数据处理附录

本数据处理附录（“附录”）纳入并补充由科睿唯安实体（及其关联公司，合称“科睿唯安”）作为协议一方与客户实体（“客户”或“您”）作为协议另一方签订且不时更新的协议。

客户代表自己签订本附录。并且，在适用的数据保护法要求的范围内，如果科睿唯安处理的是客户的授权关联公司有资格作为控制者的个人数据，则客户以其授权关联公司的名义并代表他们签订本附录。仅出于本附录的目的，除非另有说明，术语“客户”应包括客户和授权关联公司。

本附录中未定义的术语应具有协议中规定的含义。为免生疑义，凡提及“协议”，均应包括本附录，包括本附录中定义的标准合同条款（如适用）。

1. 定义

(a)“关联公司”指直接或间接控制另一实体、受另一实体控制或与该另一实体共同受控的实体；

(b)“协议”指科睿唯安与客户签订的纳入本附录且科睿唯安据其向客户提供一项或多项服务的任何协议。本附录或以引用方式纳入此类协议的其他数据处理条款统称为“协议”。

(c)“授权关联公司”指客户的任何关联公司，其 (a) 受欧盟数据保护法的约束；及 (b) 根据客户与科睿唯安签订的协议被允许使用服务，但没有与科睿唯安签署自己的订单，并且不是本附录中定义的“客户”。

(d)“客户个人数据”指科睿唯安作为处理者代表客户通过服务处理的任何个人数据，详见本附录。为明确起见，客户个人数据不包括科睿唯安是控制者并根据科睿唯安的**公司隐私声明**进行处理的个人数据。

(e)“控制”指占相关实体当时已发行的总权益百分之五十 (50%) 或以上的所有权、投票权或类似权益。术语“受控”应作相应解释。

(f)“数据保护法”指适用于一方根据协议处理客户个人数据的所有数据保护法律法规，包括（如适用）欧盟数据保护法；《加利福尼亚州消费者隐私法案》(“CCPA”)；《加拿大个人信息保护和电子文件法案》(“PIPEDA”)；《巴西通用数据保护法》("LGPD")，第 13,709/2018 号联邦法律；经修订的澳大利亚《1988 年隐私法案》（“澳大利亚隐私法”）；以及英国数据保护法。

(g)“欧盟数据保护法”指适用于欧洲的所有数据保护法律法规，包括 (i) 欧洲议会和理事会关于在处理个人数据方面保护自然人以及此类数据自由流动的第 2016/679 号条例（《一般数据保护条例》）（“GDPR”）；(ii) 关于电子通信行业中个人数据处理和隐私保护的第 2002/58/EC 号指令；(iii) (i) 和 (ii) 的适用国家实施细则；及

(h)“欧盟标准合同条款”指经欧洲委员会批准的处理者的标准合同条款。

(i)”欧洲”就本附录而言，指欧盟、欧洲经济区和/或其成员国和瑞士。

(j)“个人数据泄露”指任何未经授权或非法的安全违规行为，导致由科睿唯安管理或以其他方式控制的系统中的客户个人数据遭到意外或非法销毁、丢失、更改或未经授权披露或访问。

(k)“服务”指协议中规定的相关服务。

(l) “标准合同条款”是指欧盟标准合同条款和英国附录。

(m)“特殊类别的个人数据”指 (a) 遗传数据；(b) 用于唯一识别自然人的生物特征数据；(c) 有关健康或自然人的性生活或性取向的数据；(d) 披露种族、族裔、政治派别或宗教信仰、或工会成员身份的个人数据；及 (e) 与刑事定罪和犯罪相关的个人数据。

(n)“子处理者”指任何由科睿唯安或其关联公司为协助他们履行根据协议或本附录提供服务的义务而聘用的处理者。子处理者可能包括第三方或科睿唯安的关联公司，但不包括科睿唯安的员工、承包商或顾问。

(o) “英国附录”是指由英国信息专员办公室发布的欧盟委员会标准合同条款的国际数据传输附录。

(p) “英国数据保护法”是指任何适用的当前和未来数据保护、隐私和电子营销法律法规，包括 2018 年《英国数据保护法》、英国法律中实施的 GDPR （“英国 GDPR”）以及 2003 年《隐私和电子通信法规》。

(q)“英国国际传输”是指根据《英国数据保护法》，需要不时提供适当保障的个人数据传输。

术语**“适当保障”**、**“控制者”**、**“数据主体”**、**“个人数据”**、**“处理者”**和**“处理”**应具有适用的数据保护法（或如果其中未定义，则为 GDPR）中赋予的含义。对于任何客户个人数据，**“处理”**和**“已处理”**应作相应解释。

2. 角色和职责

(a) 双方的角色。如果适用的数据保护法适用于任何一方对客户个人数据进行的处理，则双方承认并同意 (i) 就客户个人数据的处理而言，客户是控制者，而科睿唯安是代表客户行事的处理者，详见本附录的附件 A（数据处理详细说明）；且 (ii) 客户个人数据应根据适用的数据保护法处理。

(b) 目的限制。科睿唯安应仅根据的客户的书面合法指示并在为遵守适用法律而必需的情况下处理客户个人数据。双方同意，本附录和协议规定了客户就客户个人数据的处理而向科睿唯安发出的完整和最终指示，而在此类指示范围之外的处理（如有）应以双方书面商定的方式进行（“许可目的”）。

(c) 禁止的数据。除非本附录的附件 A 另有规定，否则客户不会向科睿唯安提供（或促使他人提供）任何特殊类别的个人数据供其根据协议进行处理，并且科睿唯安对此类数据不承担任何责任，无论是与个人数据泄露还是其他方面有关。

(d) 客户合规。客户陈述并保证：(i) 其已遵守并将继续遵守所有适用的法律，包括与客户个人数据处理相关的数据保护法，以及其向科睿唯安发出的任何处理指示；及 (ii) 其已并将继续提供所有数据保护法规定的所有必要通知，并且已并将继续获得数据保护法规定的所有必要同意和权利，以便科睿唯安为协议所述的目的处理客户个人数据。客户应对客户个人数据的准确性、质量和合法性以及客户获取客户个人数据的方式全权负责。

(e) 客户指示的合法性。客户将确保：科睿唯安根据客户的指示处理客户个人数据不会导致科睿唯安违反任何适用法律、法规或规则，包括但不限于数据保护法。如果科睿唯安意识到或认为客户的任何数据处理指示违反了 GDPR 或 GDPR 任何在英国的实施细则，则除非适用的数据保护法禁止，否则科睿唯安应立即将此书面通知客户。

3. 子处理

(a) 经授权的子处理者。客户向科睿唯安提供一般书面授权，授权其代表客户聘用子处理者处理客户个人数据，从而提供服务。科睿唯安将在此处向客户提供相关子处理者名单，或者客户可以通过向 data.privacy@clarivate.com 发送书面请求来索取该名单。该名单包括我们的子处理者、其各自的组织的司法管辖区及其活动描述，以及替换或添加子处理者公告以及客户如何订阅接收此类替换和添加的事先通知的说明。订阅后，科睿唯安应通知客户有关添加或替换子处理者的任何预期变更，并且如果客户在发布此类通知后十 (10) 天内以合理的理由反对聘用新的子处理者，则科睿唯安将尽合理的努力对服务进行变更，或推荐商业上合理的变更，以避免由该子处理者进行处理。如果科睿唯安无法在合理期限内提供此类替代方法，客户只能通过在三十 (30) 天内向科睿唯安提供书面终止通知来终止受影响的服务，这些服务若不面向新子处理者使用则无法提供，任何一方均无需承担任何处罚或责任，且客户有权按比例获得被终止服务的预付费用的退款。

(b) 子处理者的义务。科睿唯安应：(i) 与每个子处理者签订书面协议，其中包含数据保护义务，为客户个人数据提供至少与本附录相同水平的保护；(ii) 对该子处理者履行在本附录项下的义务负责。

4. 安全

(a) 安全措施。科睿唯安应实施并维护适当的技术性和组织性安全措施，以保护客户个人数据，避免发生个人数据泄露，并根据附件 B 中所述的科睿唯安的安全标准保护客户个人数据的安全并为其保密（“技术和组织措施”）。

(b) 处理的保密性。科睿唯安应确保经其授权处理客户个人数据的个人负有适当的保密义务。

(c) 安全措施的更新。客户负责审查科睿唯安提供的与数据安全相关的信息，并独立确定服务是否符合客户的要求和数据保护法规定的法律义务。客户承认，安全措施受技术进步和发展的影响，并且科睿唯安可能不时地更新或修改安全措施，但前提是，此类更新和修改不会导致向客户提供的服务的整体安全性下降。

(d) 个人数据泄露响应。一旦发现个人数据泄露，科睿唯安应：(i) 立即通知客户，不得无故拖延，在可行的情况下，不得超过确定个人数据泄露确实发生后 48 小时；(ii) 在得知后或者应客户的合理要求，及时提供与个人数据泄露相关的信息；及 (iii) 立即采取合理措施遏制并调查任何个人数据泄露。客户同意，未遂个人数据泄露不受本第 4(d) 条的约束。未遂个人数据泄露是未导致客户个人数据或科睿唯安存储客户个人数据的任何设施或设备受到未经授权访问的个人数据泄露。科睿唯安根据本第 4(d) 条通知或响应个人数据泄露不得被解释为科睿唯安承认与个人数据泄露相关的任何过失或责任。

5. 审计

(a) 客户审计权。如果科睿唯安持有独立第三方出具的涵盖服务的“体系和服务机构控制”(SOC) 2 审计报告、“体系和服务部门控制”(SOC) 3 审计报告或 ISO 27001 认证，则客户同意行使客户可能拥有的任何权利，以根据本数据控制附录或标准合同条款（如适用）进行审计或检查，具体方法是以书面形式指示科睿唯安提供其最新的报告或认证的副本。该副本将被视为科睿唯安的保密信息。如果标准合同条款适用，则本条中的任何内容均不得修改或影响任何监管机构或数据主体在标准合同条款项下的权利。如果科睿唯安未能提供此类报告或认证，客户有权每年进行一次审计，除非发生个人数据泄露或涉及我们隐私和安全实践的官方投诉。

(b) 通知和范围。在客户至少提前 30 天发出书面通知的情况下，科睿唯安应向客户提供所有必要的信息，以证明符合本附录，并根据数据保护法的要求，允许并协助审计，包括客户为评估是否符合本附录而进行的检查。在开始任何审计之前，客户与科睿唯安应共同就审计的范围、时间和持续时间达成一致。对于科睿唯安或其第三方子处理者为此类审计所花费的任何时间，客户应对科睿唯安进行补偿。如果要求对我们的子处理者进行审计，客户确认此类审计可能受额外或不同的审计条款的约束。所有补偿费率均应合理，并计入科睿唯安或其第三方子处理者耗费的资源。审计和检查受科睿唯安合理的数据保护政策的约束，范围不得扩大至员工工资、人事记录，或者科睿唯安的场所、账簿、文件、记录的任何部分或其他与客户个人数据无关或具有商业敏感性或受法律特权保护的信息。在审计或检查过程中获得的信息以及此类审计或检查的结果将被视为科睿唯安的保密信息。

6. 国际传输

(a) 数据中心位置。在第 6(b) 条和 6(c) 条的约束下，除非另有书面约定，客户承认，科睿唯安可以将客户个人数据传输到美国并在美国进行处理，以及传输到科睿唯安、其关联公司或其分包商持续经营数据处理业务的世界其他地方并在该处进行处理。如下文所述，科睿唯安应确保建立机制，根据《数据保护法》和本附录有关此类传输的要求，提供适当的保护和实施个人数据保护。

(b) 澳大利亚的传输。如果科睿唯安是受澳大利亚隐私法保护的客户个人数据的接收方，双方承认并同意，科睿唯安可以在双方商定的条款允许的情况下将此类客户个人数据传输到澳大利亚境外，但科睿唯安必须遵守本附录和澳大利亚隐私法。

(c) 欧洲数据传输。如果科睿唯安是在欧洲以外的国家/地区接收受欧盟数据保护法保护的客户个人数据（“欧盟数据”）的接收方，而该国家/地区未被承认为对个人数据提供足够水平的保护（如适用欧盟数据保护法所述），双方同意遵守欧盟标准合同条款并根据欧盟标准合同条款，以附件 C 中规定的形式处理欧盟数据。就欧盟标准合同条款中的描述而言，科睿唯安同意，它是“数据输入者”，而客户是“数据输出者”（尽管客户本身可能也是位于欧洲以外的实体）。

(d) 英国数据传输。如果根据本附录进行英国客户个人数据的国际传输，则双方同意遵守英国附录并按照英国附录，以附件 D 规定的形式处理相关客户个人数据。就英国附录中的描述而言，科睿唯安同意，它是“数据输入者”，而客户是“数据输出者”（尽管客户本身可能也是位于英国以外的实体）。

(e) 替代传输机制。如果科睿唯安采用替代数据输出机制（包括标准合同条款的任何新版本或后继版本）来传输本附录中未述及的欧盟数据或英国数据（“替代传输机制”），则该替代传输机制应取代本附录中所述的传输机制（但仅限于该替代传输机制符合适用的数据保护法且范围扩大至向其传输相应数据的国家/地区的情况）。此外，如果有司法管辖权的法院或监管机构（无论出于何种原因）判令不能依赖本附录中描述的措施来合法传输欧盟数据或英国数据（定义见适用的欧盟数据保护法），则科睿唯安可以实施任何合理所需的额外措施或保障措施，以实现此类数据的合法传输。

7. 归还或删除数据

在服务终止或到期后，根据客户的书面请求以及在该终止或到期后 30 天内作出的选择，科睿唯安应（根据客户的选择）删除或向客户返还科睿唯安拥有或控制的所有客户个人数据（包括副本），但此类返还可能会按照科睿唯安当时的小时费率向客户收取额外费用。此类收费将在双方商定的单独报价和工作说明中概述。此要求不应适用于：(i) 适用法律要求科睿唯安保留部分或全部客户个人数据的情况；或 (ii) 科睿唯安已在备份系统上存档的客户个人数据，在根据科睿唯安的删除政策删除此类客户个人数据之前，科睿唯安应安全地隔离并保护此类数据，防止其被进一步处理。

8. 数据主体权利与合作

(a) 数据主体请求。作为服务的一部分，科睿唯安为客户提供了一些自助服务功能（客户可以利用此类功能检索、更正、删除或限制使用客户个人数据），客户可以利用此类功能协助其履行其在数据保护法下与通过其帐户回应数据主体的请求相关的义务，而无需支付额外费用。此外，在考虑处理性质的前提下，科睿唯安应尽可能向客户提供合理的协助，以便客户能够履行其在适用数据保护法下与数据主体权利相关的数据保护义务。如果任何此类请求是直接向科睿唯安提出的，则未经客户的事先授权，科睿唯安不得直接回应此类通信，除非回应是合理适当的（例如，在回应中指示数据主体联系客户；或者将数据主体引导至包含自助服务功能信息的公开链接；或者确认请求的性质以及请求与我们的哪些客户有关）或适用法律要求回应。如果要求科睿唯安回应此类请求，除非法律禁止，否则科睿唯安应立即通知客户，并向客户提供请求的副本。

(b) 数据保护影响评估。如果适用的数据保护法中要求，则科睿唯安应（在考虑处理的性质和科睿唯安可获得的信息的前提下）提供所有合理请求的关于服务的信息，以便客户能够根据数据保护法的要求进行数据保护影响评估或事先咨询数据保护部门。

9. 司法管辖区特定条款

如果科睿唯安处理的客户个人数据源自附件 E 中列出的其中一个司法管辖区并受该司法管辖区的数据保护法保护，则除本附录的条款之外，附件 E 中为该适用司法管辖区规定的条款（“司法管辖区特定条款”）也应适用。如果司法管辖区特定条款与本附录的任何其他条款之间存在任何冲突或歧义，则应以适用的司法管辖区特定条款为准，但仅限于司法管辖区特定条款可适用于科睿唯安的情况。

10. 与协议的关系

(a) 期限。本附录的有效期限应是科睿唯安代表客户开展客户个人数据处理业务的期限，或者持续到协议终止（并根据上文第 7 条归还或删除所有客户个人数据）为止。

(b) 优先顺序。双方同意，本附录应取代双方之前签订的与服务相关的任何现有数据处理协议或类似文件。如果本附录与协议的其余部分在客户个人数据的处理方面有任何冲突或不一致，应以以下文件的规定为准（按优先顺序）：(i) 标准合同条款；(ii) 本附录；然后是 (iii) 协议的其余部分（应按照协议中规定的优先顺序进行解释）。

(c) 变更的影响。除根据本附录进行的任何变更外，协议保持不变并保持完全的效力。

(d) 第三方权利。除本附录的一方、其继承人和许可受让人外，任何人均无权执行本附录的任何条款。

(e) 适用法律。除非适用的数据保护法另有要求，否则本附录应受协议中的适用法律和司法管辖权条款管辖并据此解释。

(f) 授权关联公司。双方确认并同意，客户通过签署协议，代表其自身并以其授权关联公司的名义和代表其授权关联公司（如适用）签署本附录,从而在科睿唯安和各授权关联公司之间建立单独的附录。各授权关联公司同意受本附录项下义务的约束。客户应负责协调与科睿唯安在本附录项下的所有沟通，并有权代表其授权关联公司进行与本附录相关的任何沟通。除非适用的数据保护法律要求授权关联公司直接针对科睿唯安行使本附录规定的权利或寻求任何救济，否则客户及各授权关联公司同意：(i) 作为协议缔约方的客户应代表授权关联公司行使任何此类权利或寻求任何此类救济，(ii) 作为协议缔约方的客户应以合并方式代表其自身及其所有授权关联公司行使本附录项下的任何此等权利或寻求任何此等救济，且 (iii) 提及一方的责任时，是指该方及其所有关联公司在协议和本附录项下的总责任。为免生疑问，授权关联公司不是协议的一方，也不会成为协议的一方。

附件 A - 数据处理详细说明

数据控制者：
客户和/或根据本附录的条款有资格成为控制者的任何授权关联公司。

数据处理者：
根据本附录的条款处理客户个人数据的科睿唯安实体和/或其关联公司。

主题：
本附录项下数据处理的主题是客户个人数据。

处理持续时间：
科睿唯安将根据本附录第 7 条和第 10(a) 条中的规定处理客户个人数据。

处理的目的和性质：
处理客户个人数据的目的和性质应包括：(i) 根据协议提供服务所需的处理；(ii) 履行科睿唯安在协议和本附录项下的合同义务；(iii) 遵守由数据控制者提供（例如通过电子邮件或支持工单提供）的符合协议条款的任何其他合理的指示；及 (iv) 下表此类适用“服务”中列明的目的和性质。

数据主体的类别：
控制者可以为服务提交客户个人数据，提交的范围由控制者自行决定和控制，可能包括但不限于与下表“服务”中列明的数据主体的类别相关的客户个人数据。

个人数据的类别：
控制者可以向服务提交符合提供服务的目的的客户个人数据，其范围由数据控制者自行决定并控制，但受本附录或协议规定的任何限制的约束，可能包括但不限于服务规定的以下个人数据类别和提供的产品文档中规定的个人数据类别。

服务	目的和性质	数据主体的类别	个人数据的类别
Converis	托管、实施和/或技术支持	• 控制者的员工、代理人、顾问和承包商 • 控制者授权使用服务的个人 • 学术界成员，如同行评审人员、参与期刊的编辑 • 控制者确定的其他数据主体	• 姓名和其他非敏感标识符，如员工识别号、研究人员识别号、用户名 • 人口统计信息 • 业务联系信息 • 专业信息 • 协议允许添加到服务中、通过服务而生成或以其他方式存储在服务中的其他个人数据类别

发现、研究和图书馆工作流解决方案：
360 Core
360 LINK
360 MARC Updates
360 Resource Manager
360 Search
Intota™
Assessment
	托管、实施和/或技术支持	• 图书馆顾客、图书馆工作人员、教师、学生、管理人员、员工、访客和校友	• 基本用户和顾客信息，包括
			  ▪ 名字和姓氏
			  ▪ 邮政地址
			  ▪ 电子邮件地址
			  ▪ 电话号码和其他联系信息
			  ▪ 机构识别号码
			  ▪ 部门和职务
			• 基本员工和员工联系信息
			• 员工相关使用信息，包括员工操作和活动记录
			• 研究活动

Pivot/Pivot-RP **RefWorks** **Summon** **Ulrichsweb** **Ulrich'sTM Serials Analysis System** **IntotaTM**			• 一般使用信息，包括连接数据（例如 IP 地址） • 供应商/供货商信息
First to File	用户帐户预注册；托管；实施和/或技术支持；以及专业服务（视情况而定）	• 控制者的员工、代理人、顾问、自由职业者（自然人） • 控制者授权使用服务的个人 • 控制者的潜在客户、客户、业务合作伙伴和供应商（自然人） • 控制者的潜在客户、客户、业务合作伙伴和供应商的员工或联系人 • 控制者确定的其他数据主体，包括发明人、专利申请人和受让人、商标所有人、律师	• 姓名和其他非敏感标识符，例如签名 • 业务联系信息 • 人口统计信息 • 专业信息 • 协议允许添加到服务中、通过服务而生成或以其他方式存储在服务中的其他个人数据类别
集成图书馆系统： **Millennium** **Polaris** **Sierra** **Vega** **Virtua** **和相关模块**	托管（除非由控制者或授权第三方托管提供商（如 Salesforce）托管）、实施和/或技术支持	• 控制者的员工、代理人、顾问、自由职业者（自然人） • 控制者授权使用服务的个人，包括图书馆顾客	• 图书馆顾客数据，如图书证号码或其他识别号码，其中可能包括数据主体图书证的照片、年龄或出生日期、联系信息、居住证明，可能包括政府签发的身份证或数据主体提供给客户的其他文件的副本 • 有关服务使用的信息；对于图书馆顾客而言，这可能包括使用图书馆资源等（包括访问的地点或分支机构、材料请求、保留、借出或访问历史） • 与图书馆工作人员互动 • 使用其他图书馆服务；为方便任何付款而提供的信息；以及任何滞纳金或罚款 • 姓名和其他非敏感标识符，如员工识别号和用户名 • 业务联系信息 • 人口统计信息 • 专业信息 • 协议允许添加到服务中、通过服务而生成或以其他方式存储在服务中的其他个人数据类别
知识产权管理系统： **FoundationIP** **IPfolio** **Ipendo** **Inprotech** **Memotech** **Patrawin** **知识产权管理系统** **Unycom**	托管（除非由控制者或授权的第三方托管提供商（如 Salesforce）托管）、实施和/或技术支持	• 控制者的员工、代理人、顾问、自由职业者（自然人） • 控制者授权使用服务的个人 • 控制者的潜在客户、客户、业务合作伙伴和供应商（自然人） • 控制者的潜在客户、客户、业务合作伙伴和供应商的员工或联系人 • 控制者确定的其他数据主体，包括发明人、专利申请人和受让人、商标所有人、律师	• 姓名和其他非敏感标识符，如员工识别号和用户名 • 业务联系信息 • 人口统计信息 • 专业信息 • 协议允许添加到服务中、通过服务而生成或以其他方式存储在服务中的其他个人数据类别
知识产权专业服务	提供与知识产权相关的专业服务，包括但不限于续费、备案和申请服务	• 控制者的员工、代理人、顾问、自由职业者（自然人） • 控制者授权使用服务的个人 • 控制者的潜在客户、客户、业务合作伙伴和供应商（自然人） • 控制者的潜在客户、客户、业务合作伙伴和供应商的员工或联系人	• 姓名和其他非敏感标识符，如员工识别号和用户名 • 业务联系信息 • 人口统计信息 • 专业信息 • 协议允许添加到服务中、通过服务而生成或以其他方式存储在服务中的其他个人数据类别

		• 控制者确定的其他数据主体，包括发明人、专利申请人和受让人、商标所有人、律师	
市场研究 - 合同要求的作为市场研究活动一部分的安全和质量报告	向客户或市场授权持有人报告协议中所述的安全和质量事件	市场研究参与者	• 姓名 • 人口统计信息 • 专业信息 • 联系信息 • 处理酬金所需的信息
市场研究 - 为初级市场研究项目进行的基于名单的招聘	处理客户提供的名单，以招聘特定人员进行初级市场研究	可能的市场研究参与者	• 姓名 • 人口统计信息 • 联系信息 • 专业信息 • 处理酬金所需的信息
我的组织 (My Organization)（InCites 对标和分析模块）	使客户能够将其研究人员的数据库上传到科睿唯安的 InCites 的 My Organization 模块中并分析和管理数据库。	• 控制者的员工、代理人、顾问和承包商（自然人） • 控制者授权使用服务的个人 • 控制者确定的其他数据主体	• 姓名和其他非敏感标识符，如员工识别号、研究人员识别号、用户名 • 人口统计信息 • 业务联系信息 • 专业信息 • 协议允许添加到服务中、通过服务而生成或以其他方式存储在服务中的其他个人数据类别

基于云的图书馆管理、发现、研究、阅读清单和移动/网络应用程序（Ex Libris SaaS 服务）：
Alma
Esploro
CampusM
Leganto
Primo SaaS/Primo VE
Rapido
	托管、实施技术支持和/或其他相关服务	图书馆顾客、图书馆工作人员、教师、学生、管理人员、员工、研究人员、访客和校友	• 基本用户和顾客信息，包括
			  ○ 名字和姓氏
			  ○ 邮政地址
			  ○ 电子邮件地址
			  ○ 电话号码和其他联系信息
			  ○ 机构识别号码
			• 图书馆/目录相关的用户和顾客信息，包括
			  ○ 图书馆活动、借款和罚款信息
			• 基本员工信息，包括联系信息
			• 员工相关使用信息，包括员工操作和活动记录
			• 研究活动
			• 一般使用信息，包括连接数据（例如 IP 地址）
			• 供应商/供货商信息
			• 移动平台信息（如适用）
			  ○ 设备信息（例如，标识符和平台）
			  ○ 出席和位置数据（如适用）

本地安装 Ex Libris 软件的软件支持和维护服务，包括： **Aleph Local** **Primo Local** **Rosetta Local** **Voyager Local** **SFX**	通过远程访问所列产品的本地安装版本，实现支持和维护	客户选择并存储在其本地安装系统上的数据主体类别，科睿唯安可能有权临时访问	• 客户在运行程序的本地系统上存储的个人数据类型，科睿唯安有权访问这些个人数据，以便提供软件维护和支持服务，和/或客户在提供软件维护和支持服务的过程中向科睿唯安提供的个人数据类型。 • 处理非常有限，主要涉及在主动和临时远程访问系统以解决支持服务呼叫期间对个人数据的偶然访问

Web of Science Reviewer Recognition **Web of Science Author Connect** **Web of Science Reviewer Locator**	仅用于处理（由客户提供的）将被邀请注册适用服务的个人的名单	学术界成员，例如研究人员和同行评审人员	• 姓名和其他非敏感标识符，例如研究人员识别号 • 人口统计信息 • 业务联系信息 • 专业信息 • 与数据主体的同行评审活动相关的其他信息
ScholarOne	托管、技术支持和相关服务	• 控制者的员工、代理人、顾问和承包商（自然人） • 学术界成员，例如出版物作者和同行评审人员 • 控制者确定的其他数据主体	• 姓名和其他非敏感标识符，如员工识别号、研究人员识别号、用户名 • 人口统计信息 • 业务联系信息 • 专业信息 • 协议允许添加到服务中、通过服务而生成或以其他方式存储在服务中的其他个人数据类别

特殊类别的个人数据（定义见 GDPR）或敏感数据：

科睿唯安不想也不会有意收集或处理与提供服务相关的任何特殊类别的个人数据，但由于合同要求的（作为市场研究活动的一部分的）可报告的安全和/或质量事件而处理的健康相关详细信息除外。

处理操作：

客户个人数据将根据协议（包括本附录以及任何工作说明书或订单）进行处理，并在必要时提供、维护和改进根据协议应向客户提供和/或适用法律强制要求向客户提供的服务，并可能接受以下处理操作：

任何操作或一组操作，无论是否通过自动化方式，例如收集、记录、组织、结构化、存储、调整或更改、检索、咨询、使用、传输、传播或以其他方式披露、统一或组合、限制、擦除或销毁。

个人数据传输频率：

将在开始之时以及整个期限内在必要时传输客户个人数据。

保留期限：

数据将在期限内保留，如附录第 **7** 节所述。

以上描述也适用于科睿唯安向子处理者的传输。

附件 B - 技术和组织措施

本附件中描述了适用于服务的技术和组织措施（根据本附录第 4(c) 条不时更新）。

信息安全计划

科睿唯安有一个明确的信息安全计划，涵盖符合公认的信息安全行业标准的技术和组织措施的相关方面，以保护信息资产的机密性、完整性和可用性

人员

我们所有的工作人员均须遵守涵盖公司价值观和使命的行为守则。他们了解自己的责任、我们的政策和标准，并从我们的信息安全团队获得定期指导和支持。

根据相关法律法规，在招聘永久编制人员时，会进行充分的背景核实检查，以减少对关键信息资产的潜在威胁。

我们持续进行强制性信息安全培训，并根据需要向特定目标群体和个人提供补充培训。我们的员工受到保密义务的约束，并了解未能遵守我们政策的后果以及他们的责任。

科睿唯安遵循员工退出流程，该流程涉及系统权限/访问权限的撤销以及公司资产的及时归还。

个人数据加密

包括加密在内的措施用于确保在电子传输或传输过程中未经授权无法读取、复制、修改或删除个人数据，且能够验证通过数据传输设施传输个人数据的目标实体。

用户访问管理

科睿唯安有一个清晰明确的流程来授予对信息资产的访问权限。我们已经制定了措施，防止未经授权的人员使用数据处理设备，包括访问管理、日志记录和密码保护。

授予数据处理设备用户权限，以根据他们的角色和责任限制访问此类个人数据，从而防止未经授权的访问和披露。科睿唯安在全公司上下对所有信息资产有明确的密码政策，以尽量缩短密码长度并确保密码的复杂性、密码过期机制、密码有历史记录以及多次尝试失败后的帐户锁定要求。

基础设施安全

我们的服务通过公共和私人网络提供。通信受到安全通道和加密的保护，防止窃听。科睿唯安已通过入侵预防系统(IPS)、防火墙和/或 AWS 安全团队保护边界安全，以便管理和限制网络访问，并在我们的数据中心采用 VLANS。

还实施了分层控制措施（包括使用网络分段）来确保系统和数据得到适当的保护。

恶意软件保护

根据我们的政策，托管在我们的数据中心或部署在云端的科睿唯安拥有和支持的操作系统均采用新一代防病毒解决方案进行保护。

补丁管理

我们从内部漏洞管理工具、供应商和其他第三方安全组织处收集并审查安全威胁情报。我们的补丁管理标准为我们的技术团队规定了适当的打补丁规程。我们的安全补丁首先要评估和定义补丁的严重性。优先级认证和全面 QA 测试用于验证系统在应用补丁后的稳定性和可用性。有时，可能会实施额外的安全控制措施来减轻已知的威胁。

安全监控

科睿唯安拥有专门的网络与安全运营中心(NOC/SOC)，对客户数据逻辑网络访问和信息资产使用提供 24×7 记录和监控。安全日志发送到我们的安全操作中心，以便实时了解情况、事件相关性和事件响应。还会记录数据输入，以确保能够检查和确定个人数据是否已输入、更改或从个人数据处理系统中删除，如果是，由谁输入、更改或移除。

安全和隐私事件响应

我们实施了事件响应流程，以在识别出事件时对其进行处理。事件由专门的事故响应团队按照书面的减轻和沟通程序进行管理。

科睿唯安的事件响应流程要求有效地报告、调查和监控事件，以确保及时采取纠正措施来控制和纠正安全事件。

运营安全

对业务信息系统环境所进行的变更（包括对服务器、网络设备和软件进行的变更）均经过正式的变更管理流程。

始终保留信息和软件的备份副本，以便在发生系统崩溃或信息意外删除等事件时进行数据恢复。

容量管理和监控

我们对系统、服务和运营进行监控，以保持我们运营环境的健康。实施管理工具是为了监控和维护一个规模适当的环境。

漏洞扫描

科睿唯安实施了多层安全漏洞管理计划，包括安全检查、自动或手动安全审查、应用和基础设施漏洞评估扫描。制定了评估、验证、优先排序和补救已识别问题的措施。

作为我们侧重漏洞管理的计划中的一项惯例，我们会定期对我们全球网络中面向互联网的网站进行扫描。

风险管理

我们的产品和技术团队定期聘请信息安全主题专家来提供风险评估服务。在风险评估活动期间会开展多项服务，其中包括：服务架构审查、漏洞扫描、应用程序安全测试和技术合规性审查等。

在风险评估活动之后，我们的信息安全风险管理团队会咨询产品和技术团队，以制定针对解决合规性方面差距或已识别风险领域的纠正计划和路线图。

此外，我们的信息技术治理、风险和合规团队根据政策、标准和法规要求来进行审计，并对调查结果进行备案，以供业务部门在内部进行审查并实施纠正措施。

物理安全和第三方供应商管理

在所有的战略数据中心（包括托管科睿唯安产品的云服务提供商）中，均根据科睿唯安已采用的物理安全行业标准进行部署和管理。我们的准则包括对物理安全、建筑维护、灭火、空调、配有备用发电机的不间断电源的要求以及不同电源和通信设备的进出要求。作为我们供应商风险管理计划的一部分，科睿唯安对第三方数据中心保证报告进行审查。

我们采用各种安全方法来控制我们设施的进出，确保只能根据运营需求以受控方式获得进出权限。这些方法可能包括以下部分或全部：在服务时间之外使用报警装置或保安服务、将场所划分为不同的安全区域、雇用保安人员、身份证、包含感应卡读卡器的电子门禁、实体门锁和个人识别号码，具体取决于设施的敏感性。

附件 C - 欧盟标准合同条款（处理者）

控制者到处理者

第一部分：

第 1 条

目的和范围

(a) 本标准合同条款旨在确保遵守 2016 年 4 月 27 日欧洲议会和欧洲委员会针对将数据传输到第三国的关于保护自然人个人数据处理及个人数据自由流动的条例 (EU) 2016/679（《通用数据保护条例》）的要求。

(b) 双方：

(i) 传输个人数据的自然人或法人、公共机关、机构或其他团体（下称“实体”），如附录 I.A 所列（下称“数据输出者”），和

(ii) 位于第三国的实体，其通过另一个实体（也是本条款的当事方）直接或间接地从数据输出者处接收个人数据，如附录 I.A 所列（下称“数据输入者”）

已同意本标准合同条款（下称“条款”）。

(c) 本条款适用于附录 I.B 中规定的个人数据传输。

(d) 本条款的附件包含其中提及的附录，构成本条款的组成部分。

第 2 条

条款的效力和不变性

(a) 本条款规定了适当的保障措施，包括条例 (EU) 2016/679 第 46(1)条和第 46(2)(c) 款规定的强制性数据主体权利和有效的法律救济，以及条例 (EU) 2016/679 第 28(7)条关于从控制者到处理者和/或从处理者到处理者的数据传输的标准合同条款，前提是它们未被修改，选择相应模块或添加或更新附件中的信息除外。这并不妨碍双方在更广泛的合同中纳入本条款中规定的标准合同条款和/或增加其他条款或附加保障措施，前提是它们不会直接或间接地与本条款相抵触或损害数据主体的基本权利或自由。

(b) 本条款不影响数据输出者根据条例 (EU) 2016/679 应履行的义务。

第 3 条

第三方受益人

(a) 数据主体可作为第三方受益人，针对数据输出者和/或数据输入者援引和执行本条款，但以下条款除外：

(i) 第 1 条、第 2 条、第 3 条、第 6 条、第 7 条；

(ii) 第 8 条 - 第 8.1(b)、8.9(a)、(c)、(d) 和 (e) 条；

(iii) 第 9 条 - 第 9(a)、(c)、(d) 和 (e) 条；

(iv) 第 12 条 - 第 12(a)、(d) 和 (f) 条；

(v) 第 13 条；

(vi) 第 15.1(c)、(d) 和 (e) 条；

(vii) 第 16(e) 条；

(viii) 第 18 条 - 第 18(a) 和 (b) 条。

(b) 第 (a) 款不影响条例 (EU) 2016/679 规定的数据主体的权利。

第 4 条

解释

(a) 如果本条款使用条例 (EU) 2016/679 中定义的术语，则这些术语应具有该条例中赋予的含义。

(b) 应根据条例 (EU) 2016/679 的规定阅读和解释本条款。

(c) 本条款的解释不得与条例 (EU) 2016/679 中规定的权利和义务相冲突。

第 5 条

优先顺序

如果本条款与双方之间在本条款订立之时既有的或在本条款订立之后签订的相关协议的规定之间存在矛盾，应以本条款为准。

第 6 条

传输说明

传输的详情，尤其是传输的个人数据的类别及其传输的目的，在附录 I.B 中规定。

第 7 条 – 可选

[故意省略。]

第二部分 – 双方的义务

第 8 条

数据保护保障措施

数据输出者保证，其已尽合理努力确定，通过实施适当的技术和组织措施，数据输入者能够履行其在本条款下的义务。

8.1 指示

(a) 数据输入者应仅按照数据输出者的书面指示处理个人数据。数据输出者可在合同存续期间提供此类指示。

(b) 数据输入者如果无法遵守这些指示，则应立即通知数据输出者。

8.2 目的限制

除非数据输出者另有指示，否则数据输入者应仅出于附录 I.B 中规定的特定传输目的处理个人数据。

8.3 透明度

根据要求，数据输出者应免费向数据主体提供本条款的副本，包括双方填写的附件。在保护商业秘密或其他保密信息（包括附录 II 中描述的措施和个人数据）的必要范围内，数据输出者在分享副本之前可遮盖本条款附件的部分文本，但如果因此导致数据主体无法理解其内容或无法行使其权利，应提供有意义的摘要。根据要求，双方应尽可能地向数据主体提供遮盖的原因，而不泄露遮盖的信息。本条款不妨碍数据输出者根据条例 (EU) 2016/679 第 13 和 14 条承担的义务。

8.4 准确性

如果数据输入者发现其收到的个人数据不准确或已过时，应通知数据输出者，不得无故拖延。在这种情况下，数据输入者应配合数据输出者删除或更正数据。

8.5 数据处理的期限以及数据的删除或返还

数据输入者只能在附录 I.B 规定的期限内处理数据。在停止提供处理服务后，数据输入者应根据数据输出者的选择删除代表数据输出者处理的所有个人数据，并向数据输出者证明其已这样做，或将代表数据输出者处理的所有个人数据返还给数据输出者，并删除现有副本。在删除或返还数据之前，数据输入者应继续确保遵守本条款。数据输入者保证，如果适用于数据输入者的当地法律禁止返还或删除个人数据，则其将继续确保遵守本条款，并且仅在当地法律要求的

范围和时间内进行处理。这一规定不影响第 14 条，尤其是第 14(e) 条的以下要求：在合同存续期间，如果数据输入者有理由认为其受不符合第 14(a) 条要求的法律或惯例约束，则应通知数据输出者。

8.6 处理的安全性

(a) 数据输入者应实施适当的技术和组织措施，以确保数据安全，包括保护数据免遭安全破坏，从而导致意外或非法销毁、丢失、更改、未经授权披露或访问数据（下称“个人数据泄露”）；在传输期间，数据输出者也应遵守这一要求。在评估适当的安全等级时，双方应适当考虑现有技术状况、实施成本、处理的性质、范围、背景和目的，以及处理期间数据主体所涉及的风险。如果可以实现处理的目的，双方应特别考虑采取加密或假名化措施，包括在传输期间。在假名化的情况下，将个人数据归属于特定数据主体的附加信息应尽可能由数据输出者独占控制。为遵守本款规定的义务，数据输入者应至少实施附录 II 中规定的技术和组织措施。数据输入者应定期进行检查，以确保这些措施继续提供适当的安全等级。

(b) 数据输入者仅应在出于执行、管理和监督合同目的严格必要的范围内向其人员授予访问个人数据的权限。其应确保经授权处理个人数据的人员已承诺保密或承担适当的法定保密义务。

(c) 如果数据输入者在根据本条款处理个人数据时发生了个人数据泄露，则数据输入者应采取适当措施来处理该泄露，包括采取措施减轻其不利影响。数据输入者还应在获悉泄露后立即通知数据输出者，不得无故拖延。此类通知应包含可提供更多信息的联系人的详情、对泄露性质的描述（尽可能包括数据主体和个人数据相关记录的类别和大致数量）、其可能的后果以及为处理泄露而采取或拟议采取的措施，包括酌情采取措施以缓解其可能的不利影响。如果无法同时提供所有信息，初始通知应包含当时可提供的信息，并且随后一旦获得进一步的信息，应立即提供。

(d) 数据输入者应配合并协助数据输出者，使数据输出者能够遵守其根据条例 (EU) 2016/679 承担的义务，尤其是根据处理的性质和数据输入者可获得的信息通知主管监管机构和受影响数据主体。

8.7 敏感数据

如果传输涉及披露种族或民族本源、政治观点、宗教或哲学信仰、工会会员身份、遗传数据、唯一识别自然人的生物特征数据、健康数据或个人性生活或性取向数据、刑事定罪和犯罪相关数据的个人数据（下称“敏感数据”），数据输入者应采用附录 I.B 中所述的特定限制和/或额外保障措施。

8.8 后续传输

数据输入者应仅根据数据输出者的书面指示向第三方披露个人数据。此外，接受数据披露的位于欧盟以外的第三方（与数据输入者在同一个国家/地区或在另一个第三国家/地区，下称“后续转移”）必须根据适当的模块受本条款的约束或同意受本条款的约束，或满足以下条件：

(i) 接受后续传输的国家/地区应根据条例 (EU) 2016/679 第 45 条获得充分性认定（涵盖相应的后续传输）；

(ii) 第三方通过其他方式就相关处理确保条例 (EU) 2016/679 第 46 或 47 条规定的适当保障措施；

(iii) 后续传输对于在特定行政、监管或司法程序中确立、行使或辩护法律索赔是必要的；或

(iv) 后续传输对于保护数据主体或其他自然人的切身利益是必要的。

任何后续传输都要求数据输入者遵守本条款下的所有其他保障措施，尤其是目的限制。

8.9 文档和合规性

(a) 数据输入者应及时、充分地处理数据输出者提出的与根据本条款进行的处理相关的问询。

(b) 双方应能够证明遵守本条款。特别是，数据输入者应保留有关代表数据输出者执行的处理活动的适当文档。

(c) 数据输入者应按合理的时间间隔或在有迹象表明存在不合规情况时，向数据输出者提供所有必要信息，以证明遵守本条款中规定的义务，并按数据输出者的要求，允许并协助审计本条款涵盖的处理活动。在就审核或审计做出决定时，数据输出者可以考虑数据输入者持有的相关认证。

(d) 数据输出者可选择自行执行审计或委托独立审计员进行审计。审计可包括对数据输入者的场所或物理设施进行检查，并且在适当情况下，应在发出合理通知后进行。

(e) 双方应根据要求向主管监管机构提供第 (b) 和 (c) 款中提及的信息，包括任何审计的结果。

第 9 条

子处理者的聘用

(a) 一般书面授权 数据输入者拥有数据输出者的一般授权，可以从商定名单中聘用子处理者。数据输入者应在商业上合理的情况下，至少提前 15 天书面通知数据输出者该名单的任何预期变更（添加或替换子处理者），但在任何情况下均应至少提前 5 天，从而为数据输出者留出足够的时间在子处理者聘用之前反对此类变更。数据输入者应向数据输出者提供必要的信息，以便数据输出者行使其反对权。

(b) 数据输入者聘请子处理者（代表数据输出者）执行特定处理活动时，应采用书面合同，其中规定本质上与本条款针对数据输入者规定的相同数据保护义务，包括数据主体的第三方受益人权利。双方同意，数据输入者通过遵守本条款履行其在第 8.8 条下的义务。数据输入者应确保子处理者遵守本条款规定的数据输入者所承担的义务。

(c) 数据输入者应根据数据输出者的要求，向数据输出者提供一份此类子处理者协议的副本和任何后续修订。在保护商业秘密或其他保密信息（包括个人数据）的必要范围内，数据输入者在分享副本之前可遮盖该协议的文本。

(d) 数据输入者仍应就子处理者履行其与数据输入者签订的合同规定的义务而对数据输出者承担全部责任。数据输入者应将子处理者未能履行其在该合同下义务的情况通知数据输出者。

(e) 数据输入者应与子处理者商定第三方受益人条款，根据该条款，在数据输入者事实上消失、在法律上不再存在或无力偿债的情况下，数据输出者有权终止子处理者合同并指示子处理者删除或返还个人数据。

第 10 条

数据主体权利

(a) 数据输入者应将从数据主体处收到的任何请求及时通知数据输出者。除非经数据输出者授权，否则其不得自行回应该请求。

(b) 数据输入者应协助数据输出者履行其义务，回应数据主体关于行使条例 (EU) 2016/679 规定的权利的请求。在这方面，双方应根据处理的性质、提供援助的方式以及所需援助的范围和程度在附录 II 中规定适当的技术和组织措施。

(c) 在履行第 (a) 和 (b) 款规定的义务时，数据输入者应遵守数据输出者的指示。

第 11 条

纠正

(a) 数据输入者应通过个人通知或其网站以透明和易于访问的格式向数据主体告知经授权处理投诉的联系人。该联系人应及时处理从数据主体处收到的任何投诉。

(b) 如果数据主体与其中一方就遵守本条款发生争议，该方应尽最大努力及时友好地解决问题。双方应随时将此类争议告知对方，并在适当情况下配合解决。

(c) 如果数据主体根据第 3 条援引第三方受益人权利，则数据输入者应接受数据主体的以下决定：

(i) 向其惯常居住地或工作地点的成员国的监管机构或第 13 条规定的主管监管机构提出投诉；

(ii) 将争议提交给第 18 条含义范围内的主管法院。

(d) 双方同意，根据条例 (EU) 2016/679 第 80(1) 条中规定的条件，数据主体可由非营利机构、组织或协会代表。

(e) 数据输入者应遵守根据适用的欧盟或成员国法律具有约束力的决定。

(f) 数据输入者同意，数据主体所做的选择不会损害其根据适用法律寻求救济的实质性和程序性权利。

第 12 条

责任

(a) 各方应就因违反本条款而给另一方造成的任何损害向另一方负责。

(b) 数据输入者应就数据输入者或其子处理者因违反本条款下的第三方受益人权利而对数据主体造成的任何重大或非重大损害对数据主体负责，数据主体有权就此获得赔偿。

(c) 尽管有第 (b) 款的规定，数据输出者应就数据输出者或数据输入者（或其子处理者）因违反本条款下的第三方受益人权利而对数据主体造成的任何重大或非重大损害对数据主体负责，数据主体应有权就此获得赔偿。这一规定不妨碍数据输出者的责任，并且如果数据输出者是代表控制者行事的处理者，也不妨碍条例 (EU) 2016/679 或条例 (EU) 2018/1725（如适用）规定的控制者责任。

(d) 双方同意，如果数据输出者根据第 (c) 款对数据输入者（或其子处理者）造成的损害承担责任，则其有权向数据输入者索赔与数据输入者对损害的责任相对应部分的赔偿。

(e) 如果有多方对因违反本条款而给数据主体造成的任何损害负责，则所有责任方均应承担连带责任，且数据主体有权向法院起诉任何一方。

(f) 双方同意，如果一方根据第 (e) 款应承担责任，则其有权向另一方/其他方索赔与该另一方/其他方对损害的责任相对应部分的赔偿。

(g) 数据输入者不得援引子处理者的行为来逃避自己的责任。

第 13 条

监管

(a) 如果数据输出者是在欧盟成员国成立的，则负责确保数据输出者遵守数据传输条例 (EU) 2016/679 的监管机构（如附录 I.C 所示）应担任主管监管机构。

如果数据输出者不是在欧盟成员国成立的，但根据条例 (EU) 2016/679 第 3(2) 条属于其适用地域范围，并且已根据条例 (EU) 2016/679 第 27(1) 条任命了一名代表，则根据 (EU) 2016/679 第 27(1) 条设立该代表的成员国的监管机构（如附录 I.C 所示）应担任主管监管机构。

如果数据输出者不是在欧盟成员国成立的，但根据条例 (EU) 2016/679 第 3(2) 条属于其适用地域范围，但根据条例 (EU) 2016/679 第 27(2) 条无需任命代表，则根据本条款传输其个人数据（以便向其提供商品或服务）或其行为被监控的数据主体所在的成员国的监管机构（如附录 I.C 所示）应担任主管监管机构。

(b) 数据输入者同意接受主管监管机构的管辖，并在旨在确保遵守本条款的任何程序中与主管监管机构合作。尤其是，数据输入者同意回复问询、接受审计并遵守监管机构采取的措施，包括救济和赔偿措施。数据输入者应向监管机构提供已采取必要行动的书面确认。

第三部分 – 当地法律和公共机关访问时的义务

第 14 条

影响遵守本条款的当地法律和惯例

(a) 双方保证，他们没有理由认为适用于数据输入者处理个人数据的第三目的地国家/地区的法律和惯例，包括披露个人数据的任何要求或授权公共机关访问的措施，会阻止数据输入者履行其在本条款下的义务。这是基于以下理解：尊重基本权利和自由的本质并且在民主社会中维护条例 (EU) 2016/679 第 23(1) 条所列目标之一所必需和相称的法律和惯例与本条款并不矛盾。

(b) 双方声明，在提供第 (a) 款中的保证时，他们已适当考虑以下要素：

(i) 传输的具体情况，包括处理链的长度、所涉及的行为者数量和使用的传输渠道、预期的后续传输、接收方的类型、处理的目的、所传输个人数据的类别和格式、传输数据的经济部门、传输数据的存储位置；

(ii) 目的地第三国家/地区根据传输的具体情况适用的法律和惯例（包括要求向公共机关披露数据或授权公共机关访问的法律和惯例），以及适用的限制和保障措施；

(iii) 为补充本条款规定的保障措施而实施的任何相关合同、技术或组织保障措施，包括在目的地国家/地区传输和处理个人数据期间采取的措施。

(c) 数据输入者保证，在根据第 (b) 款进行评估时，其已尽最大努力向数据输出者提供相关信息，并同意其将继续与数据输出者合作，以确保遵守本条款。

(d) 各方同意记录第 (b) 款下的评估，并根据要求提供给主管监管机构。

(e) 数据输入者同意，在其同意本条款后，在合同存续期间，如有理由认为其受不符合第 (a) 款要求的法律或惯例约束，包括在第三国家/地区的法律或措施（如披露请求）发生变更而表明在实践中采用了此类不符合第 (a) 款要求的法律时，应立即通知数据输出者。

(f) 在根据第 (e) 款发出通知后，或者如果数据输出者有理由认为数据输入者无法再履行其在本条款下的义务，数据输出者应及时确定数据输出者和/或数据输入者应采取的适当措施（例如确保安全和保密的技术或组织措施）以解决这种情况。如果数据输出者认为无法确保对此类传输采取适当的保障措施，或主管监管机构指示暂停数据传输，则数据输出者应暂停数据传输。在这种情况下，数据输出者有权终止与本条款下的个人数据处理相关的合同。如果合同涉及两个以上的当事方，数据输出者只能对相关的当事方行使终止权，除非双方另有约定。如果根据本条款终止合同，则第 16(d) 和 (e) 条应适用。

第 15 条

数据输入者在公共机关访问时的义务

15.1 通知

(a) 数据输入者同意在下列情况下立即通知数据输出者，并尽可能立即通知数据主体（必要时在数据输出者的帮助下）：

(i) 收到公共机关（包括司法机关）根据目的地国家/地区的法律发出的具有法律约束力的请求，要求披露根据本条款传输的个人数据；该通知应包括有关请求的个人数据、发出请求的机关、请求的法律依据和提供的回复的信息；或

(ii) 获悉公共机关根据目的地国家/地区的法律直接访问根据本条款传输的个人数据；此类通知应包括输入者可获得的所有信息。

(b) 数据输入者同意，如果数据输入者根据目的地国家/地区的法律被禁止通知数据输出者和/或数据主体，则数据输入者会尽最大努力获得禁令豁免，以期尽快传达尽可能多的信息。数据输入者同意记录其所做出的最大努力，以便能够根据数据输出者的要求证明这些努力。

(c) 数据输入者同意，在目的地国家/地区法律允许的情况下，在合同存续期间定期向数据输出者提供有关所收到的请求的尽可能多的相关信息（尤其是请求的数量、所请求数据的类型、发出请求的机关、是否对请求提出质疑以及此类质疑的结果等）。

(d) 数据输入者同意在合同存续期间根据第 (a) 至 (c) 款保存信息，并根据要求提供给主管监管机构。

(e) 第 (a) 至 (c) 款不影响数据输入者根据第 14 (e) 条和第 16 条在无法遵守本条款时立即通知数据输出者的义务。

15.2 合法性审查和数据最小化

(a) 数据输入者同意审查披露请求的合法性，尤其是披露请求是否仍在授予请求的公共机关的权力范围内，并在经过仔细评估后得出根据目的地国家/地区法律、国际法规定的适用义务和国际礼让原则有合理理由认为请求不合法的结论时，对请求提出质疑。数据输入者应在相同条件下寻求上诉的可能性。在对请求提出质疑时，数据输入者应寻求临时措施，以期暂停请求的影响，直至主管司法机关就其案情作出决定。在适用程序规则要求之前，不得披露所请求的个人数据。这些要求不影响第 14 (e) 条下的数据输入者义务。

(b) 数据输入者同意记录其法律评估和对披露请求的任何质疑，并在目的地国家/地区法律允许的范围内，向数据输出者提供此类文档。数据输入者还应根据要求向主管监管机构提供此类文档。

(c) 数据输入者同意根据对披露请求的合理解释，在回应披露请求时提供允许的最少量信息。

第四部分 – 最终条款

第 16 条

不遵守条款和终止

(a) 如果数据输入者因任何原因未能遵守本条款，应立即通知数据输出者。

(b) 如果数据输入者违反本条款或无法遵守本条款，数据输出者应暂停向数据输入者传输个人数据，直至重新确保合规或合同被终止。这一规定不影响第 14(f) 条。

(c) 在下列情况下，数据输出者有权终止与本条款下的个人数据处理有关的合同：

(i) 数据输出者已根据第 (b) 款暂停向数据输入者传输个人数据，并且未在合理时间内（在任何情况下在暂停后一个月内）恢复遵守本条款；

(ii) 数据输入者严重或持续违反本条款；或

(iii) 数据输入者未能遵守主管法院或监管机构就其在本条款下的义务作出的具有约束力的决定。

在上述情况下，应将此类不合规情况告知主管监管机构。如果合同涉及两个以上的当事方，数据输出者只能对相关的当事方行使终止权，除非双方另有约定。

(d) 对于在根据第 (c) 款终止合同前传输的个人数据，数据输出者应选择立即返还给数据输出者或全部删除。这些数据的任何副本也适用相同的规定。数据输入者应向数据输出者证明已删除数据。在删除或返还数据之前，数据输入者应继续确保遵守本条款。数据输入者保证，如果适用于数据输入者的当地法律禁止返还或删除传输的个人数据，则其将继续确保遵守本条款，并且仅在当地法律要求的范围和时间内处理数据。

(e) 如果 (i) 欧盟委员会根据条例 (EU) 2016/679 第 45(3) 条通过一项涵盖适用本条款的个人数据传输的决定；或 (ii) 条例 (EU) 2016/679 成为接受个人数据的国家/地区的法律框架的一部分，则任何一方均可撤销其受本条款约束的协议。这一规定不影响条例 (EU) 2016/679 中适用于相关处理的其他义务。

第 17 条

适用法律

如果协议的适用法律（定义见数据处理附录）是欧盟成员国的适用法律，则本条款应受该欧盟成员国的法律管辖，前提是该法律承认第三方受益人权利。如果此类法律不承认第三方受益人权利，或如果本协议的适用法律不是欧盟成员国的法律，则协议应受承认第三方受益人权利的另一个欧盟成员国的法律管辖。双方同意在这种情况下协议应受爱尔兰法律的管辖。

第 18 条

法院和司法管辖区的选择

(a) 由本条款引起的任何争议应由欧盟成员国的法院解决。

(b) 双方同意，这些法院应为第 17 条中规定的欧盟成员国的法院。

(c) 数据主体还可在其惯常居住地所在的成员国的法院向数据输出者和/或数据输入者提起法律诉讼。

(d) 双方同意服从此类法院的管辖权。

欧盟标准合同条款附录 1

A. 当事方名单

数据输出者：
根据附有本条款的数据处理附录（“数据处理附录”）中的条款传输客户个人数据的客户和/或授权关联公司。

数据输入者：
代表其自身或其关联公司（如适用）作为数据输入者的科睿唯安实体，其同意根据附有本条款的数据处理附录中的条款从数据输出者处接收客户个人数据。

B. 传输描述

请参见附有本条款的数据处理附录的附件 A 中的详细说明。

C. 主管监管机构

主管监管机构是第 13 条规定的数据输出者的监管机构。

欧盟标准合同条款附录 2

技术和组织措施，包括确保数据安全的技术和组织措施

见数据处理附录的附件 B 所述。

双方确认，本条款第 2 (a) 条允许他们纳入额外的业务相关条款，前提是不会直接或间接违反本条款或损害数据主体的基本权利或自由。

因此，本附录列出了双方对其各自在下述特定条款项下的义务的解释。如果一方遵守本附录中列出的解释，则另一方应认为该方遵守了其在本条款项下的承诺。

第 3 条和第 8.6(d) 条：本条款的披露

数据输出者同意，本条款构成数据输入者的保密信息（该术语的定义见协议），未经数据输入者事先书面同意，数据输出者不得向任何第三方披露，除非协议允许。这不应妨碍根据第 3 条向数据主体或根据第 8.6(d) 条向监管机构披露本条款。

第 8.1(a) 和 8.1(b) 条：暂停数据传输和终止

1. 双方承认，就第 8.1(a) 条而言，数据输入者只能代表数据输出者处理个人数据，并遵守数据处理附录中规定的数据输出者的书面指示。并且，根据数据处理附录，这些指示应为数据输出者的完整和最终指示，此类指示范围之外的处理（如有）应由双方在书面商定后进行。
2. 双方承认，如果数据输入者不能根据第 8.1(a) 条和/或第 8.1(b) 条遵守，则数据输入者同意，及时将其不能遵守的情况通知数据输出者，在这种情况下，数据输出者有权根据协议条款暂停数据传输和/或终止受影响的部分服务。
3. 如果数据输出者打算暂停个人数据的传输和/或终止受影响的部分服务，则应首先向数据输入者发出通知，并向数据输入者提供一段合理的时间来纠正不遵守的情况（“纠正期”）。
4. 此外，数据输出者和数据输入者应在纠正期内合理地相互配合，以商定可能合理要求的额外保障措施或其他措施（如有），以确保数据输入者遵守本条款和适用的数据保护法。
5. 如果在纠正期后，数据输入者没有或不能根据上述第 3 和第 4 款纠正不遵守的情况，则数据输出者可以根据协议的规定暂停和/或终止受影响的部分服务，而任意一方无需承担任何责任（但不得影响数据输出者在暂停或终止之前产生的任何费用）。

第 8.9 条：审计

数据输出者承认并同意，其通过指示数据输入者遵守数据处理附录第 5 条（审计）中所述的审计措施来行使第 8.9 条下的审计权。

第 9(c) 条：子处理者协议的披露

1. 双方承认，数据输入者有义务及时将其根据本条款签署的任何后续子处理者协议的副本发送给数据输出者。
2. 双方进一步确认，根据子处理者保密限制，数据输入者可能被限制向数据输出者披露后续子处理者协议。尽管有此项规定，数据输入者仍应尽合理的努力，要求其指定的任何子处理者允许其向数据输出者披露子处理者协议。
3. 即使数据输入者不能向数据输出者披露子处理者协议，双方同意，应数据输出者的要求，数据输入者应（以保密的方式）向数据输出者提供所有其能够以合理方式提供的与该子处理协议相关的信息。

第 12 条：责任

在允许的范围内，根据本条款提出的任何索赔应遵守本条款中的条款和条件，包括但不限于协议中规定的除外责任和责任限制条款。在任何情况下，任何一方都不得限制该方在本条款项下与任何数据主体权利相关的责任。

附件 D - 英国附录

根据适用的数据保护法（包括英国 GDPR），科睿唯安（下称“输入方”）和客户（下称“输出方”）（分别称为“一方”，合称为“双方”）已就以下附录达成一致，以便为输出方向输入方传输附件 1 中规定的个人数据在保护个人隐私和基本权利及自由方面提供足够的保障。

第 1 部分：表

表 1: 当事人

开始日期	双方在协议上签字的日期。	
双方	**输出方（发送受限传输）**	**输入方（接收受限传输）**
各方详情	如协议中所述。	如协议中所述。
关键联系人	如所附欧盟标准合同条款的附件 1 所述。	如所附欧盟标准合同条款的附件 1 所述。
签名（如果出于第 2 条的目的需要）	不适用	不适用

表 2: 选定的标准合同条款、模块和选定的条款

附录欧盟标准合同条款	☒本附录所附的经批准欧盟标准合同条款版本（详见下文），包括附件信息： 日期：于下方双方签署之日生效（模块 2：向第三国家传输个人数据的标准合同条款 - 控制者到处理者）

表 3: 附件信息

“**附件信息**”是指经批准欧盟标准合同条款附件中规定的必须为所选模块提供的信息（当事方除外），对于本附录而言，附件信息参见：

附件 1A: 当事方名单：请参见随附欧盟标准合同条款的附件 I。
附件 1B: 传输描述：请参见随附欧盟标准合同条款的附件 I。
附件 II：技术和组织措施，包括确保数据安全的技术和组织措施：请参见随附欧盟标准合同条款的附件 2。
附件 III：子处理者列表（仅模块 2 和 3): 本附录 III 不适用，因为未选择随附附录欧盟标准合同条款的第 9(a) 条，选项 1 (子处理者的特定授权）。

表 4: 经批准的附录更改时，终止本附录

经批准的附录更改时，终止本附录	哪一方可以按照第 19 条的规定终止本附录： ☒ 输入方 ☒ 输出方 ☐任何一方都不可以

第 2 部分：强制性条款

签订本附录

1. 各方同意受本附录中规定的条款和条件的约束，条件是另一方也同意受本附录的约束。
2. 虽然经批准欧盟标准合同条款附件 1A 和第 7 条要求双方签字，但为了进行受限传输，双方可以对双方具有法律约束力的任何方式签订本附录，并允许数据主体行使本附录中规定的权利。签订本附录与签署经批准欧盟标准合同条款或其任何部分具有同等效力。

本附录的解释

3. 如果本附录使用经批准欧盟标准合同条款中定义的术语，这些术语的含义应与经批准欧盟标准合同条款相同。此外，以下术语具有以下含义：

附录	本国际数据传输附录，由本附录和附录欧盟标准合同条款组成。
附录欧盟标准合同条款	本附录所附的经批准欧盟标准合同条款版本，如表 2 所示，包括附件信息。

附件信息	如表 3 所示。
适当的保障措施	根据英国 GDPR 第 46(2)(d) 条的标准数据保护条款进行受限传输时，英国数据保护法律要求的个人数据保护标准和数据主体权利保护标准。
经批准的附录	ICO 根据《2018 年数据保护法案》第 119A 条于 2022 年 2 月 2 日签发并提交给议会的附录模板，该模板已根据第 18 条进行了修订。
经批准的欧盟标准合同条款	2021 年 6 月 4 日的委员会执行决定 (EU) 2021/914 附件中所载的标准合同条款。
ICO	信息专员。
受限传输	英国 GDPR 第五章涵盖的传输。
英国	大不列颠及北爱尔兰联合王国。
英国数据保护法律	英国不时生效的与数据保护、个人数据处理、隐私和/或电子通信相关的所有法律，包括英国 GDPR 和 2018 年数据保护法案。
英国 GDPR	定义见 2018 年数据保护法案第 3 条。

4. 本附录必须始终以符合英国数据保护法律的方式解释，以便履行双方提供适当保障的义务。
5. 如果附录欧盟标准合同条款中包含的条款以任何经批准的欧盟标准合同条款或经批准的附录不允许的方式修改经批准的标准合同条款，则此类修订将不包括在本附录中，且以经批准的欧盟标准合同条款的相应条款为准。
6. 如果英国数据保护法律与本附录之间存在任何不一致或冲突，则适用英国数据保护法律。
7. 如果本附录的含义不明确或有多个含义，则最符合英国数据保护法律的含义适用。
8. 凡提及法规（或法规的特定条文）时，均指随着时间推移而改变后的法规（或特定条文）。这包括在本附录签订后，该法规（或特定条款）合并、重新颁布和/或更换的情况。

优先顺序

9. 虽然经批准的欧盟标准合同条款第 5 条规定，经批准的欧盟标准合同条款优先于双方之间的所有相关协议，但双方同意，对于受限传输，以第 10 条中的优先顺序为准。
10. 如果经批准的附录与附录欧盟标准合同条款（如适用）之间存在任何不一致或冲突，则经批准的附录优先于附录欧盟标准合同条款,除非附录欧盟标准合同条款的不一致或冲突条款为数据主体提供更大的保护，在这种情况下，这些条款优先于经批准的附录。
11. 如果本附录并入的附录欧盟标准合同条款是为了保护根据通用数据保护条例 (EU) 2016/679 进行的传输而签订的，则双方确认本附录中的任何内容均不影响这些附录欧盟标准合同条款。

欧盟标准合同条款的并入和变更

12. 本附录根据需要并入经修订的附录欧盟标准合同条款，以便：
    a. 如果在数据输出方进行数据传输时的处理时适用英国数据保护法，将二者一起用于数据输出方向数据输入方进行的数据传输，并为数据传输提供适当的保障；

b. 附录欧盟标准合同条款第 9 至 11 条优先于第 5 条（优先顺序）；以及

c. 本附录（包括纳入本附录的欧盟标准合同条款）(1) 受英格兰和威尔士法律管辖，(2) 由此产生的任何争议由英格兰和威尔士法院解决，除非双方明确选择苏格兰或北爱尔兰的法律和/或法院。

13. 除非双方已商定符合第 12 条要求的替代修正案，否则第 15 条的规定应适用。

14. 除非符合第 12 条的要求，否则不得对经批准的欧盟标准合同条款进行修订。

15. 对附录欧盟标准合同条款进行了以下修订（出于第 12 条的目的）：

a. 提及“条款”时是指本附录，包含附录欧盟标准合同条款；

b. 在第 2 条中，删除以下词语：

“以及，关于从控制者到处理者和/或处理者到处理者的数据传输，条例 (EU) 2016/679 第 28(7) 条的标准合同条款”；

c. 第 6 条（传输描述）替换为：

“传输的详情，尤其是传输的个人数据的类别及其传输的目的，在附录 I.B 中规定，其中英国数据保护法适用于数据输出者在进行传输时的处理。”；

d. 模块 1 的第 8.7(i) 条替换为：

“是传输至根据英国 GDPR 第 17A 条受益于充分法规（涵盖后续传输）的国家/地区”；

e. 模块 2 和 3 的第 8.8(i) 条替换为：

“后续传输是传输至根据英国 GDPR 第 17A 条受益于充分法规（涵盖后续传输）的国家/地区；”

f. 提及“条例 (EU) 2016/679”、“欧洲议会和理事会 2016 年 4 月 27 日关于处理个人数据时保护自然人以及此类数据的自由流动的条例（通用数据保护条例）(EU) 2016/679”及“该条例”处，均替换为“英国数据保护法”。提及“条例 (EU) 2016/679”的特定条款处，替换为英国数据保护法的相应条款或部分；

g. 删除所提及的条例 (EU) 2018/1725；

h. “欧盟”、“联盟”、“欧盟成员国”、“成员国”和“欧盟或成员国”均替换为“英国”；

i. 模块 1 第 10(b)(i) 条中提及的“第 12(c)(i) 条”替换为“第 11(c)(i) 条”；

j. 不使用附件 I 第 13(a) 条和 C 部分；

k. “主管监管机构”和“监管机构”均替换为“信息专员”；

l. 第 16(e) 条中的第 (i) 小节替换为：

“国务卿根据《2018 年数据保护法案》第 17A 条制定了涵盖适用这些条款的个人数据传输的法规；”；

m. 第 17 条替换为：

“本条款受英格兰和威尔士法律管辖。”；

n. 第 18 条替换为：

“由本条款引起的任何争议应由英格兰和威尔士的法院解决。数据主体还可在英国任何地区的法院向数据输出者和/或数据输入者提起法律诉讼。双方同意服从此类法院的管辖权；且

o. 除脚注 8、9、10 和 11 外，经批准欧盟标准合同条款的脚注不构成附录的一部分。

本附录的修订

16. 双方可以约定将附录欧盟标准合同条款 第 17 条和/或第 18 条修改为引用苏格兰或北爱尔兰的法律和/或法院。

17. 如果双方希望更改第 1 部分中包含的信息格式：对于经批准的附录中的表格，只要变更不会减少适当的保障措施，他们可以通过书面同意更改来这样做。

18. ICO 可能会不时发布经修订的经批准附录，其中：

a. 对经批准的附录进行合理和适度的更改，包括更正经批准附录中的错误；和/或

b. 体现英国数据保护法律的变化；

经修订的经批准附录将规定经批准附录的变更的生效日期，以及双方是否需要审核本附录，包括附件信息。本附录自指定的开始日期起按照经修订的经批准附录中的规定自动修订。

19. 如果 ICO 根据第 18 条发布经修订的经批准附录，如果任何一方在表 4 中选择“经批准附录更改时结束附录”，则作为经批准附录的变更的直接结果，将会严重地、不成比例地、明显地增加其：

a. 履行本附录项下的义务的直接成本；和/或

b. 在本附录项下的风险，

在任一情况下，该方可首先采取合理措施来降低这些成本或风险，使其不至于严重和不成比例，然后通过在经修订的经批准附录的开始日期之前向另一方发送关于通知期限的书面通知，在合理的通知期结束时结束本附录。

20. 各方无需获得任何第三方的同意即可更改本附录，但任何更改都必须根据其条款进行。

附件 E - 司法管辖区特定条款

欧洲和英国：

(a) 反对子处理者。客户可以在收到通知后的十 (10) 个日历日内，根据附录第 3(a) 节的规定，以书面形式反对科睿唯安任命新的子处理者，但前提是此类反对以与数据保护相关的合理理由为依据。在这种情况下，双方应本着善意原则商讨此类问题，以期达成商业上合理的解决方案。如果无法达成此类解决方案，则科睿唯安将自行决定不指定此类子处理者、或者允许客户根据协议中的终止条款暂停或终止受影响的服务，而任意一方无需承担任何责任（但不得影响客户在暂停或终止之前产生的任何费用）。

(b) 政府数据访问要求。作为一般惯例，科睿唯安不会自愿向政府机构或部门（包括执法部门）提供客户个人数据。如果科睿唯安收到任何政府机构或部门（包括执法部门）发出的强制要求（无论是通过传票、法院命令、搜查令还是其他有效的法律程序发出），要求访问属于某个数据主体的客户个人数据，而该数据主体的主要联系人联系信息表明该数据主体位于欧洲或英国，则科睿唯安应：(i) 通知该政府机构，科睿唯安是该数据的处理者；(ii) 努力引导该机构直接向客户要求提供数据；及 (iii) 通过向客户的主要联系电子邮件地址发送电子邮件，将该要求告知客户，以便客户能够寻求保护令或其他适当救济。作为上述工作的一部分，科睿唯安可以向相关部门提供客户的主要和账单联系人联系信息。如果法律禁止科睿唯安遵守本第 (b) 款，或者科睿唯安有合理和善意的理由认为紧急访问是防止对任何个人安全、公共安全或科睿唯安造成严重伤害的紧迫风险所必需的，则不得要求科睿唯安遵守本款。

加利福尼亚州：

(a) 定义。除非另有说明，否则在 CCPA 定义的每种情况下，“控制者”的定义包括“业务部门”；“处理者”的定义包括“服务提供商”；“数据主体”的定义包括“消费者”；“个人数据”的定义包括“个人信息”。仅就附件 D 的本“加利福尼亚州”条款而言，“许可目的”应包括在为遵守适用法律而必需的情况下，仅出于本附录所述的目的并根据本附录规定的客户书面合法指示来处理客户个人数据，除非另有书面约定（包括但不限于协议中另有书面约定），或者除非是在 CCPA 中规定的可能为“服务提供商”许可的其他情况下。

(b) 消费者权利。本附录第 8 条（数据主体权利与合作）中所述的科睿唯安与数据主体请求相关的义务，适用于 CCPA 项下的消费者权利。

(c) 许可目的。尽管本附录其他部分包含有任何使用限制，但除非适用法律另有要求，否则科睿唯安仅应出于许可目的且/或根据客户的书面合法指示来处理客户个人数据以履行服务。作为履行本附录和协议项下服务的一部分，科睿唯安可能会对客户个人数据作去身份识别化处理或聚合客户个人数据。

(d) 子处理者。如果子处理者处理客户联系人的个人数据，则科睿唯安将采取措施确保：此类子处理者是 CCPA 项下的服务提供商且科睿唯安与其订立了书面合同，合同中包含与本附录基本相似的条款；或者此类子处理者不受 CCPA 中“销售”定义的约束。科睿唯安对其子处理者进行适当的尽职调查。如果子处理者处理客户联系人的个人数据，则科睿唯安将采取措施确保：此类子处理者是 CCPA 项下的服务提供商且科睿唯安与其订立了书面合同，合同中包含与本附录基本相似的条款；或者此类子处理者不受 CCPA 中“销售”定义的约束。科睿唯安对其子处理者进行适当的尽职调查。

加拿大：

(a) 子处理者。科睿唯安采取措施，确保科睿唯安的子处理者（如本附录第 3 条（子处理者）所述）是 PIPEDA 项下的第三方，且科睿唯安与其订立了书面合同，合同中包含与本附录基本相似的条款。科睿唯安对其子处理者进行适当的尽职调查。

(b) 安全。科睿唯安将实施本附录第 4 条（安全）中规定的技术性和组织性措施。

2022 年 11 月