《Microsoft 供应商数据保护要求》

适用范围

《Microsoft 供应商数据保护要求》（以下简称为“**DPR**”）适用于负责下列事务的各个 Microsoft 供应商，即：根据与 Microsoft 签订的合同条款（例如采购订单条款、主协议），负责就有关其履约事务（例如提供服务、软件许可证、云服务）处理 Microsoft 个人数据或 Microsoft 机密数据和/或使用 AI 系统（以下简称为“**执行**”、“**履行**”或“**履约**”）。

- 若 DPR 与供应商和 Microsoft 签署的合同协议中所述之要求存在冲突，则以 DPR 为准，除非供应商在合同中标示出可取代适用数据保护要求的正确条款（在这种情况下，以合同条款为准）。
- 若本文中所载之要求与任何法律或法规要求之间存在冲突，则以法律或法规要求为准。
- 若 Microsoft 供应商的身份为数据控制方，则 DPR 中的要求对该供应商可有所放宽。
- 若 Microsoft 供应商不负责处理 Microsoft 个人数据，而只负责处理 Microsoft 机密数据，就本 DPR 而言，对该供应商的要求可有所放宽。
- 本 DPR 的 K 部分（AI 系统）仅适用于向 Microsoft 提供涉及 AI 系统的服务的供应商。

全球范围内的数据传输

在不限制履行其他义务的情况下，供应商不得在全球范围内传输任何 Microsoft 个人数据，除非获得 Microsoft 的事先书面批准，且在任何情况下，供应商均应遵守本《数据保护要求》（包括标准合同条款），或在适用情况下，遵守由适当数据保护机构或欧盟委员会（视情况而定）批准且 Microsoft 自行决定采用或同意的其他适当的跨境数据传输机制。由 (i) 欧盟委员会采纳或由欧洲数据保护监管机构采纳并经欧盟委员会批准、(ii) 由英国依据英国通用数据保护法采纳并批准以及 (iii) 由瑞士依据《瑞士联邦数据保护法》采纳并批准的后续标准合同条款，或 (iv) 由瑞士、英国以及包括欧盟/欧洲经济区在内的司法辖区以外的其他司法管辖区政府正式采纳的、对全球范围内传输个人数据进行管辖的条款，均应一并遵循，且自采纳之日起对供应商具有约束力。供应商还将确保任何及所有子数据处理方（如标准合同条款中所定义）均遵守这些要求。

重要定义

本 DPR 中使用的下列术语具有如下含义。在本 DPR 中，“包括”、“例如”、“举例来说”等术语后的一系列示例可理解为“包括但不限于”，除非以“仅”或“唯一”等词进行限定。如需了解更多定义，请参阅本文件末尾处的术语表。

“**AI 系统**”是指一种工程系统，它应用优化的模型，使系统能够针对一组给定的人为定义目标做出预测*、建议或决策，从而影响与其互动的环境。这种系统能够以不同程度的自动化方式运行。* 预测可指各种类型的数据分析或生产（包括翻译文本、创建合成图像或诊断之前的电力故障）。

“**数据控制方**”是指负责确定个人数据处理目的和方法的实体。“数据控制方”包括企业、数据控制商（如 GDPR 中关于该术语的定义）以及数据保护法中的等效术语（根据上下文要求）。

“**Cookie**”是由网站和/或应用程序存储在设备上的小型文本文件，其中包含用于识别数据主体或设备的信息。

“**数据泄露事故**”是指：(1) 导致供应商或其分包商传输、存储或以其他方式处理的 Microsoft 个人数据或 Microsoft 机密数据被意外或非法销毁、遗失、篡改、未经授权披露或访问的安全违规行为；或 (2) 供应商在处理 Microsoft 个人数据或 Microsoft 机密数据时存在的安全漏洞，或第 64 号法案（2021 年，第 25 章）定义的机密泄露事故。

“**数据主体**”是指身份可被直接或间接识别的自然人，其中的常见识别方式包括姓名、身份证号、位置数据、

在线标识符或该自然人所特有的身体、生理、遗传、心理、经济、文化或社会身份等。

“**数据主体权利**”是指数据主体依法访问、删除、编辑、导出、限制处理或反对处理属于该数据主体的 Microsoft 个人数据的权利。

“**预期用途**”是指客户、供应商或最终用户使用系统的主要预期目的。可能为单一用途，也可能为多功能系统的多个用途。

“**法律**”是指具有管辖权的任何（联邦、州、当地或国际）政府机构颁布的所有适用法律、法规、条例、法令、规章、裁决、命令、判决、法典、法案、决议及要求。“**非法**”指任何违法行为。

“**Microsoft 机密数据**”是指一旦机密性或完整性遭到破坏，便可能对 Microsoft 造成重大声誉损害或财务损失的任何信息。此类机密数据包括 Microsoft 的硬件和软件产品、内部业务线应用程序、尚未公开发布的营销材料、产品许可证密钥及与 Microsoft 产品和服务相关的技术文件等。

“**Microsoft 个人数据**”是指由 Microsoft 进行处理或由其他方代表 Microsoft 进行处理的任何个人数据。

“**个人数据**”是指与数据主体有关的任何信息，以及依法构成“个人数据”或“个人信息”的任何其他信息。

“**处理**”是指对任何 Microsoft 个人数据或 Microsoft 机密数据执行的任何操作或一系列操作（无论是否通过自动方式），例如收集、记录、整理、结构化、存储、改编或更改、检索、查阅、使用、通过传输方式披露、传播或以其他方式提供、对齐或组合、限制、删除或销毁。“正在处理”和“已处理”均具有相应的含义。

“**数据处理方**”是指负责代表另一实体处理个人数据的实体，包括服务供应商、数据处理商（如 GDPR 中关于该术语的定义）以及数据保护法中的等效术语（根据上下文要求）。

“**受保护健康信息**”或“**PHI**”是指受《健康保险可携性和责任法案》(HIPAA) 保护的 Microsoft 个人数据。

“**红色小组测试**”是指一组测试人员聚集在一起，有意识地对系统进行探测，以确定其局限性、风险面和漏洞。更多信息，请访问 https://aka.ms/CustomerRedTeamingGuide。

“**分包商**”是指受供应商委托履行合同义务（涵盖履约事务）的第三方，包括未直接与 Microsoft 签约的供应商关联公司。

“**子数据处理方**”是指由 Microsoft 聘用以履行业务的第三方，其中履约事务包括处理 Microsoft 个人数据，此时 Microsoft 作为数据处理方。

供应商响应

供应商每年通过由 Microsoft 管理的一项在线服务来确认符合本要求。请参阅《SSPA 计划指南》，了解如何管理合规。

#	《Microsoft 供应商数据保护要求》	合规证明
	A 部分：管理	
1	Microsoft 与供应商之间签署的每份适用协议（例如主协议、工作说明书、采购订单及其他订单）中均包含与 Microsoft 个人或机密数据有关的隐私和安全数据保护内容（如适用），包括禁止供应商销售 Microsoft 个人数据以及在与 Microsoft 的直接业务关系范围之外处理 Microsoft 个人数据。 对于在履约过程中负责处理 Microsoft 个人数据的数据处理方或子数据处理方公司，协议中必须包含标的和数据处理的持续时间、性质和目的，以及 Microsoft 个人数据的类型、数据主体的类别及 Microsoft 的权利和义务。	供应商必须提交 Microsoft 与供应商之间签署的适用合同。 对于数据处理方和子数据处理方，适用协议（*例如*工作说明书、采购订单）中应包含关于数据处理的说明。 如果 Microsoft 确认聘用供应商参与处理 PHI，则供应商必须与 Microsoft 签订业务合作协议和/或其他协议。 附注：对于采购订单处于在途状态的公司，可在稍后的采购流程中添加必要的数据处理活动说明。
2	在 Microsoft 确认聘用供应商担任子数据处理方的角色后，供应商必须与 Microsoft 签订适用的数据保护协议。 附注：在本条适用的情况下，Microsoft 会在供应商简介中添加此角色头衔。	“标准合同条款”、“在线客户数据附录”、“供应商和合作伙伴专业服务数据处理附录”及/或“业务合作协议”。

#	《Microsoft 供应商数据保护要求》	合规证明
	A 部分：管理（续）	
3	针对有权访问 Microsoft 个人数据或机密数据的任何人（系统管理员、运营人员、管理人员、第三方等），应建立和维护隐私保护和安全培训制度，并每年开展一次培训。供应商还应确保，任何因供应商为 Microsoft 提供服务而需在 AI 系统内处理数据的人员，均已完成与其职责相关的 AI 培训。 附注：供应商人员需要完成由 Microsoft 部门开展的额外培训。	留存培训考勤记录，并应 Microsoft 的要求提供。 培训内容定期更新，包括隐私和安全原则，如事故预防意识（包括保护密码、登录监控、与下载恶意软件相关的风险以及其他相关的安全提醒）。供应商可使用 Microsoft 的 AI 素养资源进行 AI 培训。 培训合规证明文档应包括：与隐私监管要求、安全义务、AI 系统相关的培训证据，以及遵守适用合同要求、履行合同义务的证明。 IT 员工必须接受事故响应、模拟事故和自动响应机制方面的培训，以促进对危机情况的有效响应。 如果供应商处理的 Microsoft 个人数据包括 PHI，则培训内容必须包括 HIPAA 培训、安全提醒、地址登录监控、密码保护，以及业务合作协议允许的供应商获准使用和披露。
4	对于未能遵守供应商隐私与安全政策，或在 Microsoft 企业环境下工作时违反适用 Microsoft 政策的员工，应采取相应的惩戒措施。	描述针对不遵守行为的制裁（例如，直至并包括解雇）的隐私和安全政策文件。
5	仅根据 Microsoft 的书面指示处理 Microsoft 个人数据。这包括将 Microsoft 个人数据传输至第三国或国际组织，除非法律另有要求；在此类情况下，供应商（数据处理方或子数据处理方）在处理数据之前，应将相关法律要求告知 Microsoft（数据控制方），除非该法律以维护重大公共利益为由禁止发出此类信息。	供应商应汇编所有 Microsoft 书面说明（例如协议、工作说明书或订单文件）及其隐私和安全政策与程序的电子版本，并保存到方便参与履约的供应商员工和承包商访问的位置。

#	《Microsoft 供应商数据保护要求》	合规证明
	B 部分：通知	
6	供应商在代表 Microsoft 收集个人数据时，必须采用 Microsoft 的隐私声明。 隐私声明必须发布到醒目位置，方便数据主体查阅，以帮助他们决定是否向供应商提交其个人数据。 附注：若贵公司是数据处理活动的数据控制方（例如，网站未冠以 Microsoft 品牌），供应商可展示其自身的隐私声明。	供应商必须使用 fwdlink 指向发布的最新版 Microsoft 隐私声明。 应在需要收集用户个人数据的任何情境中发布隐私声明。 在适用情况下，可使用离线版本，并在收集数据之前提供。 所使用的任何离线隐私声明必须为最新发布的版本，且日期正确。 对于 Microsoft 员工服务，应使用 Microsoft 数据隐私声明。
	C 部分：选择与同意	
7	在收集个人数据之前，供应商必须征得数据主体的同意并妥善保管此类记录，以便开展所有数据处理活动（包括任何全新和更新的数据处理活动）。 供应商应监督首选项设置管理的效果，以确保遵守当地法律要求中关于接受首选项设置更改的最严格时限。	供应商应为数据主体演示如何就数据处理活动提供同意，且同意的范围应涵盖供应商处理数据主体个人数据的所有活动。 供应商应为数据主体演示如何撤销对数据处理活动的同意。 在启动新的数据处理活动之前，供应商应演示如何选择首选项设置。 附注：可将与用户互动的屏幕截图；可将服务试用或技术文件查阅机会等作为证据。

#	《Microsoft 供应商数据保护要求》	合规证明
	C 部分：选择与同意（续）	
8	使用 Cookie（和/或在设备上存储或检索数据、或以类似方式实现用户跟踪的同类技术）的网站，在针对数据主体的浏览器或设备使用或放置 Cookie 之前，必须依法取得数据主体的同意。 若供应商负责创建和管理 Microsoft 网站和/或应用程序或带有 Microsoft 品牌标识的站点，则必须根据 Microsoft 隐私声明中的承诺和当地法律要求，向数据主体提供关于使用 Cookie 的公开通告和数据主体可进行的选择。 若网站的目标用户群体位于欧盟/欧洲经济区、颁布适用隐私保护法律的其他地区以及采用 Microsoft 隐私声明的任何地区内，本要求适用。	必须记录各种 Cookie 的用途，且必须告知用户所采用的 Cookie 类型。 • 若使用会话 Cookie 便足以满足需求，则不得使用持久性 Cookie。 • 若使用持久性 Cookie，则 Cookie 的有效期不得超过 13 个月（自用户访问网站之日起）。 验证是否符合适用的欧盟法律，例如： • 使用标签公约、隐私声明中的“隐私和 Cookie”， • 在出于广告等目的使用“非必要”Cookie 之前，必须获得用户的明确同意，以及 • 此类同意的有效期不得超过 6 个月，或必须在 6 个月后重新获得用户的同意。
	D 部分：收集	
9	供应商必须对 Microsoft 个人数据和/或机密数据的收集进行监督，以确保仅收集履行服务所必需的数据。	供应商应提供证明文件，以展示所收集的 Microsoft 个人数据和/或机密数据对于履行服务必不可少。 一经要求，供应商应向 Microsoft 提交书面证据。
10	在从未成年人（如适用司法辖区所定义）处收集数据之前，供应商必须根据当地隐私保护法律的规定征得其父母/监护人的同意。	供应商应提供关于征得未成年人父母/监护人同意的证明文件。 一经要求，供应商应向 Microsoft 提交书面证据。
11	如果供应商从 Microsoft 收到可识别性经处理后被降低的数据集，包括假名、无法识别 (NPI)、无法关联的假名、聚合、匿名或与这些分类之一相关的任何术语（如去识别），供应商将按收到时的状态保留数据。	供应商不会提高数据集的可识别性（即通过结合其他数据集的方式重新识别某个数据集中的个人的身份等）。 供应商有去识别化/匿名化数据政策/流程。

#	《Microsoft 供应商数据保护要求》	合规证明
	E 部分：数据保留	
12	确保 Microsoft 个人数据和机密数据的保留时间不得超过履行服务所需的时间，除非法律要求继续保留 Microsoft 个人数据和/或机密数据。	供应商应遵守明文规定的数据保留政策或合同（如工作说明书、采购订单）中由 Microsoft 提出的数据保留要求。 一经要求，供应商应向 Microsoft 提交书面证据。
13	在履约结束后或应 Microsoft 的要求，供应商必须确保向 Microsoft 归还或销毁由其持有或控制的 Microsoft 个人数据和机密数据，一切由 Microsoft 酌情决定。 在应用程序内，必须制定相关流程，以确保用户从应用程序内明确删除数据或基于数据龄期等其他因素删除数据时，数据会被安全地删除。 在需要销毁 Microsoft 个人数据或机密数据时，供应商必须通过焚烧、粉碎或撕碎等方式销毁包含 Microsoft 个人数据和/或机密数据的实物资产，以使其中的信息无法读取或重建。	留存关于处置 Microsoft 个人数据和机密数据的记录（其中可包括交给 Microsoft 进行销毁的数据）。 若 Microsoft 要求或请求销毁个人数据或机密数据，在销毁后，必须提供由供应商管理人员签署的销毁证明。
	F 部分：数据主体	
	数据主体依法享有某些权利，包括访问、删除、编辑、导出、限制及拒绝处理其个人数据的权利（以下简称为“数据主体权利”）。当数据主体希望对其 Microsoft 个人数据依法行使所赋予的权利时，供应商必须协助 Microsoft 或代表 Microsoft 采取下列措施：	
14	在适当情况下，通过适当的技术和组织措施，协助 Microsoft 履行其义务，以响应数据主体希望行使其作为数据主体权利的请求，不得无故拖延。 除非 Microsoft 另有指示，否则供应商均应将直接与其联系的所有数据主体转给 Microsoft，以行使他们作为数据主体的权利。	供应商应妥善留存关于已支持数据主体行使权利的书面流程和程序证明。 供应商应留存书面检验证据。一经要求，供应商应向 Microsoft 提交证据。

#	《Microsoft 供应商数据保护要求》	合规证明
	F 部分：数据主体（续）	
15	在直接响应数据主体的请求或供应商采用在线自助服务机制时，供应商应制定相应的流程和程序，以识别提出请求的数据主体身份。	供应商应将用于识别 Microsoft 数据主体身份的方法形成书面文件。 一经要求，供应商应向 Microsoft 提交书面证据。
16	若 Microsoft 要求查找关于某个数据主体的 Microsoft 个人数据，且这些数据无法通过在线自助服务机制获取，供应商必须尽一切合理努力查找所请求的数据，并保留详尽记录，以证明进行了合理的查找。	供应商应留存关于制定相关程序的书面证据，以确定是否持有 Microsoft 个人数据，并应 Microsoft 的要求，提供这些证据。 供应商应留存相关记录，以证明为满足数据主体行使权利的要求而采取了相关措施。 文件中应包括： • 提出请求的日期和时间， • 为响应请求而采取的措施，以及关于何时通知 Microsoft 的记录。 供应商应根据 Microsoft 的要求提供记录保存的证据。
17	供应商应将数据主体为了获得对其 Microsoft 个人数据的访问权或行使其他权利而必须采取的措施告知数据主体。	供应商应留存关于与数据主体沟通及 Microsoft 个人数据访问程序的书面证据。供应商应留存相关书面证据，并应 Microsoft 的要求提交这些证据。
18	供应商应记录数据主体请求行使权利的日期和时间及其为响应此类请求所采取的措施。 若按照 Microsoft 的指示拒绝数据主体的请求，则应向数据主体提供书面解释说明。 一经要求，供应商应向 Microsoft 提交关于数据主体请求的记录。	供应商应留存关于数据主体请求访问/删除数据的记录，并记录数据主体对其 Microsoft 个人数据所做的更改。 对于拒绝数据主体请求的情况，应妥善记录，并保留关于 Microsoft 审批的证据。 供应商应提供相关证据，以证明已妥善保存数据主体的请求及拒绝其访问 Microsoft 个人数据的记录。
19	供应商必须协助 Microsoft 为经身份验证的数据主体以适当的打印、电子或口头形式获取所请求的 Microsoft 个人数据副本。	供应商应以易于理解的格式和对数据主体和供应商均便捷的形式向数据主体提供其 Microsoft 个人数据。

#	《Microsoft 供应商数据保护要求》	合规证明
	F 部分：数据主体（续）	
20	供应商必须采取合理的预防措施，确保向 Microsoft 或经身份验证的数据主体披露的 Microsoft 个人数据不能用于识别他人身份。	供应商应留存关于为了避免违反协议条款识别数据主体的身份所制定的相关预防措施程序的书面证据。一经要求，供应商应向 Microsoft 提交相关证据。
21	若数据主体认为其 Microsoft 个人数据不完整和不准确，供应商必须向 Microsoft 上报这一问题，并在必要时配合 Microsoft 解决问题。	供应商应记录出现分歧的情况，并向 Microsoft 上报问题。 一经要求，供应商应向 Microsoft 提交书面证据。
22	对于数据主体的访问请求，供应商必须保存已经或将要与之共享 Microsoft 个人数据的所有接收者的记录。	一经要求，供应商应提供 Microsoft 个人数据的所有实际接收者和可能的第三方接收者的列表。
	G 部分：分包商	
	若供应商意欲聘用分包商处理 Microsoft 个人数据或机密数据，供应商必须：	
23	在分包服务或对服务进行任何变更（如增加或替换分包商）之前，通知 Microsoft。	确认是否按照适用合同（如工作说明书、附录、采购订单）或 SSPA 数据库中所要求，仅由 Microsoft 所熟知的公司处理 Microsoft 个人数据和/或机密数据。供应商可线上发布其分包商名单，并在 SSPA 数据库中添加指向此页面的链接。
24	要求分包商以书面形式同意相关条款，此等条款提供的保护力度不得低于供应商与 Microsoft 订立的协议所载条款的规定（包括隐私和数据保护条款）。	一经要求，供应商应向 Microsoft 提交与分包商签署的合同。

#	《Microsoft 供应商数据保护要求》	合规证明
	G 部分：分包商（续）	
25	记录由分包商处理的 Microsoft 个人数据和机密数据的性质和范围，确保仅收集履行服务所需的信息。	供应商应妥善保管关于向分包商披露或传送 Microsoft 个人数据和机密数据的文件。 一经要求，供应商应向 Microsoft 提交书面证据。
26	分包商应仅出于履行供应商与 Microsoft 之间达成之合约的目的，处理 Microsoft 个人数据或机密数据。 如果 Microsoft 个人数据属于 PHI 性质，还需要与分包商签订业务合作协议，以限制分包商对 Microsoft 个人数据的处理，并以与 Microsoft 和供应商之间的业务合作协议相同的方式保护 Microsoft 个人数据的机密性和安全性。	供应商应提交证明文件，以示向分包商披露的 Microsoft 个人数据对于履行服务必不可少。 一经要求，供应商应向 Microsoft 提交书面证据，如适用，包括业务合作协议。
27	一旦得知分包商出于履约以外的任何其他目的处理 Microsoft 个人数据或机密数据，应立即通知 Microsoft。	供应商应证明已向分包商提供了报告滥用 Microsoft 数据的相关说明和方法。 一经要求，供应商应向 Microsoft 提交书面证据。
28	若供应商代表 Microsoft 从第三方处收集个人数据，则供应商必须核实第三方数据保护政策和惯例是否与供应商和 Microsoft 之间的合同和本 DPR 一致。	供应商应提供相关证明，以证明对第三方的数据保护政策和惯例开展了尽职调查。 一经要求，供应商应向 Microsoft 提交书面证据。

#	《Microsoft 供应商数据保护要求》	合规证明
	H 部分：质量	
29	供应商必须保证所有 Microsoft 个人数据完好无损，同时确保数据准确、完整并与所述之数据处理目的密切相关。	供应商应证明，在收集、创建及更新 Microsoft 个人数据时，已制定了验证数据的相关程序。 供应商应证明已制定了相关监督、信息系统活动审查和采样程序，以持续验证数据的准确性，并在必要时进行更正。 一经要求，供应商应向 Microsoft 提交书面证据。
	I 部分：监督和执行	
30	供应商应制定事故应急预案，其中要求供应商在发现数据泄露事故后，必须按照合同要求、适用隐私法律或尽快通知 Microsoft（以较早者为准）。 供应商必须按照 Microsoft 的要求或指示，配合 Microsoft 对数据泄露事故开展任何调查、减轻损害或采取补救措施，包括向 Microsoft 提供事故摘要、数据泄露详情、被访问的数据范围以及所使用的缓解措施。可能还需要访问供应商人员或进行取证审查所需的硬件。 供应商应在 SupplierWeb 的安全联系人栏中填写合适的人员信息，以便在发生安全事件时能够迅速进行对接。 附注：请参阅《SSPA 计划指南》，了解在发生数据泄露事故时如何通知 Microsoft。	供应商应制定事故应急预案，其中包括通知客户 (Microsoft) 的步骤，如本章节所述。 一经要求，供应商应向 Microsoft 提交书面证据。
31	实施补救计划并监督每起数据泄露事故的解决情况，以确保及时采取适当的纠正措施。	供应商应制定明文规定的应对数据泄露事故直至事故终止的程序，其中包括及时向 Microsoft 更新，直至问题得到解决，并提供事故后审查。 一经要求，供应商应向 Microsoft 提交书面证据。
#	《Microsoft 供应商数据保护要求》	合规证明

I 部分：监督和执行（续）		
32	若 Microsoft 是 Microsoft 个人数据的控制方，则供应商应制定正式的投诉流程，以应对涉及 Microsoft 个人数据保护的所有投诉。	供应商应实施相关流程，受理涉及 Microsoft 个人数据的投诉，并明文规定投诉程序，以解决投诉。 一经要求，供应商应向 Microsoft 提交书面证据。
J 部分：安全性		
	根据行业最佳实践和法律要求，供应商必须制定、实施及完善信息安全计划（包括政策和程序），以保护并保障 Microsoft 个人数据和机密数据的安全。供应商的安全计划必须符合 下述标准（第 33 项 - 第 50 项要求）。 如果 Microsoft 个人数据属于 PHI 性质，供应商还必须针对影响 PHI 安全性的环境和操作变化定期进行技术和非技术评估，以确定供应商的政策和程序在何种程度上符合 HIPAA 安全规则的要求。	可用有效的 ISO 27001 认证代替 J 部分：安全性。 附注：您需要上传证书以申请替代。
33	执行网络安全评估，每年一次，其中包括： • 评估 Microsoft 个人数据的机密性、完整性和可用性的潜在风险和漏洞，并实施降低风险的措施， • 审查网络环境是否发生重大变化，例如采用了新的系统组件、网络拓扑及防火墙规则，和 • 保留更改日志。	供应商应将网络评估、更改日志及扫描结果记录在案。 根据要求，更改日志必须能够跟踪更改、提供关于更改原因的信息，并包括指定批准人的姓名和职务。一经要求，应能够提供过去 90 天的记录。
34	供应商应制定、传达及实施移动设备使用策略，以保护并限制在移动设备上访问或使用 Microsoft 个人数据或机密数据。	在处理 Microsoft 个人数据或机密数据需要用到移动设备时，供应商应演示如何应用符合要求的移动设备使用策略。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
35	用于支持服务履行、安全和操作的所有实物和虚拟资产均必须记录在案，并指定保管人。 供应商应负责保存信息资产的清单；确保资产的使用是恰当且经过授权的；以及在资产的整个生命周期内为其提供适当的保护级别。	用于支持服务履行、安全和操作的设备资产清单。资产清单中应包括： • 设备位置， • 设备资产上所包含的数据类别， • 聘用协议或业务协议终止时的资产收回记录， • 数据存储媒体不再使用后的处置记录，以及 • 供应商人员使用 @microsoft.com 凭证访问 Microsoft 数据时使用的所有实物和虚拟设备必须由 Microsoft 全权管理，除 Microsoft 提供的软件外，不得安装任何其他安全软件。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
36	制定并完善访问权限管理程序，以防未经授权访问由供应商掌管的任何 Microsoft 个人数据或机密数据。	供应商应证明已实施访问权限管理计划，其中包括： • 访问控制程序， • 身份识别程序， • 尝试访问失败后的锁定程序， • 无活动后自动注销， • 用于选择身份验证凭据的可靠参数， • 在用户的雇佣关系终止后 48 小时内停用其帐户（包括员工或分包商使用的帐户） • 强密码控制措施，以强制规定密码长度和复杂性，并防止重复使用，以及 • 使用多因素身份验证 (MFA)。 供应商应证明已制定相关流程，以审查用户对 Microsoft 个人数据和机密数据的访问权限，并执行“最小权限原则”。此流程应具体包括： • 清晰定义用户的角色， • 各种角色访问权限的审批和验证程序， • 验证角色中具有 Microsoft 数据访问权限的用户是否持有允许其加入该群组/角色的证明文件，以及 • 严格禁止共享帐户或密码。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
37	制定并实施补丁管理程序，其中应对用于处理 Microsoft 个人数据或机密数据的系统优先升级安全补丁。具体程序包括： • 每月进行漏洞扫描，并提供高水平合规报告以显示前 12 个月的每月扫描情况， • 制定风险控制方案，以优先升级安全补丁， • 能够处理并实施紧急补丁， • 适用于操作系统和服务器软件，如应用程序服务器和数据库软件， • 记录补丁所化解的风险并追踪任何异常，以及 • 开发公司不再提供技术支持的软件的停用要求。	供应商应证明实施的补丁管理程序满足此项要求，并至少涵盖下列内容： • 记录严重性定义，并将其分配给更新，以确定部署的优先级。 • 制定明文规定的程序，以实施紧急补丁。 • 补丁管理记录，追踪批准和异常情况，包括补丁合规数据。一经要求，应能够提供过去 90 天的记录。
38	若设备（包括服务器、生产和培训用台式计算机）连接到处理 Microsoft 个人数据和机密数据的网络，应安装防病毒和反恶意软件，以防止感染潜在的有害病毒和恶意软件应用程序。防病毒和反恶意软件应定期实施补丁和更新。 每日更新反恶意软件定义或按照防病毒/反恶意软件供应商的指示进行更新。附注：此项要求适用于所有操作系统，包括 Linux。	留存相关记录，以证明使用的防病毒和反恶意软件处于活动状态。 附注：此项要求适用于所有操作系统。
39	为 Microsoft 开发软件的供应商必须在软件构建过程中采用安全设计原则。	供应商技术规范文件中应包括开发周期中进行安全验证的检查点。 供应商使用某种形式的代码扫描来提醒存在的明显缺陷。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
40	采用“数据丢失防护”（以下简称为“DLP”）计划，在应用程序、系统和基础设施级别防止系统被入侵、数据丢失及其他未经授权的活动。供应商必须对数据进行适当的分类、标记和保护，且必须监控用于处理 Microsoft 个人数据或机密数据的信息系统是否发生入侵、数据丢失及其他未经授权的活动。DLP 计划至少应包含下列要求： • 若您负责保留 Microsoft 个人数据或机密数据，则需要使用行业标准主机、网络和基于云的入侵检测系统（以下简称为“IDS”）， • 需要部署并配置高级“入侵防护系统”（以下简称为“IPS”），以监控和主动阻止数据丢失， • 在系统被破坏的情况下，需要对系统进行分析，以确保修补任何残余漏洞， • 描述用于监控系统危害检测工具的规定程序， • 制定在发现数据泄露事故的情况下需要执行的事故应急预案和管理流程，以及 • 针对未经授权下载和使用 Microsoft 个人数据或机密数据的情况，需要（向停止为供应商履约的所有供应商员工和分包商）进行传达。	部署形成书面文件的 DLP 计划，并制定适当程序，以防发生系统被入侵、数据丢失及其他未经授权的活动（至少应包括本章节所述的所有项目）。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
41	通过以下方式保护网络和支持系统中的信息： • 实施控制措施，防止未经授权的访问。 • 确保跨网络数据传输的安全性。 • 进行网络流量细分，降低风险敞口。 • 维护最新的网络拓扑图和配置基准。 • 分配明确的网络管理角色，使其与一般的 IT 运维工作相分离。	供应商应证明： • 形成文档的网络安全程序。 • 网络拓扑图和配置文件。 • 显示监控和事件响应的日志。 • 细分和加密控制措施的证据。
42	供应商必须确保在开发过程的任何阶段都不会将机密嵌入或硬编码到软件中。	供应商应制定明文规定的程序，以确保在测试或生产环境中，用户名、密码、SSH 密钥、API 访问令牌等机密永远不会合并到源文件或配置文件中。 供应商应证明： • 使用受支持的当前版本的凭证暴露防护工具，例如 GitHub 高级安全 (GHAS) 或类似服务或工具。 • 保证如果源文件或配置文件错误地包含机密，则这些机密在发现时立即被记录为吊销。 • 保证任何替换凭证或辅助凭证未被推送回代码中。 • 记录任何假阳性结果及其补救措施。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
43	供应商必须确保制定备案流程，以保护 Microsoft 个人数据和机密数据免遭未经授权的使用、访问、披露、篡改及销毁。	供应商应证明制定了响应和恢复程序，并详细说明企业如何应对导致破坏性后果的事故，并根据经管理层批准的信息安全持续性目标，保证信息安全始终处于预定水平。 供应商应证明其制定并实施了相关程序，用于定期备份、安全存储（物理存储及通过使用数据加密）及有效恢复关键数据。
44	制定并检验业务连续性和灾难恢复计划。	灾难恢复计划必须包括以下内容： • 制定标准，以确定某个系统对于供应商的业务运营是否至关重要。 • 根据制定的标准列出关键系统，一旦发生灾难，必须针对这些系统进行恢复。 • 针对各关键系统制定灾难恢复程序，以确保即使对系统并不熟悉的工程师也可在 72 小时内恢复应用程序。 • 每年对灾难恢复计划进行一次（或多次）检验和审查，以确保能够实现恢复目标。
45	在授予相关人员访问 Microsoft 个人数据或机密数据的权限之前，要对其进行身份验证，并确保所授予的访问权限仅可由该人员用于支持履约的活动。	确保所有用户 ID 均具有唯一性，且每个 ID 均采用行业标准的身份验证方法，例如 Azure Active Directory。 必须采用多因素身份验证 (MFA) 方法，例如安全密钥、基于手机的身份验证器或智能卡等。 将信息安全计划形成书面文件，其中应涵盖相关流程，用于确保供应商的全体员工和分包商对 Microsoft 个人数据或机密数据的访问期限不得超过履行服务所必需的时长。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
46	供应商应在整个招聘和派驻流程中，通过语音及外貌特征核实其面试、聘用并派驻至 Microsoft 的员工为同一人。员工的地址信息必须与其银行信息以及任何设备的邮寄地址相匹配。	在开始工作前，该员工必须由负责其面试与录用的供应商联系人陪同，与其主要 Microsoft 联系人会面。主要 Microsoft 联系人须在正常工作时间内与该员工进行定期的实时音视频互动。 对于任何设备邮寄，供应商应记录核实信息，证明邮寄地点为实际可居住的住所（即非转运点），且与员工提供用于银行服务的地址一致。
47	在网络传输过程中，供应商必须采用“传输层安全协议”（以下简称为“TLS”）或“Internet 协议安全”（“IPsec”）加密方法，保护出于履约之目的而处理的所有数据。 在 NIST 800-52 和 NIST 800-57 标准中介绍了这些方法；也可采用等效的行业标准加密方法。 供应商不得同意通过未经加密的方式传输任何 Microsoft 个人数据或机密数据。	必须制定和执行用于创建、部署及替换 TLS 或其他证书的流程。
48	用于访问或处理 Microsoft 个人数据或机密数据的所有供应商设备（笔记本电脑、工作站等）必须启用全磁盘加密。	对所有设备进行加密，以使所有用于处理 Microsoft 个人数据或机密数据的客户端设备符合 BitLocker 或其他等效的行业磁盘加密解决方案。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
49	必须制定相关制度和程序（采用行业现行标准，如 NIST 800-111 标准中所述），对处于静态（存储时）的**任何及所有** Microsoft 个人数据和/或机密数据进行加密，具体示例包括但不限于： • 凭证数据（例如用户名/密码） • 支付工具数据（例如信用卡和银行账号） • 个人移民相关数据 • 医疗档案数据（例如用于身份识别的病历号或生物识别标记或标识符，如 DNA、指纹、眼视网膜和虹膜、声纹、面部纹理及手型） • 政府签发的身份识别信息（例如社会保障号或驾照号） • 属于 Microsoft 客户的数据（例如 SharePoint、O365 文件、OneDrive 客户） • 与尚未公布的 Microsoft 产品相关的材料 • 出生日期 • 儿童档案信息 • 实时地理数据 • 个人（非办公）实际地址 • 个人（非办公）电话号码 • 宗教信仰 • 政治观点 • 性取向/偏好 • 安全问题答案（例如 2fa、密码重置） • 母亲的婚前姓	检查是否对处于静态的 Microsoft 个人数据和机密数据进行了加密。

#	《Microsoft 供应商数据保护要求》	合规证明
	J 部分：安全性（续）	
50	将开发或测试环境中使用的所有 Microsoft 个人数据进行匿名化处理。	不得将 Microsoft 个人数据用于开发或测试环境；若别无选择，必须将个人数据进行匿名化处理，以防识别数据主体的身份或滥用个人数据。 附注：匿名化数据不同于假名化数据。匿名化数据是指数据无法关联到已确定身份或身份可识别的自然人，在这种情况下，个人数据将无法用于识别数据主体的身份。 如果 Microsoft 个人数据属于 PHI 性质，则匿名化必须符合 HIPAA 去识别化标准。
	K 部分：AI系统	
51	如果在提供服务时涉及 AI 系统，供应商必须与 Microsoft 签订适用的 AI 系统条款。 对预期用途的任何更改都必须及时披露，不得无故拖延，并至少每年审查一次，以确保准确性和合规性。	AI 系统合同条款在 Microsoft 与供应商签订的合同中列明。
52	供应商在为 Microsoft 工作期间，不得设计、开发、上市、投入使用或使用任何被视为“禁止行为”的 AI 系统。	一经要求，供应商应向 Microsoft 提交书面证据。

#	《Microsoft 供应商数据保护要求》	合规证明
	K 部分：AI 系统（续）	
53	供应商应制定 AI 系统事故应急预案，其中要求供应商在意识到数据泄露事故或发现的故障会对 AI 系统列出的任何预期用途造成不利影响时，必须按照合同要求、适用隐私法律或尽快通知 Microsoft（以较早者为准）。 注：请参阅《SSPA 计划指南》，了解在发生数据泄露事故时如何通知 Microsoft。	供应商应制定 AI 系统事故应急预案，其中包括所有端点的以下内容： • 本要求中所述的通知客户 (Microsoft) 的步骤。 • 系统回滚计划，包括回滚整个系统所需的时间。 • 对关闭功能的支持，包括关闭功能所需的时间。 • 更新和发布每个模型更新的流程，包括系统更新所需的时间。 • 有关如何通知客户、合作伙伴和最终用户系统变更、故障理解更新及其最佳缓解措施的流程。 一经要求，供应商应向 Microsoft 提交书面证据。
54	供应商应备有透明度披露文件。	一经要求，向 Microsoft 提供透明度披露文件。
55	**签署的协议：**与 AI 供应商合作时，企业应在签署的协议中制定明确的合同条款。这些协议应明确涉及数据处理、机密、知识产权、责任及事件响应。	一经要求，供应商应向 Microsoft 提交书面证据，如适用，包括协议。
56	**责任：**为 AI 系统在部署期间及之后的运行、监督和风险管理分配并明确定义职责与问责机制。指定方必须处理伦理疑虑、偏见和新出现的问题，并确保对 AI 模型进行定期监控和审计，以持续保持符合组织标准和伦理标准。	供应商应编制描述责任 AI 计划的文件，包括个人或团体的职责和责任。 供应商还应指定专人或团队负责确保 AI 系统合规性，并备有说明合规权限与问责制的文件。 一经要求，供应商应向 Microsoft 提交书面证据。

#	《Microsoft 供应商数据保护要求》	合规证明
	K 部分：AI 系统（续）	
57	**风险评估**：执行隐私、安全和/或责任 AI 风险评估，以考虑潜在的偏差、安全漏洞和意外后果。	供应商应留存风险评估的证据，或类似的文件或报告，包括系统演变的测试和监控，以及每年的持续维护，从而改进已知或已发现的错误，并实施其他必要的补救措施或技术控制，从而保持安全和隐私合规性。 一经要求，供应商应向 Microsoft 提交书面证据。
58	**透明度和可解释性**：AI 系统必须具有透明度和可解释性。供应商必须提供有关决策制定方式的见解。披露应鼓励模型架构、培训数据和决策过程的透明度。	供应商应记录所有系统故障报告、损坏、幻觉或报告的偏离预期目的的滥用情况，并提供为解决问题所采取措施的证据。 一经要求，供应商应向 Microsoft 提交书面证据。
59	**监控和调整**：供应商必须证明对 AI 系统的持续监控，并在出现新的风险时调整和更新 AI 系统。	供应商应记录所有系统故障报告、损坏、幻觉或报告的偏离预期目的的滥用情况，并提供为解决问题所采取措施的证据。 一经要求，供应商应向 Microsoft 提交书面证据。

#	《Microsoft 供应商数据保护要求》	合规证明
	K 部分：AI 系统（续）	
60	供应商必须提供所要求的披露、报告或其他类似文件，其中包含每种预期用途所要求的所有错误类型、性能指标定义、数据性能、安全性和可靠性指标。	• 定义并提供会影响每种预期用途的每个操作因素的可接受误差范围，以及会缩小可接受范围或降低可接受误差率（包括假阳性和假阴性误差率）从而影响这些预期用途的任何其他操作因素。 • 确定操作因素和/或预期用途，包括系统输入、使用和操作环境的质量，这些对于在部署环境中可靠、安全地使用系统至关重要。 • 记录系统设计中有效控制措施的实施情况，以防止自动化偏差（过度依赖系统产生的输出结果的可能趋势）。 • 记录任何系统限制、输入或输出数据模型限制或可预测的故障，包括系统设计或评估时未考虑的可能影响预期用途的用途。 • 记录针对众所周知的 AI 风险，如推理操纵（“越狱”）、模型操纵（如数据中毒）和推理信息披露（如提示提取），已实施的缓解和控制措施。 • 系统准确性和性能的证据，以及这些结果在不同情况下的通用程度。

#	《Microsoft 供应商数据保护要求》	合规证明
	K 部分：AI 系统（续）	
61	供应商将更新透明度披露，包括预期用途，并在以下情况下通知 Microsoft： • 增加新用途， • 功能变化， • 产品进入新的发布阶段， • 发现或应用有关影响预期用途的可靠、安全性能的新信息， • 提供有关系统准确性和性能的新信息。	供应商在更新透明度披露时应制定计划，其中包括通知 Microsoft 的步骤，如本章节所述。
62	作为透明度披露的一部分，供应商必须为每个 AI 系统或数据模型制定、记录并维护标准操作程序和系统健康监控框架，其中包括： • 采用的监控方法与工具，包括通过数据存储库、系统分析及关联告警生成的数据与洞察。 • 重现系统故障以支持故障排除和预防未来故障的流程。 需监控的事件、审查与响应的优先级标准， 预期的审查频率， 问题解决时限。 • 收集反馈的流程，包括关于故障及疑虑的信息。 • 将包括开源软件在内的第三方 AI 组件保持最新状态。	供应商已将本部分所述的每个 AI 系统将遵循的系统健康监控政策和程序记录在案。 一经要求，供应商应向 Microsoft 提交书面证据。

#	《Microsoft 供应商数据保护要求》	合规证明
	K 部分：AI 系统（续）	
63	如果在 AI 系统使用前或使用过程中的任何时候发现该系统不适合预期用途的证据，供应商将： • 从面向客户的材料中删除预期用途，并让当前客户了解该问题，采取行动弥补已发现的差距，或停止使用该系统， • 修订与预期用途相关的文档， • 向客户公布修订后的文档。	供应商应制定出现如本节所述的预期用途故障时应遵循的政策和程序。

术语表

“授权代表”是指具有适当权限，可代表公司签字的人员。此人应具备必要的隐私保护和安全知识，或在提交针对 SSPA 计划的应对措施之前，应咨询主题领域的专家。此外，授权代表在 SSPA 表格上添加自己的名字，即表示其证明自己已经阅读并理解 DPR。

“EUDPR”是指欧洲议会和欧洲理事会于 2018 年 10 月 23 日颁布的第 2018/1725 号 (EU) 条例，旨在在欧盟机构、团体、办事处及代理机构处理个人数据时保护自然人的权益并确保此类数据的自由传送，同时废除第 45/2001 号 (EC) 条例和第
1247/2002/EC 号决议。

“自由职业者”是指通过数字平台或其他方式执行按需任务或服务的个人。

“GDPR”是指欧洲议会和欧盟理事会于 2016 年 4 月 27 日颁布的第 2016/679 号 (EU) 条例，旨在在处理个人数据时保护自然人的权益并确保此类数据的自由传送，同时废除了第 95/46/EC 号指令（《通用数据保护条例》）。

“人为监督”是指供应商指定的人为监督类别，以及在 AI 系统内部检测到故障时可用于预期用途的干预级别：

- 人在回路中（在系统每个决策周期中的人为干预能力）
- 人在回路上（在系统设计周期和监测系统运行期间的人为干预能力）
- 人在指挥（监督 AI 系统的整体活动并决定在特定情况下何时以及如何使用 AI 系统的能力）。

“隐私数据保护要求”是指涉及任何个人数据 (a) 隐私和数据安全；或 (b) 数据使用、收集、保留、存储、保护、披露、传送、处置及其他处理的 GDPR、EUDPR 及欧盟/欧洲经济区当地的数据保护法律、《加利福尼亚州消费者隐私保护法》、《加利福尼亚州民法典》§ 1798.100 等（以下简称为“*CCPA*”）、英国《2018 年数据保护法》及在英国适用的任何相关或后续法律、法规及其他法律要求。

“欧盟示范条款”和“标准合同条款”是指 (i) 用于规管将个人数据传送至位于无法确保提供适当数据保护级别的第三国的数据处理方的标准数据保护条款，该条款如 GDPR 第 46 条所述并由欧盟委员会于 2021 年 6 月 4 日颁布的第 2021/914 号 (EU) 决议批准；
(ii) 已经 (a) 由欧盟委员会采纳、(b) 由欧洲数据
保护监察专员采纳并获得欧盟委员会批准、(c) 由英国依据英国通用数据保护法采纳、(d) 由瑞士依据《瑞士联邦数据保护法》采纳、(e) 由瑞士、英国以外司法辖区内的政府以及包括欧盟/欧盟经济区在内的司法辖区采纳的任何后续标准合同条款，此类条款将规管在国际范围内传输个人数据的情况，供应商应一并遵循上述条款，且自采纳之日起对其具有约束力。

“网站托管”网站托管服务是指在 Microsoft 的域内，代 Microsoft 创建和/或维护网站的一种在线服务，即供应商为 Microsoft 提供创建和维护网站并使网站在互联网上可供访问所需的所有材料和服务。“网络托管服务供应商”或“网络主机服务商”是指为使网站或网页可在互联网上查看而提供所需工具和服务（如 Cookie 或用于推送广告的网络信标）的供应商。