Microsoft 供应商数据保护要求

适用性

Microsoft 供应商数据保护要求（“DPR”）适用于符合以下情况的每位 Microsoft 供应商： 根据该供应商与 Microsoft 签署的合同条款（例如采购订单条款、主协议）处理与该供应商的绩效（例如配置服务、软件许可、云服务）相关的 Microsoft 个人数据或 Microsoft 机密数据（“执行”、“表现”或“绩效”）。

- 如果本文所包含的要求与供应商和 Microsoft 签署的合同协议中指定的要求有冲突，则以 DPR 为准，除非适用的供应商以 DPR 鉴证书的形式标识合同中的正确条款与适用的 DPR 部分有冲突（在这种情况下，以合同条款为准）。
- 如果本文所包含的要求与任何法律或法规要求有冲突，则以此类法律法规要求为准。
- 如果 Microsoft 供应商以控制者身份经营业务，就本 DPR 而言，只有 J 部分（“安全性”）和 A 部分（“管理”）中的要求适用于该供应商的处理活动。
- 如果 Microsoft 供应商不处理 Microsoft 个人数据而只处理 Microsoft 机密数据，就本 DPR 而言，只有 A 部分（“管理”）、E 部分（“保留”）和 J 部分（“安全性”）中的要求适用于该供应商对 Microsoft 机密数据的处理方式。

在全球范围内转移数据

如果不限制供应商的其他义务，供应商不会在全球范围内转移 Microsoft 个人数据（除非 Microsoft 事先提供书面批准），并且在任何情况下，供应商都应遵守任何标准合同条款、有约束力的企业规则或任何数据保护机构、欧洲数据保护委员会或欧盟委员会批准、Microsoft 采用或同意的其他方案的数据保护要求，包括《欧盟-美国隐私盾框架》、《瑞士-美国隐私盾框架》和《欧盟一般数据保护条例》。供应商同意在做出以下决定时通知 Microsoft：供应商无法再履行其义务来提供隐私盾原则所要求的相同级别的保护。供应商还应确保任何和全部子处理商（以欧盟委员会决定 C(2010)593 的附件形式发布的“2010 年标准合同条款”之条款 1(d) 中对此进行了定义）也遵守这些要求。

关键定义

本 DPR 中使用的以下术语的含义如下。“包括”、“例如”、“比如”、“比方说”或本 DPR 中使用的类似术语后面的示例列表是为了阐明“但不限于”或“而不限于”，除非使用“仅”或“仅仅”之类的字词进行限定。

“Microsoft 个人数据”是指由 Microsoft 处理或代表其处理的任何个人数据。

“Microsoft 机密数据”是指机密性或完整性一旦遭到破坏便会使 Microsoft 遭受重大声誉损失或财务损失的任何信息。这包括 Microsoft 硬件和软件产品、内部业务线应用程序、发布前的营销材料、产品许可证密钥和与 Microsoft 产品和服务相关的技术文档。

“处理”是指对 Microsoft 个人数据或机密数据执行的任意操作或一组操作（无论是否通过自动方法），例如收集、记录、整理、调整结构、存储、改写或更改、检索、查阅、使用、通过传输/传播披露，或以其他方式提供、调整、合并、限制、擦除或销毁。“正在处理”和“已处理”具有相应的含义。

“处理者”是指自然人或法人、公共主管当局、代理机构或代表控制者处理个人数据的其他机构。

“法律”是指具有司法权的任何政府机构（联邦、州、本地或国际）的所有适用法律、规则、法规、法令、决策、指令、法规判决、法典、规定、决定和要求。“非法”是指以任何形式违反法律规定。

“个人数据”是指与已确认身份或可确定身份的自然人（“资料当事人”）有关的任何信息；可识别的自然人是指可直接或间接确定身份的个人，特别是通过参考身份标识确定身份，身份标识包括姓名、个人识别号、位置数据、在线身份标识或特定于该自然人的身体、生理、基因、精神、经济、文化或社会身份的一个或多个因素等。

“控制者”是指自然人或法人、公共机构、代理机构或任何其他机构，他们单独或与其他机构联合确定处理个人数据的用途和方式；处理用途和方式由欧盟（“EU”）或成员国法律确定，控制者（或用于指定控制者的条件）可以根据这些法律来指定。

“数据泄露”是指在传输、存储或以其他方式处理个人数据或 Microsoft 机密数据时导致其意外或非法销毁、丢失、更改、未经授权披露或访问的安全违规行为。

“资料当事人权利”是指资料当事人访问、删除、编辑、导出、限制或反对处理该资料当事人的 Microsoft 个人数据（如果法律要求）的权利。

#	Microsoft 供应商数据保护要求	符合性证明	回复
	A 部分：管理		
1	Microsoft 与供应商之间签订的每份适用协议（例如，主协议、工作说明书、购买订单和其他订单）都包含与 Microsoft 机密数据和个人数据有关的隐私和安全数据保护语言（若适用）。 对于作为处理商经营业务的公司，该协议必须包含处理主题和持续时间、处理性质和用途、Microsoft 个人数据的类型和资料当事人的类别，以及 Microsoft 的义务和权利。	供应商必须提供 Microsoft 与供应商签署的适用合同。 对于处理商，处理说明包含在适用的协议（例如工作说明书、采购订单）中。 注意：如果公司的采购订单是在供应中发生的，他们可以在后面的采购流程中添加必要的处理活动说明。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
2	将遵守 DPR 指定为公司内部指派的人员或组应尽的责任和义务。	负责确保遵守 Microsoft 供应商 DPR 的个人或组织的名称。 介绍此人或此组织的授权和职责的文档，其中展示了隐私和/或安全角色。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
3	对可以访问 Microsoft 个人数据或机密数据的员工建立、维护和执行年度隐私培训。 如果贵公司没有准备好的内容，您可以使用本情节提要大纲，并根据贵公司情况进行调整。	提供出席人数的年度记录。 培训内容包括隐私和安全原则。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
4	必须严格按照 Microsoft 的书面说明处理 Microsoft 个人数据，包括有关向第三国家/地区或国际组织转移 Microsoft 个人数据，如有适用法律要求必须这样处理除外；在此类情况下，处理者（供应商）应在处理之前告知控制者 (Microsoft) 这种法律要求，除非该法律以重要的公共利益为由禁止转移此类信息。	合同（例如工作说明书或采购订单）中所述说明的书面证明，或在用于提供服务的电子系统中注明的书面证明。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	B 部分：声明		
5	在代表 Microsoft 收集个人数据时，供应商必须使用 Microsoft 隐私声明。 隐私声明必须以醒目的方式提供给资料当事人，以帮助他们决定是否向供应商提交其个人数据。 注意：如果贵公司是处理活动的控制者，您需要发布自己的隐私声明。 要访问正确的 Microsoft 声明，请发送电子邮件至 SSPAHelp@microsoft.com。	供应商使用 fwdlink 指向当前已发布的 Microsoft 隐私声明。 在将收集用户个人数据的任何环境中发布该隐私声明。 如果适用，系统会在收集数据之前提供离线版本。 使用的任何离线隐私声明都是已发布的最新版本，并且添加了正确的日期。 对于 Microsoft 员工服务，使用 Microsoft 数据保护声明。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
6	通过实时语音通话或录音收集 Microsoft 个人数据时，供应商必须准备好与资料当事人讨论适用的数据收集、处理、使用和保留做法。	录音脚本中包含 Microsoft 个人数据的处理方式，其中包括 ▪ 收集、 ▪ 使用、 ▪ 保留。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	C 部分：选择和同意		
7	如果供应商将同意书作为处理数据的法律依据，则必须在收集该资料当事人的个人数据之前获得并记录该资料当事人对其所有处理活动的同意书（包括所有新的处理活动和已更新的处理活动）。	供应商可以展示资料当事人如何提供对处理活动的同意书，并且同意书的范围涵盖供应商与资料当事人的个人数据有关的所有处理活动。 供应商可以展示资料当事人如何撤消对处理活动的同意书。 供应商可以展示如何在启动新的处理活动之前检查偏好设置。 供应商会监控偏好设置管理的效果，以确保接受偏好设置更改的时间范围遵循当地限制性最强的法律要求。 注意：可将用户互动屏幕截图作为证明；试用服务或查看技术文档的机会。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
8	Cookie 是网站和/或应用程序存储在设备上的小文本文件，其中包含用于识别资料当事人或设备的信息。 创建和管理 Microsoft 网站和/或应用程序的供应商必须开诚布公地向资料当事人提供有关 Cookie 用途的声明和选择。 创建和管理 Microsoft 网站和/或应用程序的供应商必须确保 Cookie 使用与 Microsoft 隐私声明和当地法律要求（例如欧盟制定的规则）中的承诺一致。	每个 Cookie 的用途必须做出书面记录，并且必须通报所实施 Cookie 的类型。 ▪ 出现会话 Cookie 时不得使用永久性 Cookie。 ▪ 使用永久性 Cookie 时，它们的到期日期不得超过 2 年（自用户访问相应网站后）。对于欧盟用户，永久性 Cookie 的到期日期不得超过 13 个月。 验证是否符合适用的欧盟法律，例如 ▪ 在隐私声明中使用标签规则“隐私和 Cookie”，并 ▪ 在将 Cookie 用于“非本质”用途（例如广告）之前获得用户的明确同意。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	D 部分：收集		
9	供应商必须监控 Microsoft 个人数据和/或机密数据的收集，以确保仅收集执行相关服务所需的数据。	供应商可以提供文档来证明执行相关服务需要收集 Microsoft 个人数据和/或机密数据。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
10	如果供应商代表 Microsoft 从第三方收集个人数据，则供应商必须验证第三方数据保护政策和惯例是否符合供应商与 Microsoft 签署的合同和 DPR 要求。	关于第三方的数据保护政策和惯例，供应商可以提供执行的审慎调查文档。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
11	通过在资料当事人的设备上安装或利用可执行软件收集 Microsoft 个人数据之前，收集该信息的必要性必须在供应商和 Microsoft 实行的合同中做出书面记录。	Microsoft 同意在资料当事人的设备上使用可执行软件在已执行合同中有所说明。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
12	在收集敏感的 Microsoft 个人数据（揭露民族或种族、政见、宗教或哲学信仰或工会会员身份的数据，基因数据，生物识别数据，与健康有关的数据或与自然人的性生活或性取向有关的数据）之前，收集该数据的必要性必须在供应商和 Microsoft 实行的合同中做出书面记录。	需要收集敏感的 Microsoft 个人数据在与 Microsoft 签署的已执行合同中有所说明。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	E 部分：保留		
13	确保 Microsoft 个人数据和机密数据的保留时间不超过执行相关服务所需的时间，法律要求继续保留 Microsoft 个人数据和/或机密数据的情况除外。	供应商应遵守 Microsoft 在合同（工作说明书或采购订单）中指定的书面保留政策或保留要求。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
14	确保 Microsoft 自行决定 Microsoft 个人数据或机密数据在供应商的处理或控制下归还给 Microsoft，或应 Microsoft 的请求在服务执行后进行销毁。 必须在应用程序内制定相关流程以确保从应用程序中安全删除数据（无论是由用户明确删除，还是根据数据期限之类的其他诱因删除）。 如果需要销毁 Microsoft 个人数据或机密数据，供应商必须烧毁、粉碎或撕毁包含 Microsoft 个人数据和/或机密数据的实物资产，以便无法读取或重建相关信息。	维护一份 Microsoft 个人数据或机密数据处置记录（这可以包括返回给 Microsoft 以供销毁）。 如果 Microsoft 要求或请求销毁，请提供一个由供应商官员签名的销毁证书。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	F 部分：资料当事人		
	资料当事人有权访问、删除、编辑、导出、限制和反对处理其个人数据（“资料当事人权利”）。当资料当事人希望根据适用的法律对其 Microsoft 个人数据行使他们的权利时，供应商必须：		
15	通过适当的技术和组织措施尽可能协助 Microsoft 履行其义务，以便对资料当事人希望行使其权利的请求做出回应。	制定相应的流程和程序来支持资料当事人行使权利。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
16	对资料当事人的所有权利请求做出回复，不得无故延迟。	供应商执行定期测试以确保他们可以支持资料当事人的权利。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
17	除非 Microsoft 另外指示，否则供应商会让联系供应商的所有资料当事人直接咨询 Microsoft 以行使他们的资料当事人权利。 供应商会向资料当事人传达个人必须采取哪些步骤才能获得 Microsoft 个人数据访问权限，或以其他方式对其 Microsoft 个人数据行使他们的权利。 如需此要求方面的帮助，请发送电子邮件至 SSPAHelp@microsoft.com。	供应商应说明访问个人数据要采取的步骤，以及可用于更新数据的方法。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
18	对资料当事人做出直接回复时，验证提出请求的资料当事人的身份。	供应商应记录用于识别 Microsoft 资料当事人的方法。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	F 部分：资料当事人（续）		
	资料当事人身份经过验证后，供应商必须：		
19	确定是否持有或控制有关该资料当事人的 Microsoft 个人数据。	供应商应采用各种程序来确定是否持有个人数据。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
20	做出合理的努力，找到请求的 Microsoft 个人数据，并保留足够的记录，证明进行的搜索是合理的。	供应商应维护一份记录，其中展示了满足资料当事人权利请求需采取的步骤。 该文档包含 ▪ 请求日期和时间、 ▪ 回应该请求应采取的措施，以及 ▪ Microsoft 接到通知的时间记录。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
21	记录资料当事人权利请求的日期和时间以及供应商响应此类请求采取的措施。 根据要求向 Microsoft 提供资料当事人请求记录。	供应商应维护访问请求的记录，并对个人数据更改做出书面记录。	
	在资料当事人经过身份验证并且供应商确认他们拥有请求的 Microsoft 个人数据时，供应商必须：		
22	如果请求获取个人数据副本，请以适当的印刷、电子或口头形式向资料当事人提供 Microsoft 个人数据。	供应商应以可理解的格式并且便于资料当事人和供应商使用的形式向资料当事人提供个人数据。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
23	如果其请求遭拒，请根据 Microsoft 之前提供的任何相关说明向资料当事人做出书面解释。 如需此要求方面的帮助，请发送电子邮件至 SSPAHelp@microsoft.com。	记录请求遭拒的情况，并保留 Microsoft 审批证据。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	F 部分：资料当事人（续）		
24	供应商必须采取合理的预防措施，确保发布给资料当事人的 Microsoft 个人数据无法用于标识其他人。	供应商必须证明已经采取了合理的预防措施，从而使之无法通过发布的信息标识其他人（例如，当所请求的某资料当事人的个人数据仅显示在一行中时，则无法影印整页数据）。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
25	如果资料当事人和供应商在 Microsoft 个人数据是否完整且准确方面持有不同的意见，供应商必须将问题呈报给 Microsoft，并在必要时与 Microsoft 合力解决该问题。 如需此要求方面的帮助，请发送电子邮件至 SSPAHelp@microsoft.com。	供应商应对分歧的情况做出书面记录，并将问题呈报给 Microsoft。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	G 部分：披露给第三方		
	如果供应商打算求助转包商来处理 Microsoft 个人数据或机密数据，供应商必须：		
26	在转包服务或对添加或更换的转包商进行任何更改之前，获得 Microsoft 明示书面许可。 如需此要求相关帮助，请发送电子邮件至 SSPAHelp@microsoft.com。	验证 Microsoft 个人数据是否仅由 Microsoft 已知的公司根据适用合同（例如，工作说明书、备忘录、采购订单） 中的要求进行处理，或者是否在 SSPA 数据库中注明。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
27	对由转包商进行中间处理的 Microsoft 个人数据和机密数据的性质和范围做出书面记录，以确保收集执行相关服务所需的信息。	供应商应维护已披露或已转让给转包商的 Microsoft 个人数据和机密数据的相关文档。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
28	确保转包商根据资料当事人的注明联系首选项使用 Microsoft 个人数据。	展示转包商如何利用 Microsoft 资料当事人首选项。 提供支持文档，其中包含转包商接受首选项更改的时间范围。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
29	限制转包商将处理 Microsoft 个人数据用于履行供应商与 Microsoft 签署的合同中规定的用途。	供应商可以提供文档来证明执行相关服务需要向转包商提供 Microsoft 个人数据。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
30	审核对任何未经授权或非法处理 Microsoft 个人数据的迹象的投诉。	供应商可以证明采用各种系统和流程，以解决有关转包商未经授权即使用或披露 Microsoft 个人数据的投诉。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
31	在得知转包商已处理完 Microsoft 个人数据或机密数据用于绩效相关用途之外的其他用途时，立即通知 Microsoft。	供应商已提供相关说明和让转包商报告误用 Microsoft 数据的方式。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
32	如果转包商因未经授权或非法处理 Microsoft 个人数据和机密数据而造成任何实际或潜在的损害，要立即采取措施降低损害。	供应商可以证明他们采用相关计划和程序，以供在转包商误用个人数据和机密数据时使用。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	H 部分：质量		
33	供应商必须保证所有 Microsoft 个人数据的完整性，并确保其准确、完整且与阐明的处理用途相关。	供应商可以证明采用相关程序，以在收集、创建和更新 Microsoft 个人数据时对其进行验证。 供应商可以证明采用监控和抽样程序来持续验证准确性，并在需要时进行更正。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
	I 部分：监控和实施		
34	供应商应制定事件响应计划，该计划要求供应商在意识到与其处理 Microsoft 个人数据或机密数据相关的数据泄露或安全漏洞时立即通知 Microsoft，不得无故延迟。 要举报事件，请发送电子邮件至 SSPAHelp@microsoft.com。	供应商应制定事件响应计划，其中包含一个通知客户 (Microsoft) 的步骤（如本节中所述）。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
35	未经 Microsoft 批准，不得发布与涉及 Microsoft 个人数据或机密数据的数据泄露相关的任何新闻稿或公共通知，除非法律有明确规定。	供应商同意在发生相应事件时履行此要求。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
36	实施补救计划并监控与 Microsoft 个人数据或机密数据相关的数据泄露和漏洞的解决，以确保及时采取纠正措施。	供应商应记录为响应数据泄露以将其关闭而采取的程序。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
37	建立与涉及 Microsoft 个人数据的所有数据保护投诉相对应的正式投诉流程。	供应商通过各种方式接收涉及 Microsoft 个人数据的投诉，并通过记录的投诉程序解决投诉。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	J 部分：安全		
	供应商必须建立、实施和维护包括政策和程序在内的信息安全计划，以根据良好行业惯例和适用法律的要求保护 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面所述的标准及第 38-56 项要求。	可以根据需要，采取所列方法以外的保护措施，以符合监管方案（例如 HIPPA、GLBA）或合同要求。 可以用与安全性有关的有效 ISO 27001 或 SOC 2 报告来替代 J 部分。要申请此替换，请发送电子邮件至 SSPAHelp@microsoft.com。 注意：您需要提供描述这些认证/报告的范围的文档。	
38	执行年度网络安全评估，其中包括： ▪ 审核环境出现的重大变化，例如新的系统组件、网络拓扑、防火墙规则； ▪ 执行漏洞扫描； ▪ 维护更改日志。	供应商应记录网络评估、更改日志和扫描结果。 所需的更改日志必须跟踪更改，提供与更改理由相关的信息，并包含指定审批者的姓名和职称。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
39	供应商负责定义、传达和实施移动设备策略，以保护和限制使用在移动设备上访问和使用的 Microsoft 个人数据或机密数据。	供应商应展示合规移动设备政策的使用（在此使用场景中，Microsoft 个人数据或机密数据处理需要使用移动设备）。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
40	用于支持绩效的所有资产都必须予以考虑并具有身份已确认的所有者。供应商负责维护这些信息资产的清单；确定资产的可接受且经授权的使用；并在整个生命周期内为资产提供保护。	用于支持绩效的设备资产清单。这些资产的清单包括 ▪ 设备位置； ▪ 资产数据的数据分类； ▪ 终止雇佣或商业协议时的资产恢复记录； ▪ 不再需要数据存储介质时的数据存储介质处置记录。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	J 部分：安全（续）		
41	制定和维护访问权限管理程序，以防在供应商控制下对 Microsoft 个人数据或机密数据进行未经授权的访问。	供应商应展示它已实施访问权利管理计划，其中包括 ▪ 访问控制程序； ▪ 识别程序； ▪ 尝试不成功后的锁定程序； ▪ 视需要经常重置密码（至少每 90 天重置一次）； ▪ 用于选择身份验证凭据的可靠参数； ▪ 在终止雇佣关系后的 48 小时内停用用户帐户。 供应商应展示其已制定相应流程来审核用户对 Microsoft 个人数据和机密数据的访问权限，并强制实施最小特权原则。此流程包括 ▪ 明确定义的用户角色； ▪ 审查角色访问权限并证明其批准合理的程序； ▪ 测试角色中有权访问 Microsoft 数据的用户是否具有加入相应组/角色的书面记录证据。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	J 部分：安全（续）		
42	定义和实施补丁管理过程，对用于处理 Microsoft 个人数据和机密数据的系统的安全补丁进行优先排序。这些程序包括： ▪ 定义用于对安全补丁进行优先排序的风险方法； ▪ 能够处理和实施应急修补程序； ▪ 适用于操作系统和服务器软件，例如应用程序服务器和数据库软件； ▪ 书面记录修补程序减轻的风险并跟踪任何例外情况； ▪ 要求停用授权公司不再支持的软件。	供应商可以展示已实施的补丁管理程序满足此项要求并至少涵盖以下内容。 ▪ 指定严重程度以通知优先顺序（严重程度定义已予以记录）。 ▪ 实施应急修补程序的书面程序。 ▪ 验证是否未使用授权公司不再支持的操作系统。 ▪ 补丁管理会记录哪个跟踪批准和例外情况。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
43	在连接到网络的所有设备（用于处理 Microsoft 个人数据和机密数据，包括但不限于服务器、生产和培训台式机）上安装防病毒和防恶意软件软件，以防范可能有害的病毒和恶意软件应用程序。 每日更新一次反恶意软件定义，或按照防病毒/反恶意软件供应商的指示来更新。 注意：这适用于所有操作系统（包括 Linux）。	存在相关记录来展示主动使用防病毒和反恶意软件。 注意：此项要求适用于所有操作系统。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
44	供应商为 Microsoft 开发的软件必须在编译流程中纳入安全设计原则。	供应商技术规范文档包含在其开发周期中进行安全验证的检查点。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	J 部分：安全（续）		
45	采用数据丢失防护（“DLP”）计划。数据必须进行正确归类、添加标签并受到保护，并且供应商必须监控信息系统的使用（在使用过程中，系统会处理 Microsoft 个人数据或机密数据以发现入侵、丢失和其他未经授权的活动）。DLP 计划至少要满足以下条件： ▪ 如果您保留 Microsoft 个人数据或机密数据的话，则需要使用行业标准主机、网络和基于云的入侵检测系统（“IDS”）； ▪ 要求实施高级入侵防护系统 (“IPS”)，将其配置为监控并主动遏制数据丢失； ▪ 如果系统遭到入侵，请分析系统以确保所有残余漏洞也会得到解决； ▪ 描述用于监控系统威胁检测工具的必需过程； ▪ 制定在检测到数据泄露事件时必须执行的事件响应和管理流程。	已部署的书面 IDS/IPS 采用相关程序在检测到漏洞或数据泄露时提交响应。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
46	立即将事件响应的调查结果告知高级管理人员和 Microsoft。 要通知 Microsoft，请发送电子邮件至 SSPAHelp@microsoft.com。	必须采用各种系统和流程，以向 Microsoft 传达事件响应调查结果。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
47	系统管理员、运营人员、管理人员和第三方必须接受年度安全培训。	建立安全培训计划，其中包括： ▪ 有关事件响应的年度培训和 ▪ 便于对紧急情况作出有效响应的模拟事件和自动化机制。 事件预防意识，例如与下载恶意软件相关联的风险。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	J 部分：安全（续）		
48	供应商必须确保备份计划流程能保护 Microsoft 个人数据和机密数据免遭未经授权使用、访问、泄露、更改和销毁。	供应商可以展示书面记录响应和恢复过程，其中详述了组织将如何根据管理层批准的信息安全持续性目标应对破坏性事件并将其信息安全性保持在预定水平。 供应商可以展示其已定义和实施相关过程以定期备份、安全存储和有效恢复关键数据。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
49	制定和测试业务连续性和灾难恢复计划。	灾难恢复计划必须包括以下各项。 ▪ 定义的条件，用于确定系统对供应商业务的运营是否起到关键作用。 ▪ 根据定义的条件列出在发生灾难时必须恢复的目标关键系统。 ▪ 为每个关键系统定义灾难恢复过程，以确保不了解系统的工程师可在 72 小时内恢复应用程序。 ▪ 对灾难恢复计划进行年度（或更频繁）测试和审核以确保可以实现恢复目标。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	J 部分：安全（续）		
50	先验证个人的身份，然后才能授予该个人访问 Microsoft 个人数据或机密数据的权限。	确保所有用户 ID 都是唯一的，且每个 ID 都有行业标准身份验证方法（例如 Azure Active Directory）。 提升访问权限（管理特权或其他类型的增强型特权）必须要求使用第二因素（例如智能卡或基于电话的验证器）。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
51	供应商必须通过采用传输层安全性 (“TLS”) 或 Internet 协议安全性 (“IPsec”) 的加密方法保护在网络中传输的 Microsoft 个人数据和机密数据。 这些方法在 NIST 800-52 和 NIST 800-57 中有所介绍；也可以使用同等的行业标准。 供应商必须拒绝发送以未加密方式传输的任何 Microsoft 个人数据或机密数据。	必须定义并强制实施创建、部署和替换 TLS 或其他证书的过程。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
52	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）都必须采用基于磁盘的加密。	对所有设备加密，以使用于处理 Microsoft 个人数据或机密数据的所有客户端设备都满足 Bitlocker 或其他行业同等磁盘加密解决方案的要求。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	J 部分：安全（续）		
53	必须采用系统和过程（使用当前行业标准，例如 NIST 800-111 标准中所述）对（已存储的）任何静态及所有 Microsoft 个人数据和/或机密数据进行加密，包括以下任何及所有数据： ▪ 凭据数据（例如用户名/密码） ▪ 付款方式数据（例如信用卡和银行帐号） ▪ 移民相关的个人数据 ▪ 医疗个人资料数据（例如病历号、生物识别标记或用于身份验证用途的 DNA、指纹、眼视网膜和虹膜、语音模式、面部特征和手掌宽度等标识符） ▪ 政府颁发的身份标识数据（如社会保险号或驾照号） ▪ 属于 Microsoft 客户的数据（例如SharePoint、O365 文档、One Drive 客户） ▪ 与未发布的 Microsoft 产品相关的资料 ▪ 出生日期 ▪ 孩子的个人资料信息 ▪ 实时地理位置数据 ▪ 个人物理（非商家）地址 ▪ 个人（非商家）电话号码 ▪ 宗教 ▪ 政治见解 ▪ 性取向/偏好 ▪ 安全问题答案（例如2fa、密码重置） ○ 母亲的娘家姓	检查此行中列出的 Microsoft 个人数据和机密数据在处于静态时是否已进行加密。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
54	代表 Microsoft 处理信用卡时，遵守适用的信用卡处理标准（由发卡单位提供）。	通过每年提供一次支付卡行业数据服务标准（“PCI-DSS”）证书来证明遵守相关要求。 将 PCI DSS 证书提交给 SSPA。如有任何疑问，请发送电子邮件至 SSPAHelp@microsoft.com。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>

#	Microsoft 供应商数据保护要求	符合性证明	回复
	J 部分：安全（续）		
55	供应商必须将 Microsoft 实物资产存储在控制访问的环境中。	必须采用各种系统和流程，以管理对 Microsoft 数据的数字副本、打印件、存档以及备份副本的物理访问。 必须在监管链中跟踪包含 Microsoft 数据的实物介质的移动和销毁。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>
56	匿名处理开发或测试环境中使用的所有 Microsoft 个人数据。	Microsoft 个人数据不得用在开发或测试环境中；如果没有任何备选方案，则必须对其进行匿名化处理以防识别资料当事人或误用个人数据。 注意：匿名化数据不同于假名数据。匿名化数据与已确定身份或可确定身份的自然人不相关，在其中无法识别或不再可识别个人数据的资料当事人。	<合规> <不合规> <不适用> <法律冲突> <合同冲突>