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。 本协议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：18，2022 年 12 月

如果此数据处理附录(下称“附录”)被明确地以参考方式纳入 Sophos Limited (定义见第 2 条), Sophos Limited 是一家在英格兰和威尔士注册的公司，注册办公地点为五角大楼，Abingdon Science Park，Abingdon，Oxfordshire，OX14 3YP，英国(“供应商”)和供应商的客户(“客户”)，本附录构成主要协议的一部分，在供应商和客户之间生效。

本附录中使用的大写术语定义如下文第 2 条所述。如有要求，我们可以提供另一种语言的本附录副本。在发生冲突时，以英文本为准。

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 https://www.sophos.com/zh-cn/legal/sophos-msp-partner-terms-and-conditions 上的 MSP 协议形式类似的 MSP 协议(“MSP 协议”)，则客户是托管服务提供商 (“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代表客户收集，使用和以其他方式处理控制人个人数据。本附录规定了双方在此类处理中的义务，并对主要协议的条款和条件进行了补充。

1.4. 无论本协议或本附录的任何其他条款如何，双方均同意控制人个人数据不应包括联系信息，付款或账单信息，或有关业务联系人和客户管理员的其他个人数据，包括姓名，电子邮件地址和联系信息，哪家供应商代表自己收集和处理，以便管理其客户关系，与当前，以前和潜在客户及业务合作伙伴进行沟通，以及以其他方式管理其业务关系(“CRM 数据”)。

1.4.1. 供应商是 CRM 数据的控制人，将根据其在适用的数据保护法 和 供应商集团隐私声明中的义务处理 CRM 数据。

1.4.2. 除第节所述 1.4.1 的情况外，供应商根据本附录所承担的义务不适用于 CRM 数据。

1.5. 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”是指在适用范围内：(a)欧洲议会和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流动的第 2016/679 号欧盟条例(《一般数据保护条例》或《一般数据保护条例》)；(b)《电子隐私指令》(欧盟指令 2002/58/EC)；(c)《保护公民权利和社会权利国际公约》；和(d)任何和所有适用的国家数据保护立法，包括根据(a)或(b)制定或依据制定的立法；在每种情况下，可不时修订或取代。

“受益人”具有 MSP 协议中赋予的含义。

“CCPA”是指经《2020 年加利福尼亚隐私权法案》修订的《加利福尼亚消费者隐私法》，该法案已在加州编纂。公民代码 § § 1798.100 - 1798.199.100 和加州消费者隐私法案(California Consumer Privacy Act Regulations)发布，Cal.代码注册 tit。11，div。6，ch.1 份，每份经修正；

“条款”的涵义，须符合《管制条文》所赋予的涵义。

“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)。

“控制人个人数据”是指供应商根据本服务代表控制人处理的个人数据。

“控制人至处理器条款”是指 SCC 的模块二条款。“CRM 数据”是指有关业务联系人和客户管理员的联系信息，付款或计费信息或其他个人数据，包括姓名，电子邮件地址和联系信息，哪家供应商代表自己收集和处理，以管理其客户关系，与当前，以前和潜在客户及业务合作伙伴进行沟通，以及以其他方式管理其业务关系。

“数据主体”是指与 Sophos 个人数据相关的个人。

“数据主体请求”是指数据主体根据适用的数据保护法(包括其访问，删除和更正的权利)行使权利的任何请求。

“EEA”指欧洲经济区，包括(a)欧洲经济区(EEA)的成员国和(b)联合王国。

“最终客户”具有 OEM 协议中赋予的含义。

“欧洲”(和"欧洲")是指(a)欧洲经济区("EEA")的成员国和(b)联合王国。

“托管 产品”是 指附件 3 中列出的产品。

“ICO”是指在联合王国设立的信息专员办公室

“主要协议”统称为书面协议，包括及其附件，附录和修订，根据这些协议，供应商向客户提供某些服务。

“个人数据”是指可识别，可用于识别或以其他方式链接或合理链接到特定个人或家庭的任何信息，以及根据适用的数据保护法律和法规定义为“个人数据”，“个人信息”或等效术语的任何信息。

“个人数据泄露”是指导致意外或非法销毁，丢失，更改，未经授权披露或访问，供应商根据本附录处理的控制人个人数据。

“处理者”是指代表控制者并在其指示下处理个人数据的个人或实体，包括根据 CCPA 作为“服务提供商”的任何实体。

“受限传输”是指客户向供应商传输控制器个人数据，如果适用的数据保护法在没有适用的标准合同条款和适用的英国附录的情况下禁止进行此类传输。

“敏感数据”是指“特殊类别的个人数据”，“敏感个人数据”，“敏感数据”以及适用数据保护法中定义的等效术语。

“服务”是指供应商根据主要协议提供和/或提供的任何和所有产品和/或服务。

“标准合同条款”或“SCC”是指根据欧洲议会和欧洲委员会执行 2021 年 6 月 4 日第(EU) 2021/914 号决定批准的条例(EU) 2016/679 向第三国传输个人数据的标准合同条款。

“子处理者”是指由供应商或代表供应商指定处理控制人个人数据的任何个人或实体(不包括供应商的任何员工)或实体。

“监管机构”是指与适用的数据保护法律和法规相关的主管监管机构，包括 GDPR 所定义的监管机构(如适用)。

“英国附录”是指由 ICO 发布的欧盟委员会标准合同条款的国际数据传输附录， 该附录 根据英国相关数据保护法由主管监管机构不时修订或替换

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. 供应商处理控制人个人数据的主题事项和持续时间，包括处理的性质和目的，要处理的控制人个人数据的类型以及数据主体的类别，应如中所述：(a)本附录；(b)主要协议；(c)附件 1 (数据处理说明)中的任何说明；以及(d)根据下面第 4 条发布的客户说明。

3.2. 客户有责任确保(a)控制者有合法依据处理供应商将代表客户执行的控制人个人数据，并且(b)控制者已从数据主体处获得客户和供应商处理控制者个人数据(包括但不限于敏感数据)可能需要的所有必要同意；并且(c)其在其他方面遵守并将确保其向供应商发出的处理控制人个人数据的指示在所有方面均遵守适用的数据保护法。

3.3. 双方同意，供应商是控制器个人数据的处理者或子处理者，而客户是(a)客户为最终用户的控制者，或(b)客户为 MSP 或 OEM 的处理器(适用于第三方控制者)。

4. 客户说明

4.1. 客户指示供应商在提供和执行服务所需的合理情况下，以及在本协议和主要协议中另有规定的情况下，处理控制人个人数据。供应商应按照客户的书面处理说明(如本协议所述)处理控制人个人数据，除非(a)供应商与客户之间另有书面协议；或(b)供应商受法律约束的情况下(在这种情况下，供应商应在处理之前将该法律要求通知客户，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示违反了适用的数据保护法(但没有规定供应商有义务积极监控客户的合规性)，则供应商将立即通知客户相同情况，并暂停处理控制人个人数据。

4.3. 在不限制放弃的情况下，如果《加利福尼亚消费者隐私法》(“**CCPA**”)适用于控制人个人数据，供应商 还同意：

4.3.1. 供应商不得使用，披露或以其他方式处理控制人个人数据，除非是出于执行服务的特定目的，符合本附录和主要协议的条款，以及适用法律的其他要求。尽管有上述规定：

a. 供应商可根据第 7 条的条款，让子处理商处理控制人个人数据；

b. 供应商不会在 客户与供应商之间的直接业务关系之外或出于供应商自身的商业目的处理 控制人个人数据；尽管有上述规定，双方同意，在 CCPA 适用的范围内，供应商只能出于主要协议和本附录中规定的特定业务目的或出于 CCPA 条例明确授权的其他目的处理控制人个人数据。

c. 供应商不会“共享”或“出售”(根据 CCPA 中定义的条款)任何控制人个人数据；

d. 供应商将(并将促使每个子处理商)遵守 其根据 CCPA 承担的义务，并将提供与 CCPA 所要求的相同级别的隐私保护；以及

e. 如果供应商认为无法遵守本附录或适用的数据保护法的条款，供应商应立即通知客户并 授予客户采取合理和适当步骤的权利，以确保以符合 控制人在 CCPA 下的义务的方式处理控制人个人数据。

f. 供应商不会在主协议到期或终止时保留控制人个人数据，第节中规定的除外 8；

5. 供应商的职责

5.1. 处理控制人个人数据的所有供应商人员应接受有关其数据保护，安全和保密义务的充分培训，并应遵守书面或法定义务以保持机密性。

5.2. 供应商将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，并保护控制人个人数据免受个人数据泄露的影响。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. 供应商应遵守以下第 7 条中规定的要求，让任何子处理商处理控制人个人数据。

5.4. 供应商应遵守以下第 8 条中规定的要求，以帮助客户回复第三方的询问，包括数据主体提出的任何请求，以行使适用数据保护法规定的权利。

5.5. 在确认发生任何个人数据泄露后，供应商应及时通知客户，并应及时提供客户合理要求的所有信息和合作，以便为客户提供服务(如果客户是 MSP 或 OEM，则为其控制人)履行适用数据保护法规定的数据违规报告义务(并按照规定的时间范围)。供应商应进一步采取合理必要的措施和行动，以补救或减轻个人数据违规的影响，并应将与个人数据违规相关的事态发展告知客户。

5.6. 供应商应向客户(或者，如果客户是 MSP 或 OEM，则应向其控制人)提供合理且及时的帮助，作为客户(或控制人，如果适用)可能要求进行数据保护影响评估或适用数据保护法律要求进行的其他评估，并在必要时咨询其相关数据保护机构。此类协助应由客户承担费用。

5.7. 除非适用法律另有要求，供应商应在本附录终止或到期后的合理时间内删除控制者的个人数据，除非适用法律禁止。供应商应根据要求向客户确认此类控制人个人数据已根据本附录删除。如果适用法律要求供应商保留任何控制人个人数据，则供应商应采取措施确保控制人个人数据的持续机密性和安全性(只要其得到维护)。

6. 客户的审计权限

6.1. 客户确认，独立第三方审计师定期根据 SSAE 18 SOC 2 标准对供应商进行审计。在合理的要求下，供应商应向客户提供其 SOC 2 审计报告的副本，该报告应作为供应商的机密信息遵守主要协议的保密规定。供应商还应对客户提交给它的合理的书面审核问题作出回应，前提是客户每年不得行使此权利超过一次。

6.2. 如果客户合理地认为第 6.1 条下提供的材料不足以证明供应商遵守本附录，则客户可以书面请求并遵守本附录中第 6.2 条(a)-(d)项的规定，供应商向客户提供证明遵守本附录中规定的义务(包括适用范围内的标准合同条款)所需的所有合理必要信息，并允许客户或客户的独立人员进行审计(包括检查)并为其提供帮助，不属于本附录所涵盖的处理活动供应商竞争对手的第三方审计员。

a. 在根据第 6.2 条请求审查或审计之前，客户应考虑第 6.1 条下所述的相关供应商第三方认证和审计；

b. 客户应至少提前 60 天向处理器合理通知根据本条款 6.2 进行审核或检查的请求，并将采取(并确保其每一名审计员采取)合理措施，避免和防止任何损害或伤害，并尽量减少这种审计或检查造成的任何干扰；

c. 每年进行一次审计或检查，除非监管机构或适用的数据保护法律要求这样做；以及

d. 客户应承担任何此类审计的全部费用，并应向供应商偿还供应商根据此类审计而产生的合理成本和费用，包括供应商，其关联公司或其子处理商按照供应商当时的专业服务费率进行任何此类审计或检查所花费的任何时间，应根据客户要求提供。

7. 子处理器

7.1. 客户同意使用在本附录之日在 https://www.sophos.com/zh-cn/legal (“子处理商列表”)列出的供应商现有子处理商 以及供应商附属公司。客户明确同意供应商在遵守本第 7 条规定的条款的前提下聘用其他第三方子处理商(每个“新子处理商”)。供应商将在添加任何新的子处理商之前提前三十(30)天向客户发出通知，通知可通过将添加的详细信息张贴到子处理商列表中来提供。

7.2. 如果客户在供应商将新的子处理商添加到子处理商列表后 30 天内，未以书面形式反对供应商任命新的子处理商(基于与保护控制人个人数据相关的合理理由)，客户同意将其视为已同意该新子处理商。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：(a)供应商不会使用新子处理商处理控制人个人数据；或(b)供应商无法或不愿意这样做。如果发出第 (b) 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，这些子处理方对本附录中规定的控制人个人数据实施同等保护。供应商仍将对每个子处理商的义务的履行承担全部责任。

8. 第三方的查询

8.1. 供应商应将其从数据主体，监管机构或其他第三方收到的与处理控制人个人数据相关的任何隐私请求，通信，询问或投诉通知客户，并提供该等数据的完整详细信息，但不应直接回复数据主体，除非法律另有规定。

8.2. 在必要的范围内，供应商将向客户(或者，如果客户是 MSP 或 OEM，则为控制器)提供合理且及时的帮助，费用由客户承担，以使客户(或者如果客户是 MSP 或 OEM，则为控制器)能够响应：(a)数据主体要求行使适用数据保护法规定的权利(包括适用情况下的访问权，更正权，异议权，擦除权和数据可移植性权)，和(b)从监管机构或其他第三方收到的与控制人个人数据处理相关的请求。

9. 国际数据传输

9.1. 某些产品可能允许客户选择将此类产品的控制器个人数据存放在何处，包括存放在数据来源管辖区之外的数据中心。这些地点可包括(a)欧洲经济区，(b)联合王国，(c)美利坚合众国；或主要协议中指定的另一地点("中央储存地点")。此选择在产品安装，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. 客户承认并明确同意，无论所选的中央存储位置(如相关)如何，均受限转让，但须遵守本第 9 条中规定的义务。

9.3. 对于任何限制性转让：

9.3.1. 特殊类别客户和英国附录明确纳入本附录，并构成本附录的一部分；

9.3.2. 根据 9.3.3 本协议第 4 节 和附件，客户和供应商特此签订并同意：(i)特殊类别客户(SCC)，适用于向供应商限制传输控制人个人数据的范围；和(ii)英国附录，该附录将适用于受英国数据保护法和法规约束的控制人个人数据的任何受限传输，并对 SCC 进行修改和补充；以及

9.3.3. 在不违反本合同附件 4 条款的前提下，《公约》模块 2 应适用。

9.4. SCC 的附录应按照以下附件 4 的规定填写。

10. 持续时间

10.1. 本附录自(a)双方签署主要协议或(b)主要协议生效之日(如果较晚)开始生效，并持续至以下两者中较早者：(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. 对本附录的修改和修改需要书面形式。这也适用于对本条款的更改和修改 11.1。

11.2. 在任何情况下，供应商就本附录引起的或与本附录相关的任何问题对客户的责任均不得超过主协议中规定的供应商责任限制。主要协议中规定的供应商责任限制应在主要协议和本附录中全部适用，因此，单一责任制度限制应在主要协议和本附录中适用。

11.3. 本增编(不包括特殊类别客户)应受英格兰和威尔士法律管辖并根据其解释，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以及双方签订的任何特殊类别客户的条款发生冲突，则适用特殊类别客户的条款(包括其任何附件)优先。

12. 法律的变化

12.1. 如果由于适用数据保护法的变更而需要对本附录进行任何修订，则任何一方均可向另一方提供有关该法律变更的书面通知。双方将真诚地讨论和谈判本附录的任何必要的修改，以解决此类更改。各方不会根据本第 12 条或其他条款不合理地拒绝同意或批准修改本附录。

12.2. 如果标准合同条款或英国附录被替换，更新或替换为新版本(“新条款”)，客户同意供应商在事先书面通知客户后，根据需要更新本附录，以纳入此类新条款，作为先前标准合同条款或英国附录的修订或替换。

附件 1.

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

控制人个人数据将接受以下基本处理活动(请具体说明)：

- 提供客户根据主协议购买的产品
- 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：

控制器个人数据将在以下持续时间内处理(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

控制人个人数据涉及以下类别的数据主体(请具体说明)：

- 客户的人员和最终用户
- 代表客户处理与 Sophos 产品相关的个人数据的其他数据主体

(d) 个人数据的类型

控制器个人数据涉及以下数据类别(请具体说明)：

- 用户名和其他标识符
- 网络和网络活动信息
- 可能与 Sophos Products 相关的其他信息

(e) 特殊类别的数据 (如适用)

控制器个人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。

1. 物理访问控制。

   (a) Sophos 有一项实际出入控制政策；

   (b)所有工作人员都携带身份证/出入证；

   (c)设施的入口受到出入证或钥匙的保护；

   (d)设施分为：(i)公共出入区(如接待区)；(ii)一般工作人员出入区；(三)仅可由具有明确业务需求的人员进入的限制进入区域；

   (五)出入证和钥匙根据个人的授权访问级别控制每个设施内限制进入区域的访问；

   (f)个人出入级别由高级工作人员批准，每季度核查一次；

   (g)较大地点入口处有接待和(或)安保人员；

   (h)设施受到警报保护；

   ㈠访客预先登记，访客记录得到维护。

2. 系统访问控制。

   (a) Sophos 有一个逻辑访问控制策略；

   (b)网络在每个 Internet 连接上都受到防火墙的保护；

   (c)内部网络由防火墙根据应用程序的敏感性进行分段；

   (d) IDS 和其他威胁检测和阻止控制在所有防火墙上运行；

   (e)过滤网络流量是根据适用"最少访问"原则的规则；

   (f)访问权只授予经授权的人员，其范围和期限为履行其工作职责所需的时间，并每季度审查一次；

   (g)对所有系统和应用程序的访问受安全登录程序的控制；

   (h)个人有唯一的用户 ID 和密码供自己使用；

   (i)密码经过强度测试，并强制改为弱密码；

   (j)屏幕和会话在一段时间不活动后自动锁定；

   (k) Sophos 恶意软件防护产品作为标准安装；

   (l)对 IP 地址和系统进行定期漏洞扫描；

   (m)系统定期修补，并使用优先级系统快速跟踪紧急修补程序。

3. 数据访问控制。

(a) Sophos 具有逻辑访问控制策略；

(b)访问权限仅授予授权人员以履行其工作职责所需的范围和持续时间，并每季度进行审查；

(c)对所有系统和应用程序的访问由安全登录程序控制；

(d)个人拥有唯一的用户 ID 和密码供自己使用；

(e)密码经过强度测试并强制更改弱密码；

(f)屏幕和会话在一段时间不活动后自动锁定；

(g)使用 Sophos 加密产品对笔记本电脑进行加密；

(h)发件人在发送任何外部电子邮件之前应考虑文件加密。

4. 输入控制。

(a)对所有系统和应用程序的访问受安全登录程序的控制；

(b)个人拥有唯一的用户 ID 和密码供自己使用；

(c) Sophos Central 产品使用传输层加密来保护传输中的数据；

(D)客户端软件与后端 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。

5. 分包商控制。

(a)能够访问数据的分包商在入职之前和之后根据需要执行信息技术安全审查程序；

(b)合同包含基于分包商职责的适当保密和数据保护义务。

6. 可用性控制。

(a) Sophos 保护其房地免受火灾，水灾和其他环境危害；

(b)备用发电机可在停电时维持供电；

(c)数据中心和服务器室采用气候控制和监测；

(D) Sophos Central 系统是负载平衡的，并且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。

7. 隔离控制。

(a) Sophos 维护并应用质量控制流程来部署新的客户产品；

(b)测试和生产环境是分开的；

(c)新软件，系统和开发在发布到生产环境之前进行测试。

8. 组织控制。

(a) Sophos 有一个专门的 IT 安全团队；

(b)风险和合规性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；

(c)事件响应流程及时识别和补救风险和漏洞；

(d)每位新员工都要接受数据保护和 IT 安全培训；

(e) IT 安全部门每季度开展一次安全意识活动。

附件 3.

托管产品

(a) Sophos Central
(b) Sophos Cloud Optix
(c) Central Device Encryption
(d) Central Endpoint Protection
(e) Central Endpoint Intercept X
(f) Central Endpoint Intercept X Advanced
(g) Central Mobile Advanced
(h) Central Mobile Standard
(i) Central Phish Threat
(j) Central Intercept X Advanced for Server
(k) Central Server Protection
(l) Central Mobile Security
(m) Central Web Gateway Advanced
(n) Central Web Gateway Standard
(o) Central Email Standard
(p) Central Email Advanced
(q) Central Wireless Standard
(r)通过 Sophos Central 管理和操作的任何其他 Sophos 产品

附件 4.

限制转让的附加条款

本附件包括根据附录由客户或代表客户向供应商进行受限转让的附加条款，以及完成适用SCC的附录(附件I-III)所需的信息。

各方同意增编即同意并据此执行增编中所有相关部分的SCC，但须遵守 9 增编第节 和本附件的条款。

1. 本附件或附录中未定义但已使用的大写术语应具有特殊类别客户和英国附录(如适用)赋予的含义。

2. 在符合本附件条款的前提下，应适用特殊类别客户的模块2，特殊类别客户的附录应参考本协议附件A完成。

3. 就SCC (模块2)而言：

3.1. 第7条：可选的停靠条款不适用；

3.2. 条例草案第9(a)条：选项2 (一般授权)适用，数据进口商应至少提前30天书面通知数据出口商任何预期更改。

3.3. 第11条：任择语言不适用。

3.4. 就第13 (a)条而言，主管监管机构应按以下方式适用：

3.4.1. 如果数据出口方位于欧盟成员国，则监管机构将是数据出口方所在司法管辖区的主管监管机构；

3.4.2. 如果数据出口方在英国成立，或者受限传输受英国数据保护法律和法规的约束，则主管监管机构应为英国信息专员办公室；

3.4.3. 如果数据出口方在瑞士设立，或者受瑞士数据保护法律和法规约束的受限传输，则瑞士联邦数据保护和信息专员应担任主管监管机构；以及

3.4.4. 如果数据出口方未在欧盟成员国，英国或瑞士建立，但属于(EU) 2016/679条例的适用范围根据其第 3 (2)条，监管机构将是数据出口方代表所在司法管辖区的主管监管机构，即爱尔兰数据保护专员。

4. 分别就第17条和第18(b)条而言，SCC应受爱尔兰共和国法律管辖争议将在爱尔兰法院解决，但以下情况除外：(i)如果数据出口方在瑞士成立或受瑞士数据保护法律和法规约束，SCC将受瑞士法律管辖，争议将在瑞士法院解决；并且(ii)如果数据出口方在英国成立或限制传输受英国数据保护法律和法规约束，则SCC应受英国法律管辖，争议将在英国法院解决。

5. **瑞士的附加条款**。如果数据出口方在瑞士成立或受限传输受瑞士数据保护法律和法规的约束：(i) SCC中提及的“欧盟”，“欧盟”或“成员国”是指瑞士；(ii)提及GDPR时还应提及《瑞士联邦数据保护法》(经修订或替换)的同等条款；和(iii)《特殊类别客户(SCC)》也适用于与已识别或可识别法律实体相关的信息的传输，前提是此类信息根据适用的瑞士数据保护法律和法规作为个人数据受到保护。

6. **适用于英国的附加条款**。如果数据出口方在英国成立或受限传输受英国数据保护法律和法规的约束：

6.1. 《特殊类别合同》应根据英国增补件第2部分(强制性条款)的规定阅读，并被视为已被其修正；以及

6.2. 就第一部分而言，表1和表2是参考本附件的附件A和B (如适用)填写的，表3是参考本附件中的信息填写的，出于表4的目的，数据进口商可以按照英国附录第19节的规定结束英国附录。

附件 4 附录 A

SCC 的附录(模块 2)：控制器到处理器的受限传输

附件一

A. 缔约方名单

1.数据出口国：[*数据出口者的身份和联系详情，以及其/其在欧盟的数据保护官员和/或代表(如适用)的身份和联系详情*]

名称	根据主协议提供给供应商
地址	根据主协议提供给供应商
确定本组织所需的其他资料	根据主协议提供给供应商
联系人姓名： 位置： 联系方式：	根据主协议提供给供应商
与根据这些特殊类别中心转移的数据有关的活动	如上文增编第 3 条所述
角色	控制器

数据导出器签名和日期：《公约》附件(模块 2)连同本附录和本附录的附件作为增编的一部分执行。

2.数据导入者：[*数据进口商的身份和详细联系信息，包括负责数据保护的任何联系人。*]

名称	Sophos Limited (代表其欧盟和瑞士子公司)
地址	The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK

确定本组织所需的其他资料	注册号 2096520
联系人姓名： 位置： 联系方式：	隐私顾问 dataprotection@sophos.com
与根据这些特殊类别中心转移的数据有关的活动	根据《协定》

Data Importer 签名和日期：《公约》附件(模块 2)连同本附录和本附录的附件作为增编的一部分执行。

B. 转让说明

1.1. *传输个人数据的数据主体*类别。

如附件 1 A 部分所述

1.2 *传输的个人数据*类别.

如附件 1 A 部分所述

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。

无。

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*

提供 Sophos 根据本协议及根据本协议采购的服务。

数据传输和进一步处理的目的

供应商将根据本协议并按照 Sophos 在使用本服务时的指示处理必要的控制人个人数据以执行本服务。

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

根据附录第 10 节的规定，除非另有书面协议，否则供应商将在协议期限内处理个人数据。

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

供应商有权使用供应商在执行本协议或附录时通知 Sophos 的子处理商。

C. 主管监督机构

3.4 如增编附件 4 第节所述 。

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

如增编附件 2 所述。

附录三 – 子处理者列表

不适用(各方已就《公约》第 9 (a)条同意选项 2 (一般授权))。