台公共服务器的访问。客户端设备可以具有某些处理能力或者可进行编程以允许用户进行工作。客户必须为其 PoE 或交易文档中所指定的评估期间 Cloud Service 管理的每个客户端设备获取受管客户端设备权利。
- d. **客户端设备** - 获取 Cloud Service 时所采用的一种计量单位。“客户端设备”指单个用户计算设备或特殊用途的传感器或遥测设备，该设备向另一个通过称作服务器或由服务器管理的计算机系统，请求执行一系列命令、过程或应用程序或接收执行的结果，或向其提供数据。多个客户端设备可以共享对一台公共服务器的访问。客户端设备可以具有某些处理能力或者可进行编程以允许用户进行工作。客户必须为其 PoE 或交易文档中指定的评估期间运行、提供数据、使用提供的服务或访问 Cloud Service 的每个客户端设备获取权利。

### 5.2 未满一个月的收费标准

根据交易文档的规定，使用未满一个月将按比例收取费用。

### 5.3 盘盈费用

如果评估期间 Cloud Service 的实际使用超出了 PoE 中指定的权利，那么将按照交易文档中的规定向客户收取盘盈费用。

## 6. 期限和续约选项

Cloud Service 期限自 IBM 通知客户可访问 PoE 中记录的 Cloud Service 之日算起。PoE 将指定 Cloud Service 是自动续订、在持续使用基础上继续，还是在期限结束时终止。

### 6.1 自动续订

对于自动续订，除非客户在期限到期日期之前，至少提前 90 天发出不再续订的书面通知，否则将按照 PoE 中指定的期限对 Cloud Service 自动续订。

续约权利数量等于原始订单数量或生成续约发票之前月份的月度报告的使用量，以较大者为准，除非 IBM 收到指定其他权利数量的通知。

STEP UP 产品的续约权利数量等于原始订单数量。

### 6.2 持续计费

对于持续使用，在客户提前 90 天发出终止书面通知之前，Cloud Service 将以月为单位继续有效。Cloud Service 的有效期将于 90 天期限过后的日历月末终止。

## 7. 支持软件

此 Cloud Service 包括支持软件，只能在 Cloud Service 期限内与客户对 Cloud Service 的使用相关联的情况下使用该软件。

## 8. 其他信息

### 8.1 Step up 限制

对于指定为“Step up for existing Customers”（“Step up SaaS”）的 Cloud Service 服务产品，客户必须预先或同时购买 Step up SaaS 服务产品名称中指定的关联 IBM 程序的相应许可权利。例如，购买“IBM MobileFirst Protect - Devices (SaaS) Step up for existing customers”的客户必须具有关联的 IBM 程序 IBM MobileFirst Protect 的许可权利。客户对于 Step up SaaS 的权利不应超过客户对于关联 IBM 程序的权利。

购买 Step up SaaS 时，客户不得在内部安装的环境中使用相同的关联 IBM 程序许可权利以及 Step up SaaS 权利。例如，如果客户具有 250 份针对关联 IBM 程序的 Managed Client Device 权利，并且选择购买 100 份 Step up SaaS Managed Client Device 权利，那么客户可通过 Cloud Service 环境管理 100 个 Step up SaaS Managed Client Device，并通过内部安装的软件管理 150 个 Managed Client Device。

客户表示，自己已购买适用的 (1) 许可权利和 (2) 针对关联的 IBM 程序的订购和支持。在 Step up SaaS 的订购时间段内，客户必须保持将 Step up SaaS 权利与 IBM 程序的最新升级和支持权利一起使用。如果使用关联 IBM 程序的客户许可或者对关联 IBM 程序的客户订购和支持终止，那么客户使用 Step up SaaS 的权利也将终止。

### 8.2 Cookies

客户同意 IBM 可以依照 <http://www-01.ibm.com/software/info/product-privacy/index.html> 中所述，使用 Cookies 和跟踪技术在收集使用统计信息及其他信息过程中收集个人可识别信息，帮助改进用户体验和/或定制与用户的交互。

### 8.3 无个人健康信息

Cloud Service 并非为符合 HIPAA 要求而设计，不得用于传输或存储任何“个人健康信息”。

### 8.4 标准数据

无论是否存在任何相反的规定，仅出于规范的研究、分析、演示和报告目的，IBM 可保留并使用匿名汇总格式的数据（即，无法将客户或客户的授权用户识别为数据来源，并且会除去可识别客户或客户的授权用户的个人信息），以数据反映客户的授权用户对于 Cloud Service 的各自体验。

## 8.5 合法使用和同意

### 8.5.1 收集和处理数据的权限

Cloud Service 旨在配置、管理、监视和控制移动设备。Cloud Service 将从客户授权的用户和设备收集信息用以与客户订购的 Cloud Service 进行交互。在某些管辖区域，Cloud Service 收集的信息可以单独或与其他信息一起被视为个人信息。收集的数据可能包括授权用户名、电话号码、注册的电子邮件地址、设备位置、用户 ID、MaaS360 浏览器的浏览历史记录，以及有关最终用户设备的硬件、软件和设置的信息，还有设备生成的信息。客户授权 IBM 依据本服务描述的条款收集、处理和使用此信息。

### 8.5.2 来自数据主体的同意书

对 Cloud Service 的使用可能涉及不同的法律和法规。Cloud Service 只可出于合法目的、采用合法方式使用。客户同意按照规定使用 Cloud Service，并承担所有责任，遵守适用的法律、法规和政策。

客户同意客户已获得或者将获得合法使用 Cloud Service 和允许 IBM 作为客户的数据处理机构通过 Cloud Service 收集并处理信息所需的任何完整的同意书、许可权或许可。客户特此授权 IBM 获取合法使用 Cloud Service 以及按照 <http://www.ibm.com/software/sla/sladb.nsf/> 中提供的最终用户许可协议的规定收集和处理信息所需的完整同意书。

## 8.6 数据保留时间

IBM 将在本服务描述到期或终止后删除收集的任何信息（这可能包括个人信息），除非前述目的或适用的法律、法规或规章需要保留这些信息。在此情况下，IBM 将在此类目的、适用法律、法规或规章所要求的期限内保留收集的信息。

## 8.7 数据隐私

### 8.7.1 跨境传输

如果客户将个人信息提供给位于欧盟成员国、冰岛、列支敦士登、挪威、瑞士、土耳其以及已颁布当地数据隐私或保护法的其他任何欧洲国家的 IBM Cloud Service，那么客户同意，IBM 可以按照相关法律和要求将内容（包括任何个人数据）跨国家或地区传输到欧盟经济区以外的下列国家或地区，以及被欧盟委员会视为具有足够安全性级别的国家或地区中的处理机构和分支处理机构：

处理机构/分支处理机构的名称	角色（数据处理机构或分支处理机构）	地区
IBM Corporation	分支处理机构	1 New Orchard Rd. Armonk, NY 10504, USA I
IBM India Private Limited	分支处理机构	No. 12, Subramanya Arcade Bannerghatta Road, Bangalore 560029 India

客户同意 IBM 在合理决定有必要提供 Cloud Service 时，可在提前通知的情况下对此国家或地区位置列表进行更改。

### 8.7.2 欧盟数据隐私

如果客户将个人数据提供给位于欧盟成员国、冰岛、列支敦士登、挪威、瑞士或土耳其以及已颁布当地数据隐私或保护法的其他任何欧洲国家的 IBM Cloud Service，或者如果客户的授权用户或设备位于这些国家或地区，那么客户作为唯一控制者，指派 IBM 作为处理机构，按照欧盟指令 95/46/EC 中定义的条款处理这些个人信息。IBM 将仅在根据 IBM 发布的 IBM Cloud Service 描述提供 IBM Cloud Service 产品所需的范围内处理此类个人信息，且客户同意，任何此类处理均符合客户的指令。

## 8.8 安全性数据

作为 Cloud Service（包括报告活动）的一部分，IBM 将准备并维护从 Cloud Service 收集的未标识化的信息和/或汇总信息（“安全性数据”）。“安全性数据”将不会识别客户或个人，以下 (d) 中提供内容除外。客户在此同意 IBM 只能出于以下目的使用和/或复制“安全性数据”：

- 发布和/或分发“安全性数据”（例如，在与网络安全相关的编译和/或分析中）；
- 开发或增强产品或服务；
- 开展内部研究或与第三方一起开展研究；以及
- 合法共享已确认的第三方罪犯信息。