数据处理附录（先前的 SaaS 附录）

本数据处理附录 (“**DPA**”) 并入提供商和客户之间就购买某些 SaaS 软件许可和/或维护和/或咨询服务（在本 DPA 下文中简称“**服务**”）而订立的软件协议和/或服务协议（“**协议**”）中，并构成提供商与客户之间订立的书面（包括电子形式）合同的一部分。本 DPA 中未定义的所有术语应具有协议中规定的含义。

1. **定义**在上下文或协议中未定义的术语应具有以下含义：

a) “***控制者***”是指单独或与他人共同决定个人数据处理目的和方式的自然人或法人、政府机构、机构或其他团体。

b) “***数据保护法***”是指适用于在协议项下处理客户个人数据的所有法律和法规，包括（如适用）：(i) 经《加州隐私权法》修订的《加州消费者隐私法》，以及据其颁布的任何具有约束力的法规 (“**CCPA**”)，(ii)《通用数据保护条例》（条例 (EU) 2016/679）（“**EU GDPR**”或“**GDPR**”），(iii) 《瑞士联邦数据保护法》(“**FADP**”)，(iv) 根据《2018 年退出欧盟法案》第 3 节构成英格兰和威尔士法律的一部分的 EU GDPR（“**英国 GDPR**”）以及 (v) 英国 2018 年《数据保护法案》；上述法律和法规均包括其不时更新、修改或替换后的版本。

c) “***数据主体***” 是指与客户个人数据相关的已识别身份或可识别身份的自然人。

d) “***个人数据***”是指有关已识别身份或可识别身份的自然人的信息，或以其他方式构成“个人数据”、“个人信息”、“个人身份信息”或数据保护法中定义的类似术语的信息。

e) “***个人数据泄露***”是指意外或非法破坏、丢失、更改、未经授权披露或第三方未经授权访问提供商正在处理的客户个人数据，在上述每种情况下，数据保护法均要求控制者通知主管数据保护机构或数据主体。

f) “***处理***”是指对个人数据执行的任何操作（无论是否通过自动方式），例如收集、记录、组织、结构化、存储、改编或更改、检索、查阅、使用、通过传输披露、传播或以其他方式提供、对齐或组合、限制、删除或销毁。

g) “***处理者***”是指代表控制者处理个人数据的自然人或法人、政府机构、机构或其他团体。

h) “***标准合同条款***”或“**欧盟标准合同条款**”是指欧盟委员会在第 2021/914 号决议中批准的标准合同条款。

i) “***子处理者***”是指提供商的关联方和由提供商（或提供商的关联方）聘用以提供任何或全部服务并根据本 DPA 处理客户个人数据的第三方。

2. **客户个人数据的处理**

提供商可以根据协议作为处理者代表作为控制者的客户处理客户个人数据（或作为子处理者（如适用）代表作为处理者的客户）。提供商承诺根据 (i) 本 DPA 和协议，以及 (ii) 客户的书面指示，或 (iii) 为了遵守适用法律规定的提供商的义务，在遵守数据保护法规定的任何通知要求的情况下，出于履行提供商对客户负有的义务的唯一目的处理个人数据。处理的主题、持续时间、性质和目的，以及客户个人数据的类型和数据主体的详细信息均在协议中有所规定，或者，如果协议中未规定，则应在本 DPA 的附件 1 中规定。客户和提供商同意遵守适用于与服务相关的个人数据处理的数据保护法规定的各自义务。在向提供商披露、传输或以其他方式提供任何个人数据之前，客户全权负责遵守有关处理客户个人数据的数据保护法。如果提供商认为客户的指示将违反数据保护法，则提供商应立即通知客户。

3. **处理的安全性**

a) **一般安全政策**。 提供商应根据协议中提及的提供商安全措施，根据客户个人数据的性质实施和维护技术和组织措施、程序和实践，以保护客户个人数据的安全性、机密性、完整性和可用性，并防止个人数据泄露，上述安全措施的详细描述参见：https://www.quest.com/legal/security.aspx（统称为“***安全网站***”），包括：

- 信息安全政策，
- 技术和组织措施声明，
- 数据泄露响应政策，以及
- 隐私政策。

提供商可以修改其安全网站，但不得实质性地降低所提供的整体保护水平。

b) **保密**。提供商应根据协议中规定的保密义务保护客户个人数据。提供商应确保处理客户个人数据的人员已订立书面保密协议。提供商应确保此类保密义务在任何此类人员的雇佣关系终止后仍然有效。提供商应定期对有权访问客户个人数据的个人进行数据安全和数据隐私要求和原则方面的培训。

4. 数据主体请求。

根据客户的要求，提供商应采取商业上合理的措施来协助客户遵守数据保护法规定的客户义务，以回应个人行使数据保护法规定的权利的请求，前提是合理情况下客户无法独立满足此类请求（包括通过使用服务）。如果提供商收到与根据本 DPA 处理的个人数据相关的数据主体请求，提供商应建议数据主体（在数据主体已提供客户识别信息的情况下）将请求提交至客户。

5. 审计权。

a) **一般提供商记录。**提供商应根据数据保护法保存其处理记录，并应客户的书面请求，向客户提供任何合理必要的记录，以证明提供商遵守了本 DPA 和适用的数据保护法规定的义务。

b) **第三方合规计划。**提供商应说明其第三方审计和认证计划（如有），并根据客户的书面请求（在遵守协议中规定的保密义务的前提下）向客户提供其审计报告的摘要副本（分别称为**"审计报告"**）。客户可以根据需要与相关政府机构共享审计报告的副本。

c) **客户审计。**客户可以根据符合以下审计参数且经双方商定的计划进行审计（**"审计"**），费用由客户承担。在以下情况下，客户可以行使其审计权：(1) 提供商提供的审计报告没有为客户提供足够的信息来验证提供商是否遵守本 DPA 或是否遵守数据保护法；(2) 客户需要回应政府当局审计，或 (3) 存在个人数据泄露。

每次审计必须 (1) 由与提供商订立了保密协议的独立第三方进行，(2) 仅限于客户评估提供商是否遵守本 DPA 以及双方是否遵守数据保护法合理需要的范围，(3) 在双方商定的日期和时间进行，并且仅在提供商的正常工作时间内进行，(4) 每年不超过一次（除非数据保护法有要求或存在个人数据泄露），(5) 仅涵盖提供商控制的设施，(6) 将调查结果仅限于客户个人数据，且 (7) 在数据保护法允许的最大范围内将任何结果视为机密信息。

6. 子处理者和国际传输。

a) **使用子处理者。**客户通常授权提供商就提供服务聘用子处理者。提供商应根据本 DPA 的规定以及客户与提供商之间的指示，与子处理者签署适当的书面协议。提供商对提供商聘用的子处理者任何违反本 DPA 的行为负责。

b) **子处理者名单。**提供商维护每个软件产品的子处理者列表，包括其职能和地点，客户可以通过在 https://support.quest.com/subprocessor 注册获得。在授权任何新的子处理者访问个人数据前，提供商应至少提前三十 (30) 天更新子处理者列表并在注册时通过电子邮件通知客户。

c) **反对新的子处理者。**如果客户不批准新的子处理者，则客户可以在通知期结束前提供书面终止通知（其中包括对不批准理由的解释）来终止适用的 SaaS 软件的任何订阅。

d) **国际传输。**为了将欧洲和/或英国的个人数据传输到位于第三方国家/地区的子处理者（该第三方国家/地区无法为个人数据提供充分保护），提供商和适用的子处理者已签订欧盟标准合同条款，以提供适当的保障措施，从而根据欧洲和英国数据保护法传输此类个人数据。

7. 个人数据泄露通知。

除了安全网站中规定的义务外，提供商在发现个人数据泄露后应立即通知客户，并提供合理的信息以协助客户履行数据保护法要求的报告个人数据泄露的义务。提供商可根据所掌握的信息分阶段提供此类信息。提供商同意尽善意努力查明个人数据泄露的原因，并采取提供商认为必要和合理的措施来补救个人数据泄露的原因。

8. 删除客户个人数据。

在协议终止或到期后，提供商将从提供商的系统中删除所有客户个人数据，除非客户在服务完成前至少提前三十 (30) 天通知提供商。提供商应根据行业标准的安全删除惯例执行删除。尽管有上述规定，但提供商可以 (i) 根据数据保护法的要求，或 (ii) 根据其标准备份或记录保留政策保留客户个人数据，前提是在任何一种情况下，提供商均应 (1) 对保留的客户个人数据进行保密，并在其他方面遵守本 DPA 中的相关适用规定，并且 (2) 不进一步处理保留的客户个人数据，适用的数据保护法规定的处理目的和持续时间除外。

9. 数据保护影响评估。

提供商应根据需要向客户提供合理的合作和协助，以履行数据保护法规定的客户义务，进行数据保护影响评估或与客户使用服务相关的类似风险评估。

DPA 附件

本附件构成 DPA 的一部分。

附件 I

A. 缔约方名单

客户（作为控制者）与提供商（作为处理者）之间的协议包含对所有必需信息的描述，例如：

- 姓名、地址、联系人姓名、
- 职位和联系方式，
- 与根据这些条款传输的数据相关的活动，以及
- 签名和日期。

B. 处理说明

1. 个人数据被处理的数据主体的类别

除非客户另有规定，否则处理的个人数据涉及以下类别的数据主体：

- 客户的员工、承包商、业务合作伙伴。

2. 处理的个人数据的类别

客户根据其对服务的使用确定数据类别。处理的个人数据通常涉及以下数据类别：

- 与客户的员工或其他第三方（其个人信息由客户或代表客户提供）有关的雇佣详情（可能包括公司名称和地址、职务、等级、人口统计和位置数据）；
- 与客户系统或客户提供给提供商的系统以及与根据协议购买的服务相关的系统信息以及提供服务所需的系统信息（可能包括用户 ID 和密码、计算机和域名、IP 地址、GUID 号或正在使用的计算机或其他设备的位置）。

根据本协议处理的客户个人数据可能涉及过去、现在和未来的业务合作伙伴或与此类业务合作伙伴相关的其他个人。

3. 处理的敏感数据（如果适用）

客户不得提供特殊类别的个人数据（敏感数据），除非根据具体情况确定，并且仅应在双方同意提供服务涵盖此类特殊类别数据的范围内提供。

4. 处理频率（例如，是一次性处理还是连续处理数据）

在使用服务期间连续处理。

5. 处理的性质

a) 根据软件维护协议：当客户因软件不可用或未按预期运行而提交支持请求时，提供商或其子处理者将提供支持。他们会接听电话并执行基本的故障排除，并在跟踪系统中处理支持请求。

b) 根据咨询服务协议：提供商或其子处理者根据服务订单提供服务。

c) 根据 SaaS 软件协议：提供客户购买的 SaaS 软件。

6. 数据传输的目的和进一步处理

提供商将对客户个人数据进行以下基本处理：

a) 使用个人数据来提供提供商服务，并在适用的情况下，根据协议提供对 SaaS 软件的访问和使用权限，并根据客户的请求和具体要求视情况提供技术支持，所有处理均应按照以下指示

b) 个人数据的存储；

c) 为数据传输而对个人数据进行计算机处理；

d) 持续改进作为提供商服务的一部分提供的服务特性和功能，包括自动化、事务处理和机器学习；

e) 根据协议执行客户的指示。

以下附加处理活动适用于存储在 SaaS 软件中的任何个人数据：

a) 在数据中心中存储个人数据（多租户架构）；
b) 备份和恢复存储在 SaaS 软件中的客户个人数据；
c) 个人数据的计算机处理，包括数据传输、数据检索、数据访问；
d) 与客户的用户沟通；
e) 发布、开发和上传 SaaS 软件的任何修复或升级；
f) 允许个人数据传输的网络访问；
g) 监控、故障排除和管理底层 SaaS 软件基础架构和数据库；
h) 安全监控、基于网络的入侵检测支持、渗透测试；以及
i) 必要时根据下文所述的指示视情况回应和解决数据主体的请求和要求。

提供商可以将匿名数据（不是客户个人数据，但可能源自客户个人数据）用于与产品改进和提供商新产品和服务开发相关的目的。

有关 SaaS 软件产品功能、它如何处理个人数据以及数据存储位置的更多详细信息，请参阅适用的产品文档和安全指南。

7. 个人数据的保留期限，或者如果无法规定期限，用于确定该期限的标准

上述个人数据应在客户根据协议使用服务期间处理，并受本 DPA 第 9 条的约束。

8. 对于面向（子）处理者的传输，还应规定处理的主题、性质和持续时间

对于欧盟标准合同条款，面向子处理者的传输应基于本 DPA 中规定的相同基础。

9. 指示、客户和提供商承诺。

提供商应遵循从客户处收到的关于客户个人数据的书面且有记录的指示，除非提供商认为此类指示 (1) 被法律禁止或可能导致违反适用的数据保护法，(2) 要求对提供商的服务进行重大变更，和/或 (3) 与协议项下销售的服务相关的协议或提供商文档的条款不一致。在任何此类情况下，提供商应立即通知客户其无法遵守此类指示。协议、本 DPA 和提供商的任何相关文件中对处理的任何描述均应视为客户的指示。

附件 II - 技术和组织措施声明

提供商应在提供商处理客户个人数据的过程中使用安全网站（定义见 DPA 第 3(a) 条）中规定的适当技术和组织措施。客户同意提供商可以修改为保护客户个人数据而采取的措施，但是不得实质性降低本文商定的整体数据保护水平。