Microsoft 采购

供应商安全和隐私保障（SSPA）计划指南

第 8 版

2022 年 6 月

简介

Microsoft 认为隐私权是一项基本权力。Microsoft 的使命是予力全球每一人、每一组织，成就不凡，在实现使命的过程中，我们每天都在努力赢得并维护顾客信任。

强有力的隐私和安全实践不仅对我们的使命至关重要，是客户信任的基础，更是多个辖区的法律要求。Microsoft 的隐私与安全政策中的各项标准反映了我公司的价值观，代表我们处理 Microsoft 数据的供应商（如贵公司）也要遵循这些标准。

供应商安全和隐私保障（“**SSPA**”）计划是 Microsoft 推出的公司计划，旨在通过《Microsoft 供应商数据保护要求》（“**DPR**”）向供应商传达 Microsoft 的基准数据处理指南，访问 SSPA on Microsoft.com/Procurement 查看 DPR。请注意，除 SSPA 外，供应商可能还要满足其他组织层面的要求，这些要求由负责聘用供应商的 Microsoft 团队决定并传达。

SSPA 的关键术语在 DPR 中进行了定义。想要更多了解该计划，请查看常见问题(FAQs)并发邮件至 SSPAHelp@microsoft.com 与我们的全球团队交流。

SSPA 计划概述

SSPA 是一个由 Microsoft 采购部、公共及法律事务部以及企业安全部合作开展的项目，旨在确保供应商遵守隐私与安全准则。

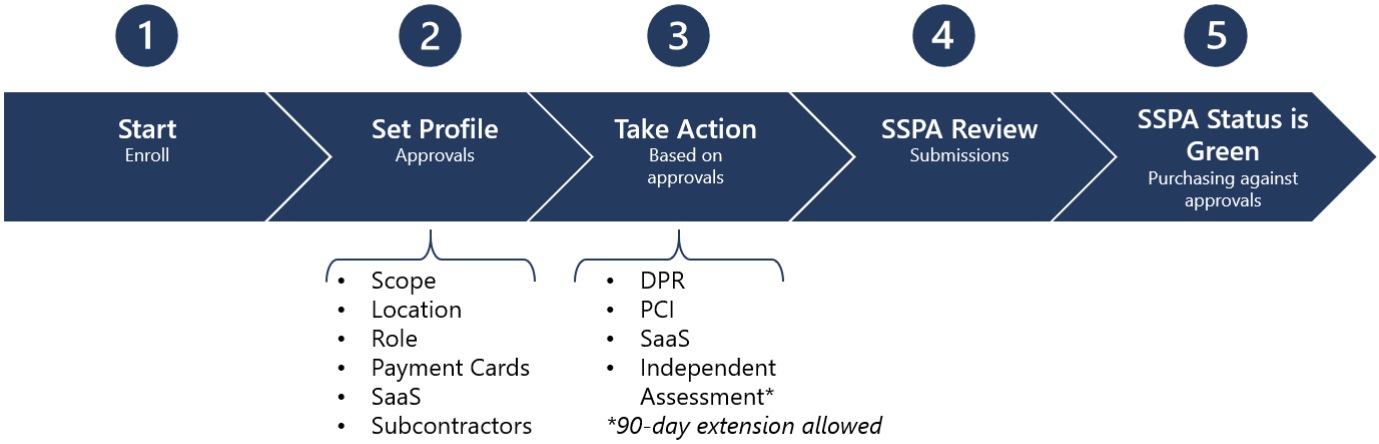
SSPA 的范围包括在履行（如提供服务、软件许可证、云服务）与 Microsoft 的合同条款（如订单条款、主协议）有关的情况下，处理个人数据和/或 Microsoft 机密数据的全球所有供应商。

SSPA 使供应商能够根据自己履约的商品和/或服务在“数据处理配置文件”中进行选择。这些选择将触发相应的向 Microsoft 提供合规保证的要求。

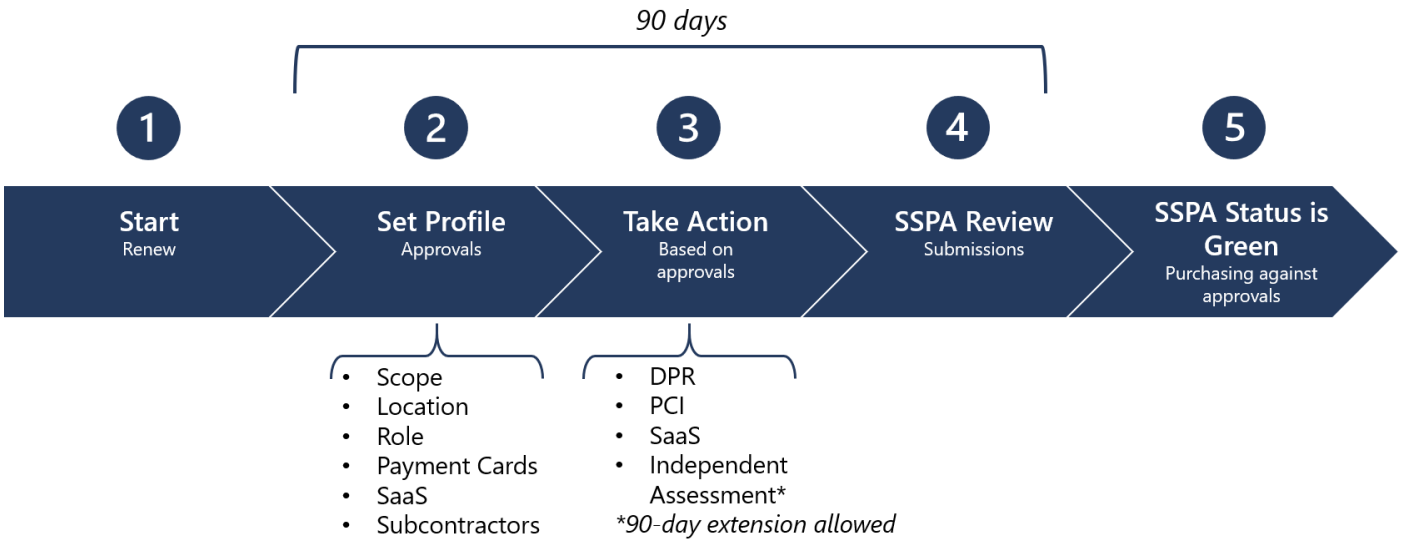
所有注册的供应商每年将完成一次 DPR 合规性自我鉴证。您的“数据处理配置文件”将决定是否向您发布整个 DPR，或者其中部分要求适用。处理 Microsoft 视为较高风险的数据的供应商可能还需满足其他要求，如提供独立的合规验证。名列已公布的 Microsoft 子处理者名单的供应商也要提供独立的合规验证。

重要提示：合规活动将决定 SSPA 的状态是“Green”（合规），还是“Red”（不合规）。Microsoft 的采购工具在确认 SSPA 的状态为“Green”（对象为 SSPA 范围内的每个供应商）后，才会为继续互动放行。

SSPA 流程示意图——新供应商注册



SSPA 流程示意图——供应商年审



SSPA 范围

为便于确定您（供应商）的工作是否涉及处理个人数据和/或 Microsoft 机密数据，请参阅以下表格中的示例。请注意，以下只是示例，并非详尽列举。

请注意：考虑到所处理数据的机密性，Microsoft 的业务负责人可能会就该列表以外的数据要求供应商注册。

个人数据（按数据类型列出）

示例包括但不限于：

敏感数据
与儿童相关的数据
遗传数据、生物特征数据或健康数据
种族或种族或民族
政治、宗教或哲学信仰、见解和立场
工会会员身份
自然人的性生活或性取向
移民身份（签证、工作许可等）
政府签发的身份标识（护照、驾照、签证、社会保障号、身份证号码）
精确的用户位置数据（300 米内)
个人银行账户号
信用卡号及到期日
客户内容数据
文件、照片、视频、音乐等
输入产品或服务的评价和/或评分
调查反馈
浏览历史、兴趣及收藏
墨迹书写、打字和语音表达（语音/音频和/或聊天/机器人）
凭证数据（密码、密码提示、用户名、用于识别的生物特征数据）
与客服个案有关的客户数据

采集与生成的数据
不精确的位置数据
IP 地址
设备首选项与个性化信息
网站的服务使用、网页点击追踪
社交媒体数据、社交图谱关系
来自连接的设备（如健身监测仪）的活动数据
联系方式数据，如姓名、地址、电话、电子邮箱地址、出生日期、依靠和紧急联络人
欺诈与风险评估、背景调查
保险、养老金、福利详情
求职者简历、面试记录/反馈
Metadata and telemetry
账户数据
支付工具数据
信用卡号及到期日
银行代号信息
银行账户号
信用请求或信用额度
税务文件及识别信息
投资或开支数据
公司卡
最终用户假名化信息（EUPI） （Microsoft 创建的用来识别 Microsoft 产品及服务用户的标识符）
全局唯一标识符（GUID）
护照用户名或唯一标识符（PUID）
散列最终用户识别信息 (EUII)
会话标识符（ID）
设备标识符（ID）
诊断数据
日志数据

Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

Microsoft 机密数据（按数据类别列出）

示例包括但不限于：

高度机密
涉及或有关开发、测试或生产 Microsoft 产品或 Microsoft 产品组件的信息 *通过任何渠道商业销售的 Microsoft 软件、在线服务或硬件均被视为“**Microsoft 产品**”。*
Microsoft 设备预发布市场营销信息
受美国证券交易委员会（SEC）管辖的尚未公布的 Microsoft 公司财务数据
机密
通过任何方式代表 Microsoft 分销的 Microsoft 产品许可证密钥
涉及或有关 Microsoft 内部业务线（LOB）应用软件开发或测试的信息
Microsoft 软件和服务（如 Office、SQL、Azure 等）的 Microsoft 预发布市场营销材料
任何 Microsoft 服务或产品（如设备，包括流程或程序指南、配置数据等）的书面、设计、电子或打印文档。

重要提示：Microsoft 的业务负责人可能就上表未曾列出的数据要求供应商加入计划。

数据处理配置文件

Microsoft 的供应商可以管理自己的 SSPA 数据处理配置文件。

这使供应商能够决定想要有资格履行哪些工作。请认真斟酌选项，并仔细考虑获得批准前所必须完成的合规活动。**参见下文“保证要求”部分和附录 A。**

Microsoft 的业务团队将只能聘用在相应的数据处理活动方面获得批准的供应商。

无待办任务时，供应商将可以随时更新自己的数据处理配置文件。修改配置文件时，相应活动将发布，获得批准前必须完成这些活动。在新发布的要求完成前，现存的已获得的批准将持续有效。

如果在允许的 90 天时限内未完成新执行的任务，SSPA 状态将变为“Red”（不合规），而且该账户将可能在 Microsoft Accounts Payable 系统中被停用。

数据处理批准	
1	数据处理范围 ▪ 机密 ▪ 个人、机密
2	数据处理位置 ▪ 在 Microsoft 或客户处 ▪ 在供应商处
3	数据处理角色 ▪ 控制者（独立或联合控制者） ▪ 处理者 ▪ 子处理者（由 Microsoft 指定）
4	支付卡处理 ▪ 是 ▪ 不适用
5	软件即服务 ▪ 是 ▪ 不适用
6	使用分包商 ▪ 是 ▪ 不适用

批准注意事项

数据处理范围

机密

如供应商履约将只涉及处理 Microsoft 机密数据，请选择此批准。

如选择此批准，您将无资格进行个人数据处理工作。

个人、机密

如供应商履约将涉及处理个人数据和 Microsoft 机密数据，请选择此批准。

处理位置

在 Microsoft 或客户处

如供应商履约涉及供应商在 Microsoft 网络环境内，其工作人员使用 *@microsoft.com* 访问凭证处理数据，或者涉及供应商在 Microsoft 客户的环境内处理数据，请选择此批准。

在以下情况下，请勿选择此选项：

- 供应商管理 Microsoft 指定的离岸设施（OF）
- 供应商为 Microsoft 提供资源，且有时断断续续地在 Microsoft 网络上工作，不在该网络上工作时的处理位置被视为“在供应商处”。

在供应商处

如“在 Microsoft 或客户处”（如上所述）的条件不适用，则选择这一选项。

数据处理角色

控制者（包括独立和联合控制者）

如供应商履约的**所有**方面都符合数据处理角色中的控制者的定义（见 DPR），请选择此批准。

如您选择此批准，您将没有资格使用“处理者”角色处理个人数据。如供应商对 Microsoft 来说既是处理者，也是控制者，则勿选择“控制者”，而要选择处理者。

处理者

这是供应商代表 Microsoft 处理数据时最常见的处理角色。请查看 DPR 中的处理者定义。

子处理者

子处理者是 Microsoft 聘请履约的第三方，其履约工作包括为 Microsoft（处理者）处理 Microsoft 个人数据。供应商不能自定为 Microsoft 的子处理者，因为该角色需要微软内部隐私团队的预先批准。只有在 Microsoft 是数据处理者并且供应商处理的是符合要求的企业个人数据类型时，供应商才能成为子处理者。子处理者将有额外的合同与合规要求，包括《数据保护附录》以及独立评估（见下文）。

支付卡处理

如果供应商所处理数据的任何部分包括代表 Microsoft 进行信用卡或其他支付卡处理的支持数据，请选择此批准。

此批准允许供应商参与支付卡处理工作。

软件

在所有软件的购买过程中，Microsoft 采购部会指导买方完成软件采购流程，这一流程包括 SSPA 鉴别分类等不同核查，以确定提供软件的供应商是否在 SSPA 的管理范围内。(Microsoft 买方可以参见内部采购网 软件与云服务网页所述步骤查看详情。)如有 SSPA 要求，供应商还需确认“软件即服务”（SaaS）配置文件选项适用。已注册 SSPA 的供应商可以在 Microsoft Supplier Compliance Portal 中填写数据处理配置文件时完成这一步骤。

为 SSPA 合规目的，请广义定义 SaaS，即它也包括平台即服务（PaaS）和基础设施即服务（IaaS）。（想要了解更多有关 SaaS 的信息，请查看此阐述。）

软件即服务(SaaS)

软件即服务（SaaS）使用户可以通过互联网连接并使用基于云的应用程序。

Microsoft 将**软件即服务（SaaS）**定义为基于通用代码、采用一对多模式、按使用付费或基于使用指标订阅的软件。云服务提供商开发并维护基于云的软件，提供自动软件更新，并在一对多、即用即付的基础上通过互联网向用户提供软件。这种软件交付和许可方式允许用户通过订阅在线上使用软件，而不是在购买软件后安装于每台计算机上。

请注意：如果个人数据或 Microsoft 机密数据托管于第三方平台上，大多数 SaaS 供应商将需要在 Microsoft Supplier Compliance Portal 中添加分包商批准。

使用分包商

如供应商使用分包商来履约（定义见 DPR），请选择此批准。

这也包括自由职业者（见 DPR）。

保证要求

基于配置文件批准的要求

您在数据处理配置文件中选择的批准有助于 SSPA 评估您在各项 Microsoft 工作中的风险水平。SSPA 的合规要求根据数据处理配置文件和相关批准的不同而异。本部分将对不同的 SSPA 要求进行阐释。

一些组合可能会提升或降低合规要求。附录 A 对这些组合进行了描述，在您完成配置文件后，可从 Microsoft Supplier Compliance Portal 执行这些组合。您随时可通过申请 SSPA 团队审查来验证您的方案与此框架的适合程度。

操作：在附录 A 中查找您的批准配置文件，并查看相应的保证要求和独立保证选项（如适用）。

重要提示：如果您的配置文件包含软件即服务（SaaS）、分包商、网站托管或支付卡，则有额外的保证要求。

DPR 合规性自我鉴证

在 SSPA 注册的所有供应商都必须在接到请求后的 90 天内完成 DPR 合规性自我鉴证。该请求每年一次，但如果在年中更新过数据处理配置文件，则请求频率可能会增加。如超过 90 天期限，供应商账户的 SSPA 状态将变为“Red”（不合规）。在 SSPA 状态变为“Green”（合规）前，将不能处理范围内的新采购订单。

新注册的供应商必须完成发布的要求，获得 SSPA“Green”状态（合规）后，才能开始履行工作。

重要提示：SSPA 团队无权延长此任务的期限。

完成自我鉴证的授权代表应确保从行业专家处获得足够的信息，以便自信地回复每一项要求。此外，向 SSPA 表单添加姓名即证明他们已阅读并理解 DPR。供应商可以向在线工具添加其他联系人，以帮助完成要求。

授权代表（定义见 DPR）的职责是：

1. 确定适用的要求
2. 对每项适用的要求发布回应
3. 在 Microsoft Supplier Compliance Portal 中签署并提交自我鉴证

适用性

供应商应响应根据数据处理配置文件发布的所有适用的 DPR 要求。预计在发布的要求中，有些可能不适用于供应商为 Microsoft 所提供的产品或服务。可以把这些要求标记为“不适用”并添加详细注释，以便 SSPA 审阅者进行确认。

在 DPR 提交中，对所发布的要求表示“不适用”、“当地法律冲突”或“合同冲突”的所有选择都将由 SSPA 团队审核。该团队可能会要求对一项或多项选择进行阐释。只有在提供证明材料并且明确存在冲突的情况下时，当地法律冲突和合同冲突的选择才会被接受。

独立评估要求

请参见附录 A 中的“基于配置文件批准的要求”，以查看触发独立评估要求的数据处理批准。

供应商可以通过更新数据处理配置文件来更改批准。但是，如供应商拥有“子处理者”的数据处理角色，则不能改变此批准，而且必须进行年度独立评估。

为获得需要独立合规验证的批准，供应商需选择一个独立评估机构，以根据 DPR 验证合规性。该评估机构需出具咨询函，向 Microsoft 提供合规保证。该函必须是无保留意见的，并且在确认函提交至 Microsoft 供应商合规门户接受 SSPA 团队审查前，所有的不合规问题都必须得到解决并纠正。评估机构可以下载经批准的咨询函模板，该模板在“首选评估机构”PDF 中随附，详情见此。

如您选择不使用独立评估机构来核实 DPR 合规情况（适用时，如 SaaS 供应商、网站托管供应商或使用分包商的供应商），**附录 A** 中列出了可接受的替代认证方式。ISO 27701（隐私）和 ISO 27001（安全）因与 DPR 标准相近而予以采用。

供应商是在美国的医疗服务提供者或者盖实体的情况下，我们将接受覆盖隐私与安全的 HITRUST 报告。

如有超出标准触发机制的情况发生，有必要进行额外尽职调查的话，SSPA 可能人工执行独立评估，这些情况包括部门隐私或安全机构提出请求、对数据事件补救的验证或数据主体权力自动执行的要求。

关于如何执行此项要求的指南：

1. 这项工作必须由具备充分技术培训与专业知识的评估机构执行，以妥善评估合规情况。
2. 评估机构必须加入国际会计师联合会（IFAC）或美国注册会计师协会（AICPA），或者必须持有其他相关的隐私与安全组织认证，如国际隐私专业协会（IAPP）或信息系统审计与控制协会（ISACA）。
3. 评估机构必须使用最新的 DPR，DPR 中包含满足每项要求所必须提供的证据。**供应商将需要向评估机构提供其最近获批的 DPR 自我鉴证回复。**
4. 对新注册的供应商，评估机构将测试流程控制的设计。在所有其他情况下，评估机构将测试控制的有效性。
5. 评估工作的范围仅限于与供应商履约有关的个人数据和/或 Microsoft 机密数据。
6. 工作范围仅限于针对收到请求的供应商账号所执行的所有的范围内数据处理活动。如果供应商选择同时拥有多个供应商账户，则**证明信必须包括评估所包含的供应商账户列表以及相关地址**。
7. 提交给 SSPA 的信函中不得包含供应商不符合书面数据保护要求的任何声明。这些问题必须在信函提交前改正。

SSPA 制定了首选评估机构名单，详请见此。这些公司熟悉 SSPA 评估流程。供应商应自行支付该评估，评估费用因数据分析的规模和范围而异。

PCI DSS 认证要求

支付卡行业数据安全标准（PCI DSS）是用于开发稳健的支付卡数据安全的框架，其中包括预防、检测以及对安全事件的适当响应。该框架由 PCI 安全标准委员会（一个自我监管的行业组织）开发。PCI DSS 的各项要求的目的是识别技术与流程的漏洞，避免对所处理的持卡人的数据安全造成风险。

Microsoft 必须遵守这些标准。如供应商代表 Microsoft 处理支付卡信息，则必须提供遵守这些标准的证据。请参见 PCI 安全标准委员会来了解 PCI 组织所制定的各项要求。

根据所处理的交易量，供应商或者必须由合格的安全评估机构认证合规，或者可以填写自我评估问卷表。

评估类型的阈值由支付卡品牌设定，通常：

- 一级：提供第三方评估机构 PCI AOC 认证
- 二或三级：提供由供应商高级管理人员签署的 PCI DSS 自我评估调查问卷（SAQ）

提交适用并满足 PCI 要求的认证。

对 SaaS 的要求

如 Microsoft 云服务协议中有要求，符合数据处理配置文件中 SaaS 定义的供应商可能需要提供有效的 ISO 27001 认证。

SSPA 审核者将确认您提交的认证是否满足合同义务。

请勿提交数据中心认证，提交的 ISO 27001 认证应适用于您与 Microsoft 合同中注明的软件服务。

使用分包商

Microsoft 认为使用分包商是高风险因素。将使用分包商处理个人和/或 Microsoft 机密数据的供应商必须披露这些分包商。此外，供应商也应披露每个分包商将在哪些国家处理这些个人数据。

数据事故

如果供应商获悉发生隐私或安全数据事故，则必须按 DPR 中的详细说明通知 Microsoft。请参见附录 B 中的使用定义。

请使用 SupplierWeb 或者发邮件至 SuppIR@microsoft.com 报告数据事件。

请务必包含以下信息：

- 数据事件日期：
- 供应商名称：
- 供应商编号：
- 已通知的 Microsoft 联系人：
- 关联的采购订单（PO），如适用/可获得：
- 数据事件摘要：

附录 A

基于配置文件批准的要求

#	配置文件	保证要求	独立保证选项
1	**范围:** 个人、机密 **处理位置：在** Microsoft 或客户处 **处理角色：** 处理者或控制者 **数据类：** 机密**或**高度机密 **支付卡：** 不适用 **SaaS:** 不适用 **使用分包商:** 不适用 **网站托管：** 不适用	DPR 合规性自我鉴证	
2	**范围:** 机密 **处理位置：** 在供应商处 **处理角色：** 不适用 **数据类：** 机密 **支付卡：** 不适用 **SaaS:** 不适用 **使用分包商:** 不适用 **网站托管：** 不适用	DPR 合规性自我鉴证	
3	**范围:** 机密 **处理位置：** 在供应商处 **处理角色：** 处理者 **数据类：** 高度机密 **支付卡：** 不适用 **SaaS:** 不适用 **使用分包商:** 不适用 **网站托管：** 不适用	DPR 合规性自我鉴证 **和** 合规性独立保证	独立保证选项: 1. 根据 DPR 完成独立评估 **或** 2. 提交 ISO 27001

#	配置文件	保证要求	独立保证选项
4	**范围:** 个人、机密 **处理位置：** 在供应商处 **处理角色：** 处理者 **数据类：** 高度机密 **支付卡：** 不适用 **SaaS：** 不适用 **使用分包商:** 不适用 **网站托管：** 不适用	DPR 合规性自我鉴证 **和** 合规性独立保证	独立保证选项: 1. 根据 DPR 完成独立评估**或** 2. 根据 DPR 的 A-I 部分完成独立评估和 ISO 27001 **或** 3. 提交 ISO 27701 **和** ISO 27001
5	**范围:** 个人、机密 **处理位置：** 在供应商处 **处理角色：** 处理者 **数据类别：** 机密 **支付卡：** 不适用 **SaaS:** 不适用 **使用分包商:** 不适用 **网站托管：** 不适用	DPR 合规性自我鉴证	
6	**范围:** 个人、机密 **处理位置：** 在供应商处 **处理角色：** 控制者 **数据类别：** 高度机密或机密 **支付卡：** 不适用 **SaaS:** 不适用 **使用分包商:** 不适用 **网站托管：** 不适用	DPR 合规性自我鉴证	

#	配置文件	保证要求	独立保证选项
7	**范围:** 个人、机密 **处理位置：** 任何 **处理角色：** 子处理者（该角色由 Microsoft 决定——配置文件将写明 “子处理者批准：是”） **数据类：** 高度机密或机密 **支付卡：** 不适用 **SaaS:** 不适用 **使用分包商:** 不适用 **网站托管：** 不适用	DPR 合规性自我鉴证 **和** 合规性独立保证	独立保证选项: 1. 根据 DPR 完成独立评估**或** 2. 根据 DPR 的 A-I 部分完成独立评估和 ISO 27001 **或** 3. 提交 ISO 27701 **和** ISO 27001

#	配置文件	保证要求	独立保证选项
添加 SaaS、分包商、网站托管的影响			
8	**范围:** 个人、机密 **处理位置：**在供应商处 **处理角色：**处理者 **数据类：**高度机密或机密 **支付卡：**不适用 **分包商：**是，或者 **SaaS:** 是，或者 **网站托管：**是	DPR 合规性自我鉴证 **和** 合规性独立保证	独立保证选项: 1. 根据 DPR 完成独立评估**或** 2. 根据 DPR 的 A-I 部分完成独立评估和 ISO 27001 **或** 3. 提交 ISO 27701 **和** ISO 27001
9	**范围:** 个人、机密 **处理位置：**在供应商处 **处理角色：**控制者 **数据类：**高度机密或机密 **支付卡：**不适用 **分包商：**是，或者 **SaaS:** 是，或者 **网站托管：**是	DPR 合规性自我鉴证	

#	配置文件	保证要求	独立保证选项
支付卡和 SaaS 的额外保证			
10	上述任何配置文件加**支付卡**	上述适用要求**和**支付卡行业保证	提交 PCI DSS 认证
11	上述任何配置文件加**软件即服务（SaaS）**	上述适用要求**和**提交合同要求的、覆盖功能服务的 ISO 27001 认证	提交 ISO 27001 认证，涵盖所提供服务的功能范围