SOPHOS
Cybersecurity made simple.

注解: 这仅仅是为了方便而提供的由机器生成的翻译。这种由机器生成的翻译与人工翻译的质量不一样，可能存在错误。此翻译按“原样”提供，对翻译的准确性、完整性或可靠性不作任何保证。本文档的英文版本与翻译版本如有不一致之处，以英文版本为准。

数据处理附录

修订日期：2022 年 1 月 20 日

如果 Sophos Limited 之间的协议 (**主要协议**) 中明确引用了本数据处理附录 (**附录**) (一家在英格兰和威尔士注册的公司，编号为 2096520 ，其注册办事处位于 Pentagon, Abingdon Science Park, Abingdon, Oxfordshire OX14 3YP， 英国 (“**供应商**”) 和供应商的客户 (“**客户**”)，本附录构成主协议的一部分，在供应商和客户之间生效。

1. 序言

1.1 双方就供应商向客户提供某些产品和 / 或服务 (统称“**产品**”) 达成了主要协议。

1.2 如果主协议是与位于 https://www.sophos.com/zh-cn/legal/sophos-msp-partner-terms-and-conditions.aspx (以下简称“**MSP 协议**”) 的 MSP 协议类似的 MSP 协议，则客户是托管服务提供商 (以下简称“**MSP**”)。如果主协议是 OEM 协议，根据该协议，客户有权将供应商产品与客户的产品组合作为捆绑单元的一部分 (“**OEM 协议**”) 分发，再授权或向第三方提供，则客户是原始设备制造商 (“**OEM**”)。否则，客户是最终用户 (“**最终用户**”)。

1.3 产品的提供可能包括供应商为客户收集，处理和使用控制器数据。本增编规定了双方在 处理数据方面的义务，并补充了《主要协议》的条款和条件。

1.4 主要协议，本附录以及主要协议和本附录中明确提及的文档应构成双方就供应商代表客户收集，处理和使用的与主要协议相关的个人数据达成的完整协议， 并应取代双方先前就该主题达成的所有协议，安排和谅解。

2. 定义

2.1 在本增编中，以下术语具有以下含义：

“**适用的数据保护法**”是指 (i) 欧洲议会和欧盟理事会关于在处理个人数据方面保护自然人和此类数据自由移动的第 2016/679 号欧盟条例 (一般数据保护条例或“**GDPR**”)； (ii) 电子隐私指令 (欧盟指令 2002/58/EC) ；以及 (iii) 任何和所有适用的国家数据保护立法，包括根据 (i) 或 (ii) 制定或依据 (i) 或 (ii) 制定的立法；在每种情况下，可能会不时修正或取代。

“**受益人**”具有 MSP 协议中赋予的含义。

“**控制器**”表示：(a) 客户 (如果客户是最终用户)； (b) 受益人 (如果客户是 MSP)；或 (c) 最终客户 (如果客户是 OEM)。

“**控制器数据**”是指根据适用的数据保护法，控制器是其控制器的任何和所有个人数据。

“**最终客户**”具有 OEM 协议中赋予的含义。

“**欧洲**” (和“**欧洲**”) 是指 (i) 欧洲经济区 (“**EEA**”) 的成员国，以及 (ii) 自欧盟法律不再适用于英国之日起立即生效。

“欧盟标准合同条款”或“欧盟 SCC ” 是指根据欧盟委员会 2021 年 6 月 4 日执行决定 (欧盟) 2021/914 批准的欧洲议会和欧盟理事会条例 (欧盟) 2016/679 向第三国传输个人数据的标准合同条款；

“欧盟控制者对处理者条款”是指欧盟 SCC 的模块二条款；

“欧盟处理器到处理器条款”是指欧盟 SCC 的模块三条款。

“托管 产品”是 **指附件 3 中列出的产品**。

“个人数据泄露”是指安全漏洞 (客户或其用户造成的安全漏洞除外)，导致意外或非法破坏，丢失，修改，未经授权披露或访问， 供应商根据本附录处理的控制器数据。

“英国附录”是指在适用情况下在附录中列出的欧盟 SCC 附录。

2.2 在本附录中，小写术语**“控制者”**，**“处理者”**，**“数据主体”**，**“个人数据”**和**“处理”** (及其衍生品) 应具有适用的数据保护法中给出的含义。

3. 范围

3.1 供应商处理控制器数据的主题和持续时间 (包括处理的性质和目的，要处理的控制器数据的类型以及数据主体的类别) 应如下所述：(i) 本增编； (ii) 主要协议； (iii) **附件 1 中的任何指示**； 和 (v) 客户根据第 4 条发出的指示。

3.2 客户有责任确保 (i) 主计长有合法依据处理由供应商代表其执行的主计长数据， ㈡主计长已从数据主体获得客户和供应商处理主计长数据所需的所有必要同意 (包括但不限于特殊类别数据)； 以及 (iii) 在其他方面遵守并将确保供应商处理控制器数据的指示在所有方面都符合适用的数据保护法。

3.3 本附录的其余条款描述了双方各自对主计长数据的义务，其中包括：(i) 如果客户是最终用户，则客户是控制者，供应商是处理者；或者 (ii) 如果客户是 MSP 或 OEM，则客户是第三方控制者的处理者，而供应商是子处理者。

4. 客户说明

4.1 供应商应按照客户记录的处理指令处理控制器数据，该指令仅在条款中规定 3.1 ，以下情况除外：

(a) 供应商和客户之间以书面形式另行约定的情况；或

(b) 供应商应遵守的法律要求 (在此情况下，供应商应在处理前将该法律要求告知客户，除非该法律禁止提供此类信息)。

4.2 如果供应商意识到客户的处理指令违反了适用的数据保护法 (而供应商没有义务主动监控客户的合规性)，则供应商将立即通知客户该指令，并暂停对控制器数据的处理。

5. 供应商的职责

5.1 所有处理控制器数据的供应商人员都应接受有关其数据保护，安全和保密义务的充分培训，并应承担维护机密性的书面义务。

5.2 供应商将自费实施适当的技术和组织措施，以确保与风险相称的安全级别，并保护控制器数据免遭个人数据泄露。这些措施将考虑到最新技术，实施成本以及性质，范围， 处理的背景

和目的，以及自然人的权利和自由的可能性和严重程度不同的风险，以确保与风险相适应的安全水平。 特别是，供应商采取的措施应包括 本附录 2 中所述的措施。未经客户事先书面同意，供应商可以更改或修改**附件 2** 中所述的技术和组织措施，前提是供应商必须保持至少同等水平的保护。应客户要求，供应商将以 **附件 2** 中所示的形式提供技术和组织措施的最新说明。

5.3 供应商应遵守第 7 条中规定的要求，要求任何分包商处理控制器数据。

5.4 供应商应遵守第 8 条中规定的要求，协助客户响应第三方的询问，包括数据主体根据适用的数据保护法行使其权利的任何请求。

5.5 在确认任何个人数据泄露事件发生后，供应商应立即通知客户，并及时提供客户为客户所合理要求的所有信息和合作 (如果客户是 MSP 或 OEM ，则应提供其控制人) 根据适用的《数据保护法》 (并按照规定的时间表) 履行其数据泄露报告义务。 供应商应进一步采取所有必要措施和行动，以补救或减轻个人数据泄露的影响，并应随时向客户通报与个人数据泄露相关的所有动态。

5.6 供应商应向客户 (如果客户是 MSP 或 OEM ，则为其控制人) 提供客户 (或在适用情况下为控制人) 可能需要的所有合理且及时的协助，以便进行数据保护影响评估，并在必要时 请咨询其相关的数据保护机构。 此类协助应由客户承担费用。

5.7 供应商应在本附录终止或到期后的合理时间内删除控制器的控制器数据，在每种情况下，在适用的欧洲法律允许的范围内删除控制器的控制器数据。

5.8 供应商应遵守第 6 条中规定的要求，向客户 (如果客户是 MSP 或 OEM ，则为其控制人) 提供必要的信息，以证明供应商遵守本附录中规定的义务。

6. 客户的审计权限

6.1 客户承认，独立第三方审计员定期根据 SSAE 18 SOC 2 标准对供应商进行审计。 供应商应根据要求向客户提供其 SOC 2 审计报告的副本，该报告应遵守主要协议的保密规定，作为供应商的机密信息。客户承认并同意，撰写此类报告的第三方审计师 (“**作者**”) 不对客户或客户审计师承担任何责任或责任，除非客户与提交人另行签订了“照顾责任协议”。供应商还应回复客户提交的任何书面审计问题，前提是客户每年不得多次行使这项权利。

7. 子处理器

7.1 客户同意本附录日期供应商的现有子处理器，这些子处理器列在 https://www.sophos.com/zh-cn/legal 上 (“**子处理器列表**”)。供应商不会在未事先通知客户的情况下将任何控制器数据的处理分包给任何其他第三方子处理器 (每个都是“**新的子处理器**”)。供应商将提前提供关于添加任何新的分包商的通知 (包括其执行或将要执行的处理的一般详细信息) ，可以通过在分包商列表中发布此类添加的详细信息来发出通知。如果客户在供应商将新的子处理器添加到子处理器列表后 30 天内未以书面形式反对供应商任命新的子处理器 (基于与控制器数据保护相关的合理理由) ， 客户同意将被视为已同意该新子处理器。如果客户向供应商提供此类书面异议，供应商将在 30 天内以书面形式通知客户：(i) 供应商不会使用新的分包商来处理控制器数据；或 (ii) 供应商无法或不愿这样做。如果发出第 (ii) 款中的通知，客户可在该通知发出后 30 天内， 选择终止本附录，并在向供应商和供应商发出书面通知后终止关于受影响处理的主要协议，该协议仅适用于位于欧洲经济区和英国的客户， 授权按比例退还或贷记终止后剩余期间的任何预付费。但是，如果在该时间范围内未提供此类终止通知，客户将被视为已同意新的分包商。供应商将对新的子处理商实施数据保护条款，以保护控制方数据符合本附录规定的相同标准，对于任何此类子处理商导致的任何违反本附录的行为，供应商将承担全部责任。

8. 第三方的查询

8.1 供应商应向客户 (如果客户是 MSP 或 OEM ，则为控制器) 提供所有合理且及时的协助，费用由客户承担，以使客户能够对以下事项作出响应：(i) 数据主体为行使其在适用的数据保护法下的任何权利 (包括其访问，更正，异议，擦除和数据可移植性等权利 (如适用) 而提出的任何请求； 和 (ii) 从数据主体，监管机构或其他第三方收到的与处理控制器数据相关的任何其他通信，查询或投诉。 如果有任何此类请求，信函，咨询或投诉直接向供应商提出，供应商应立即通知客户，并提供相关的全部详细信息。

9. 国际数据传输

9.1 某些产品使客户能够选择是否将此类产品的控制器数据存放在数据中心，这些数据中心可能位于 (i) 欧洲经济区， (ii) 英国或 (iii) 美利坚合众国 (“**中央存储位置**”)。此选项在安装，帐户创建或首次使用相关产品时进行。一旦选中，则无法在以后更改中央存储位置。

9.2 客户承认并同意，无论选择的中央存储位置 (如果相关) 如何，控制器数据都可以通过或导出到其他司法管辖区 (英国和 / 或欧洲经济区以外) ：(i) 针对 Sophos 的恶意软件，安全威胁，误报分析以及研究和开发目的的全球技术人员和工程师团队， (ii) 为了提供技术和客户支持，帐户管理，计费和其他辅助功能，以及 (iii) 第 3.1 条提及的文档中明确描述的功能。

9.3 供应商不应传输控制器数据 (也不允许处理控制器数据) 欧洲以外的国家 / 地区，除非根据适用的数据保护法将数据传输到被认为足够的国家 / 地区，或者供应商采取必要措施确保数据传输符合适用的数据保护法律，例如但不限于 使用欧盟 特殊类别客户 (不时修订)。

9.4 如果联合王国不再受欧盟法律约束，第 9.3 条所述的转移限制也将适用于从欧洲经济区向联合王国转移控制器数据。

9.5 如果第 9.3 条适用，因为供应商或供应商附属机构将在英国或欧洲经济区以外的国家 / 地区处理控制器数据，则在这种情况下 (仅限于控制器数据的任何传输， 不存在适用的数据保护法中承认的允许此类传输的其他措施 (例如，但不限于 向根据适用的数据保护法被视为为个人数据提供充分保护的国家 / 地区的接收者转移或向根据适用的数据保护法获得具有约束力的公司规则授权的接收者转移) 转移控制器数据， 双方同意：

(a) 对于从欧洲经济区转移的款项，欧盟控制者对处理者条款应适用，此类欧盟 SCC 在此作为参考纳入本附录；

(b) 对于从英国转账，欧盟控制者对处理者条款应适用 (在此将欧盟 SCC 纳入本附录) ，前提是此类欧盟控制者对处理者条款应受英国附录的约束。

9.6 如果第 9.3 条适用，因为供应商或供应商附属机构将在英国或欧洲经济区以外的国家 / 地区处理控制器数据，则在这种情况下 (仅限于控制器数据的任何传输， 不存在适用的数据保护法中承认的允许此类传输的其他措施 (例如，但不限于 在适用的数据保护法下，向被视为为个人数据提供充分保护的国家 / 地区的收件人转移或向根据适用的数据保护法获得具有约束力的公司规则授权的收件人转移) (如第 3.3 (ii) 条所述) 客户是第三方控制者的处理者，而供应商是子处理者，双方同意：

(a) 对于从 EEA 进行的转账，应适用欧盟处理器至处理器条款，此类欧盟 SCC 在此作为参考纳入本附录；

(b) 对于从英国转账，欧盟处理人对处理人条款应适用 (在此将这些欧盟 SCC 纳入本附录)，前提是此类欧盟处理人对处理人条款应受英国附录的约束。

9.7 欧盟特殊类别客户的附录应按照下文附件 4 的规定完成。

9.8 对于欧盟 SCC 的每个模块，如果适用：

(a) 第 7 条中的可选对接条款不适用；

(b) 第 9 条下的备选案文 2 应适用。 数据进口方应在子处理方列表的任何预期更改 (通过添加或替换) 发生前 30 天通知数据出口方。

(c) 在第 11 条中，任择语言不适用；

(d) 就第 13(a) 条而言：

- 如果数据出口者是在欧盟成员国中建立的：负责确保数据出口者遵守 (欧盟) 第 2016/679 号法规 (数据传输) 的监管机构将是数据出口者成立所在的主管监管机构，并将担任主管监管机构。

(e) 为第 17 条的目的，欧盟 SCC 应受数据出口国所在欧盟成员国的法律管辖；

(f) 为第 18(b) 条的目的，争议将在数据出口者所在欧盟成员国的法院得到解决。

10. 持续时间

10.1 本附录自主要协议双方执行 (或主要协议生效之日，如以后) 开始，并持续至：(i) 客户使用和接收产品的权利到期 (如主协议或任何相关许可权利中所述)；以及 (ii) 主协议终止。

11. 其他法规

11.1 对本增编的修改和修正需要书面形式。这也适用于对第 11.1 条的更改和修改。

11.2 在任何情况下，供应商对客户的责任都不应超出主协议中规定的供应商对责任的限制。 主协议中规定的供应商责任限制应在主附录和本附录中全面适用，因此单一的责任限制制度应适用于主协议和本附录。

11.3 本增编应受英格兰和威尔士法律管辖并根据其进行解释，而不考虑法律冲突原则。在适用法律允许的范围内，英格兰法院应拥有专属管辖权，以裁决因本增编引起，根据本增编产生或与本增编相关的任何争议或索偿。

11.4 如果与本数据处理附录的条款和双方签订的任何 SCC 的条款有任何冲突，适用的欧盟 SCC 的条款应优先。

SOPHOS
Cybersecurity made simple.

附件 1.
数据处理说明

本图 1 描述了供应商将代表客户执行的处理。

(a) 加工作业的标的物，性质和目的
控制器数据将受以下基本处理活动的制约 (请具体说明) ：

1. 提供客户根据主协议购买的产品
2. 提供客户管理和客户技术支持服务

供应商提供的产品旨在检测，防止和管理或协助供应商检测，防止和管理系统，网络，设备，文件和客户提供的其他数据内部或针对这些数据的安全威胁。 这些系统，网络，设备，文件和其他数据中所包含的任何信息的内容仅由客户决定，而不是由供应商决定。

(b) 处理作业的持续时间：
控制器数据将在以下时间内处理 (请具体说明) ：

主要协议中指定的持续时间 (或主要协议的期限，如果未另行指定)。

(c) 数据主体
主计长数据涉及以下类别的数据主体 (请具体说明) ：

‘s 主体包括客户或客户最终用户通过产品向供应商提供数据的相关人员 (或按其指示提供)。

(d) 个人数据的类型
控制器数据涉及以下类别的数据 (请具体说明) ：

客户或客户最终用户通过产品， (或按其指示) 或联系信息向供应商提供的个人相关数据

(e) 特殊类别的数据 (如适用)
主计长数据涉及以下特殊类别的数据 (请具体说明) ：

除非另有说明，否则供应商的产品不能用于处理特殊类别的数据。

附件 2.
技术和组织措施

其中某些措施可能仅与托管产品相关或适用。

A) 物理访问控制。

- Sophos 具有物理访问控制策略；
- 所有工作人员都持有身份证 / 出入证；
- 设施入口由出入证或钥匙加以保护；
- 设施分为：(一) 公共进入区 (如接待区)，(二) 一般工作人员进入区和 (三) 限制进入区，只有那些有明确业务需求的人员才能进入；
- 出入证和钥匙根据个人的授权出入级别控制对每个设施内受限区域的出入；
- 个人的访问级别由高级工作人员批准，并每季度进行一次验证；
- 大型场地入口处有接待人员和 / 或安保人员；
- 设施受到警报的保护；
- 访客已预先注册并维护访客日志。

B) 系统访问控制。

- Sophos 具有逻辑访问控制策略；
- 网络在每个互联网连接上都受到防火墙的保护；
- 内部网络由防火墙根据应用程序敏感度进行分段；
- 所有防火墙上都运行 IDS 和其他威胁检测和阻止控制；
- 过滤网络流量基于应用“最少访问”原则的规则；
- 只有在执行职务所需的范围内和期限内，授权人员才能获得访问权，并每季度审查一次；
- 对所有系统和应用程序的访问由安全的登录程序控制；
- 个人拥有唯一的用户 ID 和密码供自己使用；
- 对密码进行强度测试，并强制对弱密码进行更改；
- 屏幕和会话在一段时间不活动后自动锁定；
- Sophos 恶意软件保护产品作为标准安装；
- 定期对 IP 地址和系统进行漏洞扫描；
- 系统会定期修补，并设置优先级优先级系统以快速跟踪紧急修补程序。

C) 数据访问控制。

- Sophos 具有逻辑访问控制策略；
- 只有在执行职务所需的范围内和期限内，授权人员才能获得访问权，并每季度审查一次；
- 对所有系统和应用程序的访问由安全的登录程序控制；
- 个人拥有唯一的用户 ID 和密码供自己使用；
- 对密码进行强度测试，并强制对弱密码进行更改；
- 屏幕和会话在一段时间不活动后自动锁定；
- 使用 Sophos 加密产品对笔记本电脑进行加密；
- 发件人在发送任何外部电子邮件之前被指示考虑进行文件加密。

D) 输入控制。

- 对所有系统和应用程序的访问由安全的登录程序控制；
- 个人拥有唯一的用户 ID 和密码供自己使用；

- Sophos Central 产品使用传输层加密来保护传输中的数据；
- 客户端软件和后端 Sophos 系统之间的通信通过 HTTPS 执行，以保护传输中的数据，通过证书和服务器验证建立信任通信。

E) 分包商控制。
- 拥有数据访问权限的分包商在入职前并在入职后根据要求执行 IT 安全审查程序；
- 根据分包商的职责，合同包含适当的保密和数据保护义务。

F) 可用性控制。
- Sophos 保护其场所免受火灾，洪水和其他环境危害；
- 备用发电机可在断电时维护电源；
- 数据中心和服务器机房使用气候控制和监控；
- Sophos Central 系统负载平衡，并在三个站点之间进行故障转移，每个站点运行两个软件实例，其中任何一个都能够提供完整的服务。

G) 隔离控制。
- Sophos 维护并应用质量控制流程来部署新的客户产品；
- 测试和生产环境是分开的；
- 新软件，系统和开发在发布到生产环境之前进行测试。

H) 组织控制。
- Sophos 拥有一支专门的 IT 安全团队；
- 风险和合规团队管理内部风险报告和控制，包括向管理层报告关键风险；
- 事件响应流程可及时识别和补救风险和漏洞；
- 每位新员工都要接受数据保护和 IT 安全培训；
- IT 安全部门每季度开展安全意识活动。

附件 3.
托管产品

- Sophos Central
- Sophos Cloud Optix
- Central Device Encryption
- Central Endpoint Protection
- Central Endpoint Intercept X
- Central Endpoint Intercept X Advanced
- Central Mobile Advanced
- Central Mobile Standard
- Central Phish Threat
- Central Intercept X Advanced for Server
- Central Server Protection
- Central Mobile Security
- Central Web Gateway Advanced
- Central Web Gateway Standard
- Central Email Standard
- Central Email Advanced
- Central Wireless Standard
- 通过 Sophos Central 管理和操作的任何其他 Sophos 产品

附件 4.

欧盟标准合同条款的参考数据

欧盟标准合同条款附录 1

答：缔约方名单

数据出口国：[*数据出口者的身份和详细联系信息，包括负责数据保护的任何联系人*]

客户名称：根据主协议提供给供应商

地址：根据主要协议联系电子邮件向供应商提供：

联系人姓名 / 职位：根据主要协议提供给供应商

与根据本条款传输的数据相关的活动：如上文第 3 条所述

角色 (控制器 / 处理器) ：控制器

数据导入者：[*数据进口方及其数据保护官员和 / 或欧洲联盟代表的身份和详细联系信息 (如适用)*]

姓名：Sophos Limited (代表其欧盟和瑞士子公司)

地址：The Pentagon， Abingdon Science Park Abingdon， OX14 3YP， UK

注册号：2096520

联系人的姓名，职位和详细联系信息： dataprotection@sophos.com

与根据本条款传输的数据相关的活动：如上文第 3 条所述。

角色 (控制器 / 处理器) ： 处理器

B. 转让说明

个人数据被传输的数据主体类别：

如上文 C 节附件 1 所述

传输的个人数据类别：

如上文 D 节附件 1 所述。

传输敏感数据 (如果适用) ，并实施充分考虑数据性质和所涉风险的限制或保障措施，例如严格的目的限制，访问限制 (包括仅限经过专门培训的员工访问) ，保存数据访问记录， 继续转让的限制或其他安全措施：

如上文 E 节附件 1 所述。

传输频率 (例如数据是一次性传输还是连续传输)。

连续

处理的性质

如上文 A 节附件 1 所述。

数据传输和进一步处理的目的

如上文 A 节附件 1 所述。

个人数据将被保留的期间，或者，如果无法保留，用于确定该期间的标准

在合同期内。

对于传输到 (子) 处理器，还应指定处理的主题，性质和持续时间

如上文第 3 条所述。

主管监督机构

见上文第 9.8 条

附件二 - 确保数据安全的技术和组织措施，包括技术和组织措施[1]

这些措施见 上文附件 2。

附录三 – 子处理者列表[2]

由于第 9(a) 条，未 选择备选案文 1 ，因此不是必需的。

[1]除模块四外，所有模块都必须填写附件二。
[2]附录 III 仅适用于已选择第 9(a) 条选项 1 的模块 2 (将控制器转移到处理器) 和模块 3 (将处理器转移到处理器)。