Microsoft

保护云中的数据和隐私

目录

为了让企业客户能够从云计算获得收益，客户必须愿意将自己最重要的资产之一，即最有价值的数据托付给云服务供应商。本白皮书概括介绍由世纪互联运营的 Microsoft Azure 和 Office 365 企业服务中保障客户数据隐私的方法和流程。在讨论过围绕云环境隐私的问题后，我们还将讨论在构建这些服务，以及在数据中心内运行这些服务时保障隐私所采用的方法，借此确保客户在云中存储自己的数据时能够做出最妥善的选择。

保护云中的数据和隐私—简介

对于全球组织，无论政府部门，非盈利机构，或商业机构来说，云计算都已成为其持续 IT 战略的关键。云服务使得不同规模的组织能够获得几乎无限容量的数据存储，同时无需继续购买、维护、更新自己的网络和计算机系统。云服务供应商提供了 IT 基础架构、平台 ,以及软件"即服务"产品，使得客户能够根据需求快速扩大或收缩自己的 IT 环境，并只需要为自己实际使用的计算能力和存储容量付费。

然而，随着组织持续从云服务中获得各种收益，例如更丰富的选择、更高的敏捷度、更大的灵活性，以及更高的效率和更低的 IT 成本，他们还必须考虑使用云服务会对自己的隐私、安全，以及合规性态势产生怎样的影响。由世纪互联运营的 Microsoft Azure 和 Office 365 通过不断的努力，不仅可以提供可扩展、可靠、可管理的云服务，而且能够确保客户数据受到妥善保护，并以一种透明的方式加以使用。

在购买云服务和云基础架构时，客户有着非常丰富的选择，如本页左侧边栏所示。要确定哪一种云模式最适合客户，这主要取决于客户的要求和客户对数据保护的需求，以及客户需要的处理类型。实际上"通用"的方式可能并不适合于需要处理不同类型数据的所有组织。私有或混合云解决方案可以让客户将指定的数据保存在内部部署环境，这些方案最适合对数据保护有着特殊需求的组织。

Azure 和 Office 365 提供了完善的私有和混合云解决方案。

当然，对任何在线计算环境而言，安全性都是数据安全保护环节的一个重要组件。但仅仅做到安全本身还是不够的。消费者和企业是否愿意使用某种云计算产品，同时还取决于他们对自己的信息所能受到保护的信任程度，以及自己数据的使用方式是否与预期相一致。

长期积累的经验使得 Azure 和 Office 365s 采用业界领先的业务实践、隐私策略、合规性项目以及安全指标，并将其应用于云计算生态系统。云服务可能造成了独特的安全和隐私挑战，Azure 和 Office 365 久经时间考验的策略和实践为打消客户顾虑，增强客户对云计算的信任程度提供了切实的基础。

Azure 和 Office 365 在云服务中所实施的隐私和数据保护方法完全基于对

云服务的分类

- 软件即服务(SaaS)。指云服务供应商托管的一个或一系列应用程序，例如由世纪互联运营的 Office 365，其中可能包含各种产品的组合，例如 Exchange Online，SharePoint Online，和 Skype for Business。
- 平台即服务(PaaS)。用户使用云服务供应商提供的软件开发工具以及底层的基础架构和操作系统自行创建并运行自己的软件应用。例如 由世纪互联运营的 Microsoft Azure 就是这样的云平台。
- 基础架构即服务（ IaaS ）。用户租用计算能力—可能是真实的物理硬件或虚拟机—部署并运行自己的操做系统和软件应用。由世纪互联运营的 Microsoft Azure 也提供了此类服务。

云计算基础架构

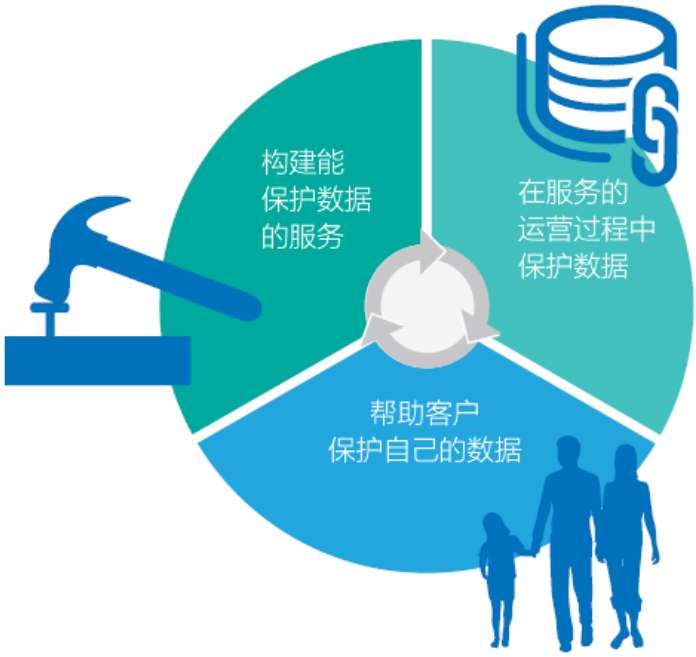
- 公有云。客户通过大型数据中心访问云服务并存储自己的数据，这些数据中心通常装备有数百台虚拟化服务器，托管了多个组织的数据。
- 私有云。每个组织使用自己专属的云基础架构。
- 社区云。私有云的一种类型，这种云被一系列有着共同使命、兴趣或关注点的组织所共用。例如，云服务供应商可以为政府客户提供专用的云服务实例。
- 混合云。将私有云扩展至公有云，借此对组织的数据中心进行扩展；或将两个或更多类型的云环境连接在一起，使得数据和应用程序能够用一种受控的方式在不同环境之间流转。

世纪互联在 Azure 和 Office 365 云服务中实施隐私和数据保护措施的努力可划分为三个主要类别。

用户的承诺：帮助组织控制自己信息的收集、使用，以及传播。通过提供这些功能，并实施强有力的运营保护实践，世纪互联通过认证、证明，以及合同条款等形式对客户做出合规性承诺。在管理客户与合作伙伴信息的过程中，把一般公认隐私实践和公平信息实践原则作为指导。

通过上述方式，世纪互联用隐私原则、数据处理协议，以及企业隐私策略管控着公司内部所有客户与合作伙伴信息的收集和使用，为员工提供清晰的框架，同时帮助他们保障隐私合规性。

世纪互联定期审阅隐私策略，以及在线应用中所需遵守的行为准则，如果需要改动以满足客户不断变化的需求和预期，会定期对其进行更新。



首先，世纪互联将客户数据的保护工作放在首位。其次，使用基于标准的技术和方法，保护客户使用服务的过程中在数据中心内存储的客户数据。第三，为用户提供建议，让用户为自己数据的保护工作做出最佳决策，满足其业务所适用的合规性要求。

下文将深入介绍每种方法的具体细节。

构建能保护数据的服务

作为云服务技术提供商，世纪互联鼓励所有云服务供应商构建不仅可以保护系统和数据本身的完整性，同时也能维持客户隐私的服务。同时利用微软在开发企业软件解决方案过程中积累的经验，帮助用户发掘所需要的隐私和保护需求。

承诺保护数据，限制数据的使用

企业客户在云服务中存储的任何数据都属于用户自己，不应被云服务供应商用于为客户提供服务之外的其他用途。世纪互联已将这一条款包含在服

务协议中，并在 Azure 和 Office 365 信任中心网站对其进行了详尽的解释。客户数据是指"使用在线服务的过程中，由客户创建，或代表客户创建的所有数据，包括所有文字、声音、软件或映像文件"。世纪互联不会将客户数据用于提供服务以外的其他用途，例如展示广告。此外，Azure 和 Office 365 在存储和备份数据，以及收到客户请求后，以安全的方式删除这些数据时，都建立了一套严格的标准。

构建能保护客户数据的云服务，其重点在于：

- 做出强有力的承诺，以保护客户数据，限制客户数据的使用。
- 遵循"与生俱来的隐私保护"这一原则，在开始构建云服务时就将客户隐私的保护工作放在首位。
- 提供各种功能，帮助客户保护并控制自己信息在云服务中的流动。

与生俱来的隐私保护

当微软构思新的产品和技术时，开发工作的每个阶段都将隐私和数据保护放在首位。这也是所谓的"与生俱来的隐私保护"这一方法的重要组成部分，该方法不仅规定了微软开发产品的方式，同时规定了世纪互联运营服务，以及规划内部管理实践的方式。这套全面的方法涵盖了所有人员、流程以及技术，有助于维持并提高我们为客户提供的隐私保护水平。

隐私方面的考虑也已融入到安全开发生命周期（SDL）内。SDL 是一种软件开发流程，可以帮助开发者构建更安全的软件，能在降低开发成本的同时满足有关安全与隐私的合规性需求。Azure 和 Office 365 的开发都遵循 SDL 的要求，以确保所有功能是安全的，可充分满足客户对数据和隐私保护的需求。

SDL 由七个阶段组成，包括在基础性概念阶段对开发者和项目经理进行培训；构建安全的，能保护隐私的软件；以及在遇到安全和隐私事件后所做出的响应。

在开发过程中，为了实施一致的隐私实践，使用工具来定义标准的隐私功能和实践。因为安全是隐私保护的重要一环，因此完善的隐私保护与安全流程的相互匹配有助于将软件代码中包含的漏洞数量降至最低，保护并防止数据外泄，进而确保开发者能够从一开始就将隐私保护纳入产品和服务的开发过程中。Azure 和 Office 365 严格遵循 这些工具所规定的流程。

在产品开发过程中，通过隐私审阅流程确认产品恰当地满足了有关隐私保护的需求。对于云服务，这些审阅可以：

- 验证具备与隐私保护有关的功能，可以让客户控制谁能访问自己的数据，并配置相关服务，以满足客户有关隐私监管的需求。
- 发现隐私隐患。
- 确定需要由工程部门实施的补救操作。
- 在最后审阅中，确定所有需求是否得以满足。

为服务提供能保护隐私的功能

在保护客户隐私方面，除了已经到位的投资和流程，Azure 和 Office 365 还实施了高级的数据保护和安全功能。例如，Office 365 可充分利用 Azure Active Directory 这一完善的云身份和访问管理解决方案。当客户在 Office 365 服务中创建帐户后，这些帐户即可自动关联至一个 Active Directory 云帐户，借此可为用户提供无缝的单一登录体验。用户甚至可以将内部部署的目录扩展至 Azure Active Directory，这样用户只需要使用一套企业凭据即可对云中的资源进行身份验证。

通过将 Azure Active Directory 帐户自动关联至 Office 365 订阅，可以帮助客户更充分地利用目录服务中提供的诸多安全与隐私保护功能，其中包括：

- 联合身份验证和访问管理。
- 权限管理服务。

通过将 Azure Active Directory 帐户自动关联至 Office 365 订阅，可以帮助客户更充分地利用目录服务中提供的诸多安全与隐私保护功能，其中包括：

- 联合身份验证和访问管理。当客户订阅了多个服务时，组织可以在订阅 Office 365 ,以及 Azure 的其他在线服务时使用同一个 Active Directory 帐户。组织也可以利用 Azure 对混合云的支持，将不同服务的身份与内部部署环境中现有的 Active Directory 服务联合在一起。这样管理员即可通过一个目录，管理内部部署环境以及云中企业资源的访问，进而降低管理工作的复杂度，改善最终用户体验。
- 权限管理服务（RMS）。通过使用 RMS，组织可以进一步完善自己的数据保护策略，通过与信息持续相伴的使用策略对信息提供保护，而无需考虑信息到底存储在哪里。Office 365 中包含了 RMS 功能，因此无论电子邮件，或是由 Word、Excel 和 PowerPoint 等程序创建的文档，都可以受到 RMS 的保护，防范机密信息外泄。用户可以定义谁能打开、修改、打印、转发信息，或执行其他操作。组织可以创建自定义的使用策略模板，例如“机密—只读”，并直接应用给不同的信息。

除了有关 Active Directory 的这些功能，Office 365 中的 Exchange Online 邮件服务还提供了强大的数据防丢失（DLP）服务。通过深入的内容分析功能，DLP 可帮助组织识别、监控、保护机密信息。DLP 功能对企业信息系统来说正变得越来越重要，因为企业机密邮件中包含的敏感数据必须获得妥善的保护。DLP 可以在邮件中扫描财务信息、个人可识别信息（PII），以及知识产权数据，如果扫描邮件发现存在匹配的内容，还可酌情执行相关操作，例如拦截信息禁止发送到外部，或对信息进行加密。

在服务的运营过程中保护数据

如果部署在不够安全的环境中，就算有着一流设计与实施的服务也无法保护客户数据和隐私。客户都不希望自己的数据被暴露给其他云客户。他们还会假设数据中心内所使用的流程，以及数据中心内的工作人员，都应致力于保护自己的数据隐私和安全。

要实现这一切，需要进行规划和协调，以及一支训练有素的团队。在本节中，我们将介绍在服务运营过程中，用于保护客户数据隐私的流程和协议。同时我们还将重点介绍服务管理过程中，为确保满足客户的隐私义务与承诺，所需要遵守的重要数据隐私标准，并会介绍这些服务如何帮助客户满足有关 IT 隐私与安全要求的各种制度。此外，我们还会讨论我们对运营透明度的承诺，只有这样才能证明我们的服务符合监管部门、政府机构，以及客户自身的合规性要求。

保护服务隐私所用的技术

云服务运营过程中，为了保护数据隐私，世纪互联使用了一系列通用的技术。

首先是数据访问控制。数据访问控制主要分为两个类别：物理和逻辑。在物理层面上，对数据中心设施的访问受到由外到内的妥善保护，每一层面都提供了逐级提高的安全机制，包括边界围墙、安保人员、服务器机架锁、多重访问控制、集成式警报系统，以及运营中心提供的 24x7 全面视频安防监控。

对客户数据的访问会根据业务需求进行严格限制。对此类访问的限制是由基于角色的访问控制、双重身份验证、生产数据最小化访问，以及在生产服务环境中所执行的工作活动日志记录和审计等因素控制的。

世纪互联对生产环境中与隐私和安全有关的威胁进行定期监控，通过一套严格的内部管理流程对数据中心内潜在的安全隐患进行汇报。启动之后，该流程会将具备相同技能背景的工程师结合在一起，以团队的方式完成隐私保护、取证、法务，以及沟通工作，借此决定最适宜的行动方针，确保能及时解决隐私问题。

为确保同一个云服务中不同客户所存储的数据受到隐私保护，Azure 和 Office 365 使用了数据隔离技术从逻辑上对云租户进行了分隔，进而创建出每个客户只能访问自己数据的安全环境。

世纪互联仅在位于中国大陆的数据中心运营 Azure 和 Office 365。客户可以指

由世纪互联运营的 Office 365 信任中心

21vbluecloud.com/office365/TrustCenter/

由世纪互联运营的 Microsoft Azure 信任中心

azure.cn/support/trust-center/

上图概括列出了 Azure 技术提供商微软企业云服务所用到的数据中心所在地。Office 365 和 Azure 都允许客户自行选择自己数据的存储地区。

定用于存储客户数据的数据中心所在的地理区域。可用区域分别为中国东部（位于上海）和中国北部（位于北京）。这两座数据中心，两地距离超过 1000 公里，具有地理冗余的数据可以在每个数据中心中存有 3 个副本，两地共 6 个副本，不仅实现了异地灾备，还能帮助 Azure 和 Office 365 的用户实现更好的网络访问效率以及数据和业务的可靠性。在网络接入方面，世纪互联运营的 Microsoft Azure 和 Office 365 服务的数据中心直接接入中国移动、中国电信、中国联通多家主流运营商的骨干网络，可为用户提供高速的网络访问体验。

世纪互联持续监控提供服务的过程中两个数据中心所涉及的全部系统，通过预测恶意行为发现潜在威胁，并对可能代表此类威胁的反常事件进行监控。

数据隐私标准合规性

Azure 和 Office 365 服务不仅符合全球数据隐私标准的要求，而且可以帮助我们的客户遵守这些标准的要求。Office 365 和 Azure 都已获得 ISO/IEC 27001 认证、公安部信息系统安全等级保护评定认证、以及相应的数据中心联盟可信云服务认证，并有获得授权的独立审计机构发布的合规证书。

透明度

面对执法部门或其他政府机构提出的有关客户数据的访问申请，世纪互联只会为符合法律要求的申请提供申请中明确要求索取的数据。对于 Azure 和 Office 365 服务，客户应当自行控制自己存储在内部环境或云服务中的数据。因此除非客户或者法律要求我们这样做，否则我们不会将客户数据披露给第三方（包括执法部门，其他政府机构，或是民事诉讼当事人）。如果第三方联系我们索取客户数据，我们会让第三方直接联系客户并尝试获取。如果我们必须向第三方披露客户数据，除非法律禁止我们这样做，否则我们会立刻通知客户并提供所申请数据的副本。

世纪互联只会为客户自己要求或符合法律要求的数据访问申请提供最小范围的数据访问。

帮助客户保护自己的数据

世纪互联致力于确保客户数据私密性的三项努力中的最后一个领域，是为客户和潜在客户提供足够的信息，不仅帮助他们清晰地知晓世纪互联如何保护客户数据，并且清楚了解世纪互联的隐私承诺，以及为确保自己数据的私密性，客户需要自行承担的责任。

数据保护责任范围

世纪互联非常重视保护和维持客户数据私密性所做出的承诺，并会帮助客户用一种受保护的方式实施并使用 Azure 和 Office 365 服务。数据保护和隐私是服务供应商及其客户共同的责任。供应商应负责整个平台，并负责创建能满足客户的安全、隐私，以及合规性需求的服务。

客户则需在服务设置完成后负责配置并运营自己的服务，包括管理访问凭据，以及制度和法规的合规性，通过服务的配置选项为应用程序、数据内容，以及

自己帐户中所使用的任何虚拟机或其他数据提供保护。

下表详细分解了云服务供应商的责任，及其客户所需承担的责任。这些责任之间的界限并非总是很清晰，可能取决于客户所签署的协议或其他因素。世纪互联会针对这些角色和责任，尽最大努力维持透明度。世纪互联提供明确的合同承诺，并在 Azure 和 Office 365 信任中心页面分别详细介绍注意事项。

虽然供应商需要负责构建服务与功能，确保与相应的数据保护和隐私制度与标准的合规性，但客户依然要对服务进行配置，并为员工提供培训，以便用一种满足所在行业和所处地区合规性要求的方式使用这些服务。同时，虽然需要由供应商创建强有力的运营控制机制，以保护客户在云中存储的数据，但依然需要由客户使用这些控制机制限制非必要的数据共享和访问。最后，供应商需要负责通过获取认证，分享认证报告，签署协议等方式证明自己有关数据保护的承诺。然而云服务的客户也需要负责验证供应商的审计报告、认证，以及其他证明能够满足自己对数据保护工作的预期。

数据可移植性

Azure 和 Office 365 都可以让客户无需世纪互联的协助，直接下载自己的数据副本。

例如，作为对此目标的支持，Office 365 为 Exchange Online 提供了导入和导出向导，借此最终用户可以随时将邮件、日历约会、联系人，以及任务信息下载到本地计算机。此外，该服务还提供了 Windows PowerShell "命令工具"或脚本命令，可将其用于管理支持 Microsoft PowerShell 接口的服务，这就使得管理员可以在需要时下载最终用户的元数据。最后，当客户结束自己的云服务订阅时，世纪互联会使用一个功能受限的帐户将所有数据保存 90 天，以便用户提取自己的数据。随后这些数据会被删除。这就确保了客户有足够的时间可以将数据迁移至业务所需的其他服务。同时也确保了客户数据会在特定时间段内彻底删除，进而保障前任客户数据的隐私。

要详细了解世纪互联的数据可移植性、数据保留，以及数据删除策略，请访问 Azure 和 Office 365 信任中心页面。

世纪互联确保所有客户数据的所有权皆属于客户自己。

为客户提供帮助的资源

为了让客户有足够的信息以便做出与数据保护和隐私有关的决定，世纪互联尽最大努力确保策略和客户沟通方面的透明度：

- 提供在线版的信任中心或隐私声明。Office 365 和 Azure 具有分别的信任中心页面，并且提供在线版的隐私声明。

结论

由世纪互联运营的 Microsoft Azure 和 Office 365 在建过程中提供与生俱来的隐私保护，并提供必要的合规性机制，信守承诺，将客户数据的保护要求放在首位。

云计算为组织和个人提供了更多选择、更大灵活性，以及更低的成本。然而为了获得这些收益，云客户需要从云供应商处获得有关数据隐私和安全的可靠保障。国际与国内的云计算标准组织通过制定标准和指标，帮助供应商与客户定义自己的数据隐私需求，才让云计算的潜力得以顺利实现。

在世纪互联提供运营的 Microsoft Azure 和 Office 365 云服务中，安全与客户数据的隐私是最为重要的考虑因素。

Azure 和 Office 365 致力于为商业客户提供最高级别的隐私和安全标准的云服务，也期待着与客户携手，继续完善我们的数据隐私和保护实践，将客户对我们云计算服务的信任发扬光大。

更多资源

通过为客户提供指南和透明度，我们可以帮助客户更清晰地了解自己的数据隐私是如何得到保障的。

由世纪互联运营的 Office 365 信任中心

21vbluecloud.com/office365/TrustCenter/

由世纪互联运营的 Microsoft Azure 信任中心
azure.cn/support/trust-center/