数据处理附录

本数据处理附录（连同其附件，合称“**附录**”）纳入由科睿唯安实体作为协议一方（与其关联公司合称“科睿唯安”）与客户实体作为协议另一方（下称“客户”或“您”）签订的协议（定义见下文）。

本附录规定了科睿唯安在根据本协议提供服务过程中处理客户个人数据（定义见下文）时应遵守的条款、要求和条件。科睿唯安保留不时更新本附录的权利。如果发生任何此类更新，科睿唯安应相应地通知客户。如果本附录、协议以及科睿唯安与客户之间的任何其他适用协议之间存在任何冲突或不一致之处，应以本附录的条款为准。

本附录中使用但未定义的粗体术语应具有协议中规定的含义。

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。

c) **“客户个人数据”**指科睿唯安在根据协议向客户提供的服务过程中处理的任何个人数据。

d) **“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。**“受控”**一词应作相应解释。

e) **“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和隐私法律法规，包括但不限于：《欧盟通用数据保护条例》（the EU General Data Protection Law Regulation，**“GDPR”**）；经《加州隐私权法》(California Consumer Privacy Act) 修订的《加州消费者隐私法》（the California Privacy Rights Act，**“CCPA”**）；《儿童在线隐私保护法案》（the Children's Online Privacy Protection Act，**“COPPA”**）；加拿大《个人信息保护和电子文件法》（the Canadian Personal Information Protection and Electronic Documents Act，**“PIPEDA”**）；《巴西通用数据保护法》（the Brazilian General Data Protection Law，**“LGPD”**）；《澳大利亚1988年隐私法》（the Privacy Act 1988 of Australia，**“《澳大利亚隐私法》”**）；《瑞士联邦数据保护法案》（the Swiss Federal Act on Data Protection，**“FADP”**）；英国采纳的 GDPR（**“英国 GDPR”**），上述每项法律均经不时修订。

f) **“欧盟 SCCs”**指欧盟委员会为根据 GDPR 向第三国/地区传输个人数据而采纳的标准合同条款(standard contractual clauses)，特别是经不时更新的模块一（控制者到控制者）（如适用）和模块二（控制者到处理者）。

g) 就本附录而言，**“欧洲”**指欧盟、欧洲经济区和/或其成员国。

h) **“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。

i) **“服务”**指协议中规定的相关服务。

j) **“特殊类别个人数据”**指以下个人数据：(i) 表明种族或民族本源、政治观点、宗教或哲学信仰或工会身份的个人数据，以及为唯一识别自然人身份而处理的基因数据、生物特征数据，健康数据，或关于自然人性生活或性取向的数据；(ii) 与刑事定罪及违法犯罪相关的数据。

k) **“子处理者”**指科睿唯安聘用的任何第三方或科睿唯安关联公司（视情况而定），其被委托协助履行与科睿唯安根据本协议提供服务相关的义务。

l) **“英国附录”**指由英国信息专员办公室（**“UK ICO”**）发布的《欧盟委员会标准合同条款国际数据传输附录》（the EU Commission Standard Contractual Clauses， B1.0 版，于 2022 年 3 月 21 日生效）。

“适当保障措施”、**“控制者”**、**“出售”**、**“分享”**、**“数据主体”**、**“个人信息”**、**“个人数据”**、**“处理者”**和**“处理”**（包括“处理”的任何变体形式）等术语，应具有数据保护法所规定的含义。若数据保护法中存在与上述术语含义相同或相近的术语，则应适用此类含义相同或相近的术语。

2. 角色和职责

(a) 双方的角色。如果数据保护法适用于任何一方对客户个人数据的处理，则双方承认并同意，就客户个人数据的处理而言，客户是控制者，科睿唯安是处理者，具体详见本附录的附件 A（“**数据处理详细说明**”）。尽管双方角色通常按上述分配，但科睿唯安可以出于运营目的（例如计费和账户管理、财务报告、业务建模和内部报告等）进行统计分析，作为独立控制者处理客户个人数据，详见科睿唯安的隐私政策（详见：https://clarivate.com/legal/privacy-statement/）。

(b) 目的限制。科睿唯安应根据客户书面的合法指示并在遵守适用法律的必要情况下处理客户个人数据；在后一种情况下，如果相关法律未以重大公共利益为由明文禁止，科睿唯安应告知客户相关法律要求。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，并且科睿唯安对此类数据的处理不承担任何责任，无论是与个人数据泄露还是其他方面有关。这也适用于协议或数据保护法禁止的其他类别的个人数据。

(d) 客户合规。客户陈述并保证，其在处理客户个人数据及向科睿唯安发出的任何处理指示方面，已遵守且将继续遵守所有数据保护法。客户应对客户个人数据的准确性、质量和合法性以及客户收集客户个人数据的方式全权负责。如果科睿唯安作为处理者按照客户的指示以及本附录和协议的条款行事，客户应保护科睿唯安免受因任何违反数据保护法而产生的损害。

(e) 客户指示的合法性。客户应确保：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。如果科睿唯安发现客户的任何数据处理指示违反适用法律（包括数据保护法），科睿唯安可停止处理相关客户个人数据。在这种情况下，科睿唯安应在合理的期限内以书面形式通知客户。如果客户未调整其指示，导致违反适用法律，科睿唯安可立即终止协议和本附录。

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，允许科睿唯安委托子处理者代表客户处理客户个人数据，以实现提供服务的目的。客户可以通过科睿唯安的隐私中心（参见“透明度和选择”部分）访问子处理者名单，或直接发送邮件至 **data.privacy@clarivate.com** 向科睿唯安索要。此外，客户可以通过子处理者名单中包含的表格订阅接收任何拟替换和新增其子处理者的通知。订阅后，科睿唯安应通知客户有关新增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（在数据保护法要求的情况下）。

4. 安全

(a) 安全措施。科睿唯安应根据附件 B 中所述的科睿唯安安全标准，实施并维持适当的技术和组织安全措施（“**技术和组织措施**”），确保达到与客户个人数据风险相适应的安全水平。

(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) 在合理可行的情况下尽快通知客户，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；(iii) 立即采取合理措施遏制并调查任何个人数据泄露。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**。在客户至少提前六十 (60) 天发出书面通知的情况下，科睿唯安应向客户提供证明其遵守本附录所需的所有合理必要信息，同时允许且协助审计工作（若在合理范围内可行），包括客户进行检查以评估是否遵守本附录，相关费用由客户独自承担。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，则客户同意通过书面指示科睿唯安提供其最新报告或认证文件副本的方式行使其审计权，此类报告或认证文件将被视为科睿唯安的保密信息。如果科睿唯安未能提供此类报告或认证文件，客户（包括其委托的审计机构）有权自行进行审计，费用自理。除非科睿唯安发生个人数据泄露事件或面临与其隐私及安全实践相关的正式投诉，否则该审计每年仅限一次。

(b) **适用于客户审计的范围和条款。**客户委托的审计机构不得为科睿唯安的竞争对手，且应遵守符合科睿唯安要求的保密协议，该协议要求审计机构对科睿唯安的保密信息及所有审计结果承担保密义务。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。对于科睿唯安为此类审计所花费的任何时间产生的费用，客户应对科睿唯安进行补偿。如果要求对科睿唯安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。所有补偿费率和费用应按照科睿唯安的小时费率计算，并计入科睿唯安或其第三方子处理者所耗费的资源。审计和检查应遵守科睿唯安合理的数据保护及信息安全政策。审计范围应限于科睿唯安的信息系统，或适用于保护客户个人数据的政策和程序。客户同意不审查科睿唯安的原始数据、私人、敏感、保密或专有商业信息，包括员工薪资单、人事记录，以及与客户个人数据无关，或属于其他商业敏感信息或受法律保密特权保护的科睿唯安网站、账簿、文件、记录或其他信息的任何部分。客户不得复制科睿唯安的安全信息或任何材料，也不得将其从科睿唯安的场所或系统中移除。
客户应向科睿唯安提供审计结果的副本，且科睿唯安无需承担任何费用。完成审计后，若在审计过程中发现科睿唯安存在违反本附录项下其应承担的安全、保密或数据保护义务的情况（如有），客户应立即向科睿唯安详细通报。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. 国际数据传输

(a) **从科睿唯安向第三方进行的数据传输**。在遵守第 3 条和第 6 条的前提下，科睿唯安可将客户个人数据传输给数据保护法所定义的第三国/地区境内的数据接收方，但需确保遵守数据保护法中关于跨境数据传输的规定。

(b) **GDPR 数据传输**。如果科睿唯安位于欧盟/欧洲经济区之外，并接收受 GDPR 保护的客户个人数据，但 GDPR 第 45 (3) 条所指的充分性决定不适用于该传输，则双方同意通过签订本附录来采用欧盟标准合同条款 (“欧盟 SCC”)。因此，欧盟 SCC 应被视为纳入本附录，其中科睿唯安应作为“数据输入者”，客户作为“数据输出者”。双方特别约定如下：(i) 欧盟 SCC 第 7 条不适用；(ii) 针对模块二，适用第 9(a) 条中的选项 2（一般授权），且通知期限至少为十 (10) 天；(iii) 不设立争议解决机构（第 11 条）；(iv) 适用第 17 条中的选项 2，且适用协议中确定的成员国法律；若未就成员国法律达成一致，则适用爱尔兰法律；且(v) 第 18 条规定的法院选择以协议约定为准；若未就成员国法院达成一致，则约定爱尔兰法院。欧盟 SCC 附件 1 中要求的信息载于本附录的附件 A 中，而主管监管机构应为欧盟 SCC 第 13 条中确定的、对数据输出者具有管辖权的监督机构。欧盟 SCC 附件 2 中要求的信息载于本附录的附件 B 中。

(c) **英国数据传输**。如果科睿唯安位于英国境外并接收受英国 GDPR 保护的客户个人数据，但不适用英国充分性法规所规定的充分性认定，则双方同意采用经英国附录（UK Addendum）修订的欧盟 SCC（其形式如第 6(b) 条所述），此类条款应通过援引视为纳入本附录。

(d) **FADP 数据传输。**如果科睿唯安位于瑞士境外并接收受 FADP 保护的客户个人数据，但不适用 FADP 所规定的充分性决定，则双方同意采用欧盟 SCC（其形式如第 6(b) 条所述），并按以下方式修订：(i) 对 GDPR 的援引应解释为对 FADP 相应条款的援引；(ii) 对“欧盟”、“联盟”、“成员国”及“成员国法律”的提及，应视情况解释为对瑞士及瑞士法律的提及；(iii) 附件 B 中指定的主管监管机构为瑞士联邦数据保护与公开事务专员（Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter）；(iv) 适用瑞士法律（第 17 条）；(v) 第 18 条中的法院和管辖地选择为瑞士；(vi) 第 18 (c) 条中“成员国”一词的解释，不得排除居住在瑞士的数据主体主张赔偿的权利。

(e) **替代传输机制**。如果科睿唯安实施或采用数据保护法规定的替代数据传输机制（包括欧盟 SCC 的任何新版本或

后续替代版本）（以下合称“**替代传输机制**”），以按照数据保护法规定传输客户个人数据，则此类替代传输机制应取代本附录中规定的传输机制适用。如果有司法管辖权的法院或监管机构（无论出于何种原因）裁定，不能依赖本附录中所述的措施来依据数据保护法合法传输客户个人数据，则科睿唯安可以实施为实现客户个人数据合法传输而合理所需的任何额外措施或保障措施。

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三十 (30) 天内作出的选择，科睿唯安应（根据客户的选择）删除或向客户归还科睿唯安拥有或控制的所有客户个人数据（包括副本），但该等归还可能导致按照科睿唯安当时的小时费率向客户收取额外费用，此类费用将在单独的报价单和工作说明中列明。此要求不应适用于：(i) 适用法律法规要求科睿唯安保留部分或全部客户个人数据的情况；(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；或(iii) 科睿唯安作为独立控制者处理的客户个人数据（如第 2 条所述）。

8. 协助行使数据主体权利和履行数据保护法项下的其他义务

(a) **数据主体请求**。在服务过程中，科睿唯安为客户提供了一些自助服务功能，客户可以利用这些功能检索、更正、删除或限制使用客户个人数据，并履行数据保护法项下的义务，以回应数据主体提出的行使数据保护法赋予的数据主体权利的请求，而不收取额外费用。如有需要，考虑到处理的性质，科睿唯安应向客户提供进一步的合理协助，以使其履行数据保护法项下的义务，回应数据主体提出的行使数据保护法所赋予的数据主体权利的请求。如果任何此类请求是直接向科睿唯安提出的，除在合理适当的情形下（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科睿唯安的哪些客户有关）或适用法律要求外，科睿唯安应争取获得客户的事先授权，以直接回应此类沟通请求。若科睿唯安回应此类请求，则科睿唯安应通知客户并向客户提供请求副本——除非法律禁止科睿唯安这样做，或科睿唯安认为此举不切合实际、不合理（该请求对客户无价值或价值极低），或违反适用法律。

(b) **数据保护法项下的义务**。在数据保护法要求的范围内，且始终仅与服务相关的情况下，科睿唯安应（在考虑处理的性质及科睿唯安掌握信息的基础上）提供合理程度的协助，以使客户能够确保履行其在数据保护法项下的义务，例如开展数据保护影响评估。

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 C 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 C 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，应以下列文件的规定为准（按优先顺序）：首先是 (i) 标准合同条款；其次是 (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。但是，为明确起见，本条款不应限制数据主体依据欧盟 SCC（经修订，以适用英国 GDPR 和 FDPA）享有的任何权利。

(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。

附件 A — 数据处理详细说明

本附件 A 概述了科睿唯安作为处理者和客户作为控制者的数据处理活动的具体详细信息。

数据控制者：
协议中定义的客户。

处理者：
本附录引言中定义的科睿唯安。

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在必要情况下处理：(i) 根据协议提供服务；(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；(iv) 保持服务的更新和性能，提升用户生产力、可靠性、效率、质量及安全性；(v) 修复服务中的漏洞并排查问题；(vi) 下表中按此类适用服务列明的目的和性质。

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中按服务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，可能包括但不限于下表中按服务列明的个人数据类别以及所提供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	• 姓名和其他非敏感身份识别信息，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类别的个人数据

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
	托管、实施和/或技术支持	• 图书馆读者、图书馆工作人员、教职员工与学生、行政管理人员、员工、访客和校友	• 基本用户和读者信息，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
			• 与员工相关的使用信息，包括员工操作和活动记录

Intota™ Assessment Pivot/Pivot-RP RefWorks Summon Ulrichsweb Ulrich's™ Serials Analysis System Intota™			• 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
EndNote	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 • 客户 • 潜在客户 • 控制者确定的其他数据主体	• 姓名和其他非敏感身份识别信息，如电子邮件地址、研究人员识别号、用户名 • 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类别的个人数据
First to File	用户账户预注册；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	• 姓名和其他非敏感身份识别信息，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类别的个人数据
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，包括图书馆读者	• 图书馆读者数据，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；对于图书馆读者而言，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 • 姓名和其他非敏感身份识别信息，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类别的个人数据

知识产权管理系统： **FoundationIP** **IPfolio** **Ipendo** **Inprotech** **Memotech** **Patrawin** **知识产权管理系统（The IP Managemen）** **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	• 姓名和其他非敏感身份识别信息，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类别的个人数据
知识产权专业服务（IP Professional Services）	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 • 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	• 姓名和其他非敏感身份识别信息，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类别的个人数据
市场研究 — 合同要求的作为市场研究活动一部分的安全与质量报告	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 enchmarking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	• 姓名和其他非敏感身份识别信息，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	图书馆读者、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	• 基本用户和读者信息，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/目录相关的用户和读者信息，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	• 姓名和其他非敏感身份识别信息，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	• 姓名和其他非敏感身份识别信息，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

特殊类别个人数据：

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 条所述。

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。

此外，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 7*24 小时全天候记录和监控。安全日志发送到我们的安全运营中心，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 — 特定司法管辖区条款

欧洲经济区、英国和瑞士：

政府数据访问请求。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经济区、英国或瑞士，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；(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。

美国加利福尼亚州：

附件 C 中的本“美国加利福尼亚州”条款仅在科睿唯安根据 CCPA 的范围处理客户个人数据时适用并对双方具有约束力。附件 C 中的本“美国加利福尼亚州”条款优先于协议或本附录的任何冲突条款，但除此之外不修改协议或本附录的其他内容。双方一致同意如下：

(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 C 中的本“加利福尼亚州”条款而言，“**许可目的**”包括：仅出于本附录中所述的有限且特定的商业目的处理个人数据；根据本附录中规定的客户书面合法指示进行处理；为遵守适用法律所必需的处理；经书面另行约定的处理（包括但不限于协议中的约定）；CCPA 中可能规定的允许为服务提供商进行的其他处理。

(b) 合规。科睿唯安将遵守 CCPA 的适用条款，包括提供 CCPA 要求的企业达到的同等隐私保护水平。科睿唯安在确定其无法再履行其在 CCPA 项下的义务后，可通知客户。客户可以采取合理适当的措施，确保科睿唯安以遵守客户在 CCPA 项下的义务的方式使用客户个人数据。客户可在提前书面通知的情况下，采取合理适当的措施，阻止并纠正科睿唯安未经授权使用客户个人数据的行为。

(c) 禁止的用途。科睿唯安不会：

- 按照 CCPA 对“出售”或“分享”的定义，出售或分享根据协议收集的客户个人数据；
- 出于协议和本附录中规定的业务或商业目的以外的目的保留、使用或披露客户个人数据；
- 在与客户的直接业务关系之外保留、使用或披露客户个人数据（除非适用的数据保护法或法规明确允许）；
- 将客户个人数据与从他人处或代表他人收到的个人信息合并，或与科睿唯安通过自身与消费者互动所收集的个人信息合并（CCPA 允许的情况除外）。

美国学生数据 —《家庭教育和隐私权》(Family Educational and Privacy Rights，“FERPA”)：

附件 C 中的本“美国学生数据”条款仅在科睿唯安处理 FERPA 范围内的客户个人数据（“**FERPA 数据**”）且客户属于受 FERPA 项下规定约束的教育机构或组织时，才对双方具有约束力。附件 C 中的本“美国学生数据”条款优先于协议或本附录的任何冲突条款，但除此之外不修改协议或本附录的其他内容。双方一致同意如下：

(a) 客户将负责提供任何必要的通知，并获取任何在科睿唯安处理 FERPA 数据过程中依据适用法律要求可能需要的父母的同意。

(b) 根据《美国联邦法规》（Code of Federal Regulations，“CFR”）第 34 编第 99.31 (a)(1)(i) 条，除非协议或本附录授权，或客户以书面形式另外授权，或适用法律要求，否则科睿唯安不得向任何其他方披露 FERPA 数据。为避免疑问，客户同意科睿唯安可出于提供服务的目的，向其子处理者披露 FERPA 数据。

2025 年 06 月 (Version 3.0)