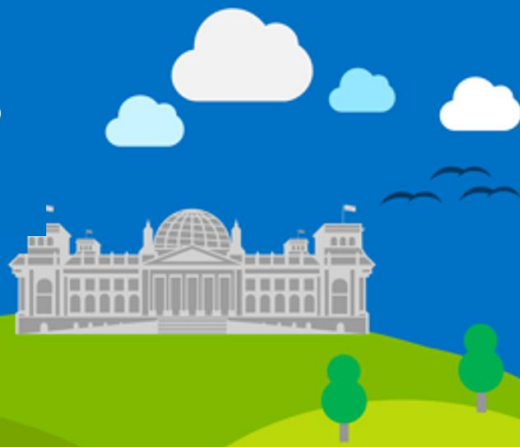


由世纪互联运营的 Microsoft Azure 和 Office 365 云服务运营模式



目录

简介	2
由世纪互联运营的 Microsoft Azure 和 Office 365 在线服务	2
微软云技术	4
主要特色	4
客户数据	5
客户数据的存储位置	6
基础架构的安全性	6
客户数据的访问	7
基础架构的访问	7
基于角色的访问控制 (RBAC)	7
合同承诺	8
微软和世纪互联的合作模式	8
角色和责任	9
微软	9
世纪互联	9
执法请求	9
合规性	10
合规性认证	11
总结	13

简介

互联网时代，无论是个人用户、创业团队、还是大型的企业，数据都是最具价值的资产之一。数据是企业的生存之本，正是依赖这些数据，企业可以更好的维系客户关系、发掘客户的需求、更好的管理员工与业务……数据的拥有者因此对在线数据的存储和使用的各种不确定性产生顾虑，例如客户数据存储在哪里，谁能访问这些数据，当第三方需要访问客户数据时有无法律法规约束，等等。

中国关于对数据的隐私保护有明文规定：网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密，不得泄露、篡改、毁损，不得出售或者非法向他人提供。网络服务提供者和其他企业事业单位应当采取技术措施和其他必要措施，确保信息安全，防止在业务活动中收集的公民个人电子信息泄露、毁损、丢失。在发生或者可能发生信息泄露、毁损、丢失的情况时，应当立即采取补救措施。

由世纪互联运营的 Microsoft Azure 和 Office 365 在线服务

在中国，由世纪互联运营的 Microsoft Azure 和 Office 365 服务是在中国大陆独立运营的公有云平台，由北京世纪互联宽带数据中心有限公司的全资子公司上海蓝云网络科技有限公司（简称为“世纪互联”）独立运营和销售。采用微软服务于全球的 Azure 和 Office 365 技术，为客户提供全球一致的服务质量保障。

作为由世纪互联运营的 Microsoft Azure 和 Office 365 的客户，可获得以下服务：

- 在中国大陆数据中心托管且由世纪互联独立运营的云服务。世纪互联是中国领先的互联网数据中心提供商。
- 源于微软应用于全球企业客户数十年的丰富在线服务经验而开发的世界一流的 Azure 和 Office 365 技术，全面服务于中国的客户。



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。

微软向世纪互联许可相关技术、提供后台技术支持、就运营管理制度进行移植、培训，确保中国用户能够在世纪互联运营的 Microsoft Azure 和 Office 365 的云服务中享受与国际水准一致技术、功能和服务。微软全球技术支持中心与世纪互联在人员培训、技术转移、技术支持和服务等方面展开了深入、广泛的合作，确保更稳定可靠的技术实现和最佳客户体验。

世纪互联运营 Azure 和 Office 365 的所有服务器位于中国电信在北京和上海的数据中心，均由世纪互联运营。世纪互联掌握所有 Azure 和 Office365 服务相关的密钥和数据，以及系统与数据中心出入控制。微软仅在世纪互联无法独立解决相关疑难问题的情况下，在世纪互联相关人员陪同并监督的场合，帮助世纪互联解决相关技术问题。



在中国大陆由世纪互联运营的 Microsoft Azure 和 Office 365 与全球其他地区由微软运营的 Azure 和 Office 365 服务在物理上和逻辑上都是独立的。这些服务运行与全球微软云服务完全相同的技术，可提供与全球微软云相同级别的客户服务。客户对自己的客户数据拥有所有权，可以随时使用自己的客户数据，也可以随时出于任何原因下载自己所有数据的副本，无需世纪互联协助。此外除了客户及其最终用户，其他任何人都无权访问客户数据。世纪互联不会将客户数据用于为客户提供服务之外的其他目的。

世纪互联的供应商并不具有客户数据的逻辑或物理访问权限，除非在极少数情况下，世纪互联需要供应商技术协助来对客户支持事件进行故障排除或解决技术问题。世纪互联仅在解决问题所需的时间期限内授予此类访问权限，并且会密切监控此类授权访问，在问题解决后终止访问权限。

微软云技术

由世纪互联运营的 Microsoft Azure 和 Office 365 服务在物理和逻辑上与全球微软云服务处于隔离状态，但运行与全球微软云相同的技术，由世纪互联运营并提供客户服务。Azure 提供了包括计算、存储、数据、网络，以及应用程序在内的集成式服务；Office 365 使得最终用户能够随时随地在几乎任何设备上使用自己熟悉的 Office 工具，例如 Word、Excel、PowerPoint，以及 Outlook。客户可以借助 Azure 和 Office 365 可信赖的基础服务设计、构建、管理自己的安全云应用和基础结构。

主要特色

为了满足中国政府和标准化组织在监管安全、合规，以及隐私保护方面的要求，与全球微软云相比，由世纪互联运营的 Microsoft Azure 和 Office 365 在线服务提供针对中国市场的特性：

- 在物理和逻辑上维持与全球微软云隔离的 Azure 和 Office 365 服务
- 位于中国境内，独立于全球微软云公有云网络的专属网络由中国领先的互联网数据中心提供商世纪互联独立运营，确保所有客户数据，以及任何可能用于访问客户数据的支撑系统，全部位于中国境内的数据中心
- 满足中国政府和标准化组织的合规要求和认证，例如公安部信息系统安全等级保护定级认证，数据中心联盟可信云服务认证

客户数据

客户数据是由客户或其他人代表客户在使用服务时提供给世纪互联的所有数据，包括所有文本、声音、软件或图像文件。例如，客户数据包括客户上载以在服务中存储或处理的数据，以及客户或最终用户上传以在服务中托管的应用程序。它不包括配置、技术设置或服务记录信息。

Azure 客户数据的范例包括：

- 由客户提供，在 Azure 虚拟机中运行的二进制文件，以及虚拟磁盘（VHD）文件的内容
- 客户 Azure 存储 Blob 的内容
- 客户 SQL Azure 数据库的内容
- 客户所拥有的安全信息/密文（例如证书、加密密钥、存储密钥）
- 客户创建的 Active Directory（AD）数据（例如最终用户的 AD 标识或用户名）
- 服务总线消息内容

Office 365 客户数据的范例包括：

- 客户的邮件和附件
- 任务和待办事项列表
- 日历和约会信息
- 联系人和备注
- 客户的 SharePoint 网站内容
- 客户上传的文档和照片
- 客户的即时信息（IM）或语音对话
- 客户的 Global Address List（GAL）数据（例如姓名、邮件地址、办公室地址、电话号码、经理/直接下属、通讯组成员身份）

客户数据的存储位置

所有客户数据、处理这些数据的应用程序，以及承载世纪互联在线服务的数据中心，全部位于中国境内。位于中国东部(上海)和中国北部（北京）的数据中心在距离相隔 1000 公里以上的地理位置提供异地复制，为 Azure 和 Office 365 在线服务提供了业务连续性支持。



基础架构的安全性

Azure 和 Office 365 在线服务通过持续不断的入侵检测和预防系统、拒绝服务攻击预防系统、定期的渗透测试，以及取证工具为整个基础架构提供了 24x7 的安全保护，借此发现并减缓威胁。

Azure 和 Office 365 在线服务所使用的数据中心在外围边界、建筑物、机房，以及网络层面部署了全面的控制机制，借此提供多层次的安全防护。这些控制机制配合使用了技术措施和传统的物理安全措施管理和监视数据中心，防止未经授权访问数据和服务，以及防范一些环境风险。

在外围边界安全方面，每个数据中心都有全天候值守的安保人员、物理屏障，以及围栏。



为保护物理结构，数据中心的每栋建筑物都具备抗震支撑，以及针对各种环境条件的保护机制。运营中心还部署了全天候监控的监视摄像机。

为了进一步保护客户数据和应用程序，数据中心内使用了具备双重身份验证机制的访问控制系统，例如生物特征识别/智能卡。针对自然灾害或断电等故障，机房提供了自适应电源系统，可维持数天的供电。

客户数据的访问

基础架构的访问

世纪互联作为运营方管理对客户数据的物理和逻辑访问。除了上文介绍的基础架构安全措施，世纪互联严格控制对存储客户数据的 Azure 和 Office 365 在线服务基础架构的所有访问。这意味着对于任何需要访问客户数据，或访问存储有客户数据的基础设施的运营任务或其他任务，只有世纪互联能够负责执行或监控。世纪互联之外的其他人员无法访问存有客户数据的服务器，也无法登录到任何此类服务器。微软无权访问客户数据，除非世纪互联需要微软的技术协助来对客户支持事件进行故障排除或解决技术问题，但仅限极少数情况下。世纪互联仅在解决问题所需的时间期限内由客户授予此类访问权限。世纪互联会密切监控此类授权访问，并在问题解决后终止访问权限。

基于角色的访问控制 (RBAC)

世纪互联通过实施专门的基于角色的访问控制 (RBAC) 工具控制着对客户数据的逻辑访问，该工具可以识别并控制服务团队中每个成员的访问权限。这些工具在设计上为世纪互联控制对客户数据的所有访问操作（不包含客户或客户的最终用户主动发起的访问行为）提供了所需的技术能力。RBAC 使得世纪互联能够根据服务团队中具体人员在团队中的预设角色控制访问特权。这些特权是通过一个内部专用的标识管理工具定义的，并通过中国境内部署的 Active Directory 强制实施。

与客户有关的管理活动的边界和工具集，与全球微软云在线服务数据中心是类似的，在很多情况下甚至是相同的。主要差异在于访问权的批准者为世纪互联。任何能够用于访问客户数据的工具都受到世纪互联的控制，若对其进行修改，使其必须首先获得世纪互联的批准才能使用。例如，即时 (Just-in-Time, JIT) 访问管理工具，必须首先得到世纪互联的批准才能授予访问权。



所有获取客户数据访问权的技术机制都必须首先得到世纪互联的批准。这些限制是在技术设计层面上实施的，也就意味着微软员工不能获得数据访问权。RBAC 访问控制基于已获证实的技术构建并交付，借此实施上文提到的策略，并且在任何客户的数据迁移至该环境前，首先需要通过世纪互联的验证。

微软员工不具备任何可用于让微软访问客户数据的顶级管理权，任何此类权力都是由世纪互联（或客户）自行控制的。世纪互联可能会向微软提交申请，请求微软出于合理用途访问包含客户数据的系统，例如解决特定的支持事件、执行特定的升级操作，或对事件进行排错。这种访问请求必须符合世纪互联与微软之间确立的访问控制策略要求。如果微软被授权了访问，这样的访问只能适用于每个具体的事件（例如为了解决某一具体的支持事件，或执行某一特定的升级），并且访问的有效期会被限制为必要的时间段内。

基于上文所述的策略，世纪互联向客户提供了合同承诺，在没有得到世纪互联或客户批准的情况下，微软将无法访问到客户数据。

合同承诺

微软和世纪互联的合作模式

根据微软和世纪互联的合作协议，Azure 和 Office 365 公有云服务的在华运营完全由世纪互联负责，包括与客户签订合同、付款交易、开具发票、提供运营保障、技术支持和后续服务等。同时，责任追究和赔偿的相关主体亦为世纪互联。

微软向世纪互联许可相关技术、提供后台技术支持、就运营管理制度的进行移植、培训，确保中国用户能够在世纪互联运营的 Microsoft Azure 和 Office 365 的云服务中享受与国际水准一致技术、功能和服务。微软全球技术支持中心与世纪互联在人员培训、技术转移、技术支持和服务等方面展开了深入、广泛的合作，确保更稳定可靠的技术实现和最佳客户体验。世纪互联有 400 名经过微软培训和认证的工作人员，专职负责运营 Azure 和 Office 365 云服务。

角色和责任

微软

微软针对所有客户数据所能获得的非常有限的权力如下：

- 微软无法直接访问客户数据，从技术的角度来看，在未经世纪互联数据保管方根据相应访问控制策略的要求进行批准的情况下，也无从获得客户数据。由于这些是已经落实到位的物理和技术控制，因此甚至紧急时刻或服务中断等场景也会受到这些限制。
- 在未经世纪互联根据相应访问控制策略的要求进行批准的情况下，微软将无法从物理上访问存储有客户数据的数据中心。仅限极少数情况下，世纪互联需要微软的技术协助来对客户支持事件进行故障排除或解决技术问题，仅在解决问题所需的时间期限内授予此类访问权限。

世纪互联

世纪互联是独立运营的互联网数据中心提供商。世纪互联需负责控制对客户数据的全部访问（客户或其最终用户的访问除外），并执行需要访问存有客户数据的服务器所需的执行或监控任务。

世纪互联可以针对具体某一事件（例如为了解决某个具体的支持事件，或执行某个具体的升级操作）允许微软访问客户数据，但仅限于极少数的情况下。世纪互联所批准的访问有时效性，仅限解决问题的过程中有效，问题解决完毕后访问将被撤销。世纪互联会慎重监控并审计所批准的访问，并在问题成功解决后彻底终止访问。

执法请求

客户自己的信息无论存储在内部部署环境或云中，都应由客户自己进行控制。由世纪互联运营的 Microsoft Azure 和 Office 365 在线服务也是这样设计的，只有在遵守并符合中国法律并且在执法机关要求的情况下，世纪互联或客户自己，才能将客户数据共享给第三方。服务中建立的访问控制机制确保了在未经世纪互联批准的情况下，微软无法从技术上访问客户数据，也无法对可能用于访问客户数据的生产环境进行管理性访问。

所有执法部门或其他第三方有关访问客户数据的申请，均由 Azure 和 Office 365 在线服务的运营方世纪互联处理。

世纪互联作为在中国运营的独立互联网数据中心提供商，需要遵守中国法律，除非中国法律要求，世纪互联将不会披露客户数据。如果世纪互联在执法机关的要求下必须披露客户数据，除非法律禁止，世纪互联将采用商业上合理的努力立即通知客户，并提供披露数据的副本。

合规性

云服务的安全性、隐私，以及合规性是需要云服务供应商和客户共同承担的责任。为了降低客户在提供给最终用户安全与合规性方面的工作量，由世纪互联运营的 Microsoft Azure 和 Office 365 提供了可信赖的企业级云服务，同时为使用这些服务并需要符合相应应用标准的客户提供了必要的安全能力与灵活性。

由世纪互联运营的 Microsoft Azure 和 Office 365 提供了可信赖的基础服务，客户可以借助这些服务设计、构建、管理自己的安全云应用程序和基础结构。世纪互联负责确保整个平台和所提供的云服务可以满足中国客户对安全、隐私，以及合规性的各项需求。在服务交付后，将由客户负责确保自己内容的安全，并为自己的最终用户实施所需的安全策略。

世纪互联的运营流程已经为 Azure 和 Office 365 服务实施了强有力的隐私保护，并承诺会保护客户数据的隐私性。同时，透明服务管理帮助客户更清楚地了解自己的数据保存在哪里，什么人可以访问这些数据。



合规性认证

世纪互联正在通过不断的投入满足并维持日趋严格，并且不断变化的合规性要求。通过向客户提供合规的，通过了独立验证的云服务，世纪互联帮助客户更容易地确保云中运行的基础结构和应用程序能够满足合规性要求。世纪互联为使用云服务的客户提供了包括审计报告在内的有关安全与合规性项目的详细信息，借此帮助客户在满足自己的法律与制度要求的情况下使用 Azure 和 Office 365 服务。

(1) ISO/IEC 20000 和 ISO/IEC 27001 认证

由世纪互联运营的 Microsoft Azure 和 Office 365 已获得北京塞西认证有限责任公司针对 ISO/IEC 20000 和 ISO/IEC 27001 的认证，并且每年定期更新。ISO/IEC 27001:2005 证书确认世纪互联已实施此标准中定义的国际上认可的信息安全控制措施，包括有关启动、实施、维护和改进组织中的信息安全管理指南和一般原则。世纪互联承诺每年基于 ISO/IEC 27001:2005 进行认证。

(2) 信息系统安全保护等级

公安部授权的测评机构依据相关要求，对由世纪互联运营的 Microsoft Azure 和 Office 365 进行测评，其中 Azure 信息安全保护等级评定为第三级，Office 365 信息安全保护等级评定为第三级，并均已获得公安部备案。

(3) 可信云服务认证

在 2014 年 7 月首批可信云服务测评中，世纪互联运营的 Microsoft Azure 的虚拟机、存储和 SQL 数据库三项服务，通过了 SLA 服务协议框架内数据管理、业务质量及权益保障三大类共 16 项指标的测评。在运行的稳定性方面，世纪互联提供的 Azure 虚拟机提供有财务保障的、高达 99.95% 的服务等级协议。世纪互联还为用户提供按服务功能组建的仪表盘，是目前云计算市场唯一一家实时显示整个云平台的运行状态、供用户随时验证 SLA 承诺的云服务提供商。2015 年 1 月，在数据中心联盟发起的第三批可信云服务认证评选结果公布，世纪互联运营的 Microsoft Azure 又获得云引擎、全网负载均衡 2 项认证。Azure 凭借其超越 IaaS 平台之上的领先的 PaaS 平台云服务，是业内第一家获得全网负载均衡可信云服务认证的云服务，体现了世纪互联运营的 Microsoft Azure 领先的技术和安全可靠的运维和服务。



2015 年 7 月，在第四批可信云服务认证评选中，世纪互联运营的 Office 365 又荣获企业级电子邮件（Exchange Online）、文件共享（SharePoint Online）、共享日历和视频电话会议（Skype for Business）3 项可信云服务认证。Office 365 还凭借为用户提供了卓越的生产力和高效协作的高端云服务应用，荣获“可信云 2014-2015 年度行业云服务奖”的办公应用奖。

在 2016 年 3 月的第五批可信云服务认证评选中，由世纪互联运营的 Microsoft Azure 再次获得一项云备份可信云服务认证，与此同时也通过了 Office 365 在线应用服务——企业级电子邮件（Exchange Online）、文件共享（SharePoint Online）、共享日历与视频电话会议（Skype for Business）新增的“安全性、用户体验性能”2 项指标的认证，进一步印证了由世纪互联运营的 Microsoft Azure 和 Office 365 云服务拥有一流可靠的技术、安全稳定的运维、以及完善规范的服务体系，为中国用户提供高标准的安全、可信云服务。世纪互联蓝云此次获得认证的 Azure 云备份服务拥有 99.9% 的服务可用性，提供了稳定的运行能力。此外，通过两个数据中心提供 6 份数据备份，世纪互联蓝云成为业界提供最高备份数量的服务商之一，为用户提供可靠、安全、灵活、高效、稳定的云备份服务。

总结

由微软提供技术，世纪互联运营的 Microsoft Azure 和 Office 365 在线服务可以帮助客户以符合中国隐私与安全标准的方式充分运用云服务，同时确保用户消除有关自己的客户数据访问权的顾虑。Azure 和 Office 365 在技术创新、行业领先地位、安全性、隐私保护，以及合规性等方面为客户提供了长期承诺。通过使用 Azure 和 Office 365 在线服务，客户及其合作伙伴将获得可信赖的云环境，借助这样的云环境，充分获得云计算技术在性能、规模，以及经济效益等诸多方面的优势，同时在这样的云环境中，所有客户数据都存储在中国大陆境内，对客户数据的所有访问行为都由客户管理和控制。由世纪互联运营的 Microsoft Azure 和 Office 365 服务是针对中国市场专门设计，以安全性作为基本要求的产品和技术，能够为用户提供创新的技术选择，同时在兼顾功能与性能的前提下满足业务的安全和隐私需求。