软件即服务附录

本软件即服务附录（“**附录**”）由作为客户的您（“**客户**”或“**您**”）与提供商共同签订，并构成您和提供商之间的引用本附录的协议（“**协议**”）的一部分。本附录中未另行定义的术语应具有本附录中规定的含义。

1. **定义。**未在上下文中或协议中定义的黑体术语具有下文赋予的含义：
   (a) “***适当的保障措施***”指通用数据保护条例（GDPR）第 46 条规定的适当保障措施，例如欧盟委员会采用的具有约束力的公司规则或标准数据保护条款（例如下文定义的标准合同条款）。
   (b) “***控制者***”、“***数据主体***”、“***个人数据***”、“***处理***”、“***个人数据泄露***”、“***处理者***”、“***监督机构***”具有 GDPR 第 4 条规定的含义。
   (c) “***客户个人数据***”指客户通过使用软件即服务（SaaS）软件向提供商（以提供商作为处理者的身份）提供的个人数据。
   (d) “***数据保护法***”指适用于个人数据的处理的所有法律法规，包括欧盟的法律法规，例如 2016 年 4 月 27 日欧洲议会和理事会的法规（EU）2016/679（“***GDPR***”），以及已实施类似 GDPR 的数据保护原则，并已获欧洲委员会承认提供足够程度保护的任何其他国家的法律法规（视属何情况而定）。
   (e) ***“SaaS 环境”***指客户在使用“SaaS”软件时获得访问权限的系统。
   (f) ***“标准合同条款”***指由欧盟委员会公布的未经改动的标准合同条款（载于 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914），参考 2021/914 或其任何后续最终版本应自动适用。
   (g) “***分处理者***”指提供商关联公司和与 SaaS 软件有关的提供商或提供商关联公司聘请并根据本附录处理个人数据的第三方。

2. **SaaS 条款。**
   (a) **数据。**客户可以在 SaaS 环境中存储数据。客户全权负责收集、输入、验证和更新存储在 SaaS 环境中的所有客户数据。客户陈述并保证，其已获得在“客户”或其相关关联公司所在国家内外使用和转移所有“客户”和/或第三方数据所需的所有权利、授权和同意（包括提供充分的披露，并从客户的雇员、客户、代理和承包商处获得合法的充分同意或授权）。如果客户将数据传输到供 SaaS 软件访问的第三方网站或其他位置，则客户将被视为已同意和/或授权由提供商进行访问。
   (b) **行为。**在使用 SaaS 软件时，用户不得：(i) 违反适用法律使用“SaaS”软件，特别是用户不得传输任何非法的或侵犯第三方任何知识产权的内容或数据；(ii) 规避或危害 SaaS 软件的运行或安全，或试图探测、扫描或测试 SaaS 软件、SaaS 环境或提供商或提供商的任何客户或供应商的系统、帐户或网络的漏洞；(iii) 发送未经请求的批量或商业信息；或 (iv) 故意散布蠕虫、特洛伊木马、病毒、损坏的文件或任何类似物品。客户应配合提供商对 SaaS 环境中断、安全问题和任何涉嫌违反本条内容的行为进行的合理调查，并应自费为提供商及其关联公司进行辩护，应对第三方声称因客户违反本条任何规定而对该第三方造成损害的任何索赔、诉讼或行动（***“第三方索赔”***）。此外，客户应支付与第三方索赔有关的任何判决或和解，以及提供商应对第三方索赔时产生的费用。
   (c) **暂停。**如果继续使用 SaaS 软件有足够的可能性会导致对 SaaS 软件、其他提供商客户或第三方权利的损害，从而必须立即采取行动以避免损害，或者客户违反上述行为，则提供商可以暂时限制或暂停客户对 SaaS 软件的访问，以防止损害。提供商应就有关限制或暂停的事项通知客户，不得无故延迟。如果情况允许，应提前以书面方式或通过电子邮件通知客户。提供商应根据具体情况在合理的时间和范围内限制暂停访问或限制访问，并在导致暂停访问或限制访问的问题解决后，立即恢复访问，并就恢复访问一事通知客户。
   (d) **可用性。**提供商将作出商业上合理的努力，使 SaaS 软件能够每周 7 天、每天 24 小时可用，但定期维护、安装更新、超出提供商合理控制范围的因素、客户未能满足提供商向客户传达的任何最低系统要求，以及客户违反本协议或本附录而影响 SaaS 软件可用性的任何情况除外。对于任何计划内的维修，提供商应向客户提供合理的预先通知。

3. **SaaS 安全。**
   (a) **一般安全政策**。提供商认真对待客户数据（包括个人数据）的安全性和保密性。提供商致力于维护和改进其信息安全实践，并把对安全风险的暴露降到最低。为此，有关提供商信息安全实践、数据泄漏响应政策、技术和组织措施以及软件开发安全实践的详细信息可在以下网站获取：www.oneidentity.com/legal/security.aspx（统称“安全网站”）。客户同意，提供商可以修改其安全网站，但前提是不显著降低所提供的整体保护水平。
   (b) **数据中心的安全性和位置**。提供商使用商业托管提供商来托管 SaaS 环境。SaaS 环境适用的托管提供商将被标识为分处理者。提供商将只使用符合行业标准安全要求并对其安全程序进行过独立评估（如服务组织控制 (SOC) 审计、SSAE 18 审计和/或 ISO 认证）的托管提供商。提供商应提供托管提供商的认证的复印件。在初始配置 SaaS 软件时，将向客户提供选择托管 SaaS 环境的地理区域的选项。一经选择，提供商不得在未经客户事先同意的情况下更改地理区域。
   (c) **数据保密。**提供商将只使用已获知在本协议项下被视为“机密”的数据（包括客户个人数据）具有的机密性质的人员来处理任何此类数据。提供商将要求根据本附录和本协议支持 SaaS 软件的所有提供商人员签署与数据（包括客户个人数据）保护有关的保密协议。提供商应确保该保密义务在任何此类人员的雇佣关系终止后继续存在。提供商将定期对有权限访问数据（包括客户个人数据）的个人进行数据安全和数据私隐要求及原则方面的培训。
   (d) **有限的处理和披露。**提供商可以在以下情况下处理和披露数据，包括客户的个人数据：(i) 为符合本协议的目的并根据本附录的条款向关联实体披露，或 (ii) 根据处理者所遵守的欧盟或成员国法律的要求进行处理和披

露，包括回应传票、司法或行政命令；在此类情况下，处理者应在处理和披露前将该法律要求告知控制者，除非该法律以保护公共利益为由禁止披露该等信息。

4. **合作。**除法律或合同禁止的情况外，应客户要求，提供商应合理地与客户就数据主体的要求进行合作，并在提供商收到根据本协议提供数据的数据主体的关于 (a) 要求查阅、更正、修改或删除该数据主体个人数据的权利；(b) 反对根据本协议处理其个人数据；和/或 (c) 希望行使其在 GDPR 下的可携带性或被遗忘的权利要求时，及时通知客户。提供商不得在未经客户事先书面批准的情况下回应此类数据当事人的要求，除非是为了确认此类数据主体的要求是向客户提出的。

5. **审计权利。**应客户要求，并在遵守本协议保密义务的前提下，提供商应向客户提供合理必要的信息，以证明其遵守本附录项下的义务，并允许和协助审计，包括由客户（或其第三方审计师）自费就提供商处理其个人数据的活动开展检查。

6. **国际数据传输。**如果 SaaS 软件和相关服务的提供涉及将个人数据（受 GDPR 或适用数据保护法约束）传输到未被欧盟委员会根据 GDPR 第 45 条确认为提供充分数据保护的一个或多个国家（“***第三国***”），并且 GDPR 或适用的数据保护法律规定的任何所需的充分数据保护手段可以通过签订标准合同条款予以满足，则提供商（或代表其行事的提供商关联公司）已经与作为数据输入者的每个分处理者签订标准合同条款。标准合同条款的模块 3（处理者对处理者）应适用于该等传输。就与该等传输有关的所有目的而言，本附录也应构成标准合同条款的附录。

7. **分处理者。**
   (a) 客户确认并同意，在提供 SaaS 软件时，提供商可聘请分处理者。
   (b) 提供商应按照本附录的规定以及客户与提供商之间的说明，与分处理者签署适当的书面协议。本附录中规定的相同数据保护义务应施加于任何分处理者。
   (c) 如果提供商聘请的分处理者造成对本附录的任何违反，则提供商应承担责任。
   (d) 提供商在 https://support.oneidentity.com/subprocessor 维护关于每个产品的分处理者的名单。提供商应在授权任何新分处理者访问个人数据前至少十 (10) 个工作日更新分处理者名单，并向“客户”提供获取关于该更新的通知的机制。如果提供商是处理者，则适用以下条款：
      (i) 如果客户不批准新的分处理者，则客户可以通过在通知期结束前提供书面终止通知（其中包括不予批准的理由说明），从而终止对受影响的 SaaS 软件的任何订阅，而不受到惩罚。
      (ii) 如上所述终止后，客户仍有义务支付任何订单或其他合同义务下要求支付的所有款项，并无权从合作伙伴和/或提供商处获得任何退款。

8. **个人数据泄露通知。**除安全网站规定的义务外，提供商在知晓任何个人数据泄露后，应毫不迟延地通知客户，并提供其所拥有的合理信息以协助客户根据数据保护法的规定履行其报告个人数据泄露的义务。提供商可以在信息可用时分阶段提供这些信息。提供商同意作出善意努力，识别个人数据遭到泄露的原因，并采取提供商认为必要和合理的措施，以便在提供商合理控制的范围内，对个人数据遭到泄露的原因进行补救。

9. **归还和删除客户个人数据。**
   (a) 客户应在 SaaS 期限届满或因任何原因提前终止前至少 30（三十）天通知提供商，要求将客户个人数据归还给客户或将其删除。如被要求归还客户个人数据，提供商应在适用法律允许的范围内以常用格式归还客户个人数据。
   (b) 除非客户要求归还客户个人数据，否则，在 SaaS 期限终止后，提供商应删除其持有的客户个人数据，但为了提供商使能够遵守法律或监管命令或要求的必要情况除外。

10. **数据保护影响评估。**提供商应向客户提供合理的合作和必要的协助，以履行客户在 GDPR 下的义务，从而对客户使用 SaaS 软件的情况进行数据保护影响评估。

附录的
附件

本附件是附录的一部分。

附件 I

A. 相关方名单

作为控制者的客户与作为处理者的提供商之间的协议包含对所有必要信息的描述，如：

- 姓名、地址、联系人姓名、
- 职位和联系方式、
- 与根据本条款传输数据有关的活动，以及
- 签名和日期。

B. 处理描述

1. 其个人数据被处理的数据主体的类别

除客户另有规定外，被处理的个人数据涉及以下类别的数据主体：员工、承包商、业务合作伙伴或在 SaaS 软件中存储个人数据的其他个人。

2. 被处理的个人数据的类别

客户根据其对 SaaS 软件的使用决定数据的类别。被处理的个人数据通常涉及以下数据类别：

- 与客户员工或其他第三方（其个人信息由客户或代表客户提供）有关的雇佣详细信息（可能包括公司名称和地址、职位、级别、人口统计资料和位置数据）；
- 与客户系统有关的系统信息，或由客户提供给提供商的系统信息，以及与根据本协议购买的服务有关的系统信息，以及提供 SaaS 软件所需的系统信息（可能包括用户 ID 和密码、计算机和域名、IP 地址、GUID 编号或正在使用的计算机或其他设备的位置）。

根据本附录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该等业务合作伙伴有关的其他个人。

3. 被处理的敏感数据（如适用）

特殊类别的个人数据（根据 GDPR 第 9 条的定义）不得由客户提供，除非根据具体情况确定，并且仅在双方同意 SaaS 软件将涵盖该等特殊类别数据的情况下提供。

4. 处理频率（例如，数据是一次性处理或连续处理）。

在使用 SaaS 软件期间持续进行处理。

5. 处理性质

提供客户购买的服务。

6. 数据传输和进一步处理的目的

提供商处理的客户个人数据须进行以下基本处理活动：

- 使用客户个人数据以根据本协议提供对 SaaS 软件的访问和利益，并应客户要求及根据客户的具体要求，在适当情况下向客户提供协助和技术支持，并且一切均按照下面所述的说明进行；
- 在数据中心（多租户架构）存储客户个人数据；
- 对存储在 SaaS 软件中的客户个人数据进行备份和恢复；
- 计算机处理客户个人数据，包括数据传送、数据检索、数据访问。
- 与客户的用户进行沟通；
- 发布、开发和上传对 SaaS 软件的任何修复或升级；
- 提供网络访问权限以允许传输个人数据；
- 监控、排除故障和管理底层 SaaS 软件基础设施和数据库；
- 安全监控、基于网络的入侵检测支持、渗透测试；
- 根据本协议和本附录，执行客户的指示；以及
- 必要时，根据下面所述的说明，对数据当事人的请求和要求作出适当的回应和处理。

提供商可将匿名化数据（不是客户个人数据，但可能源自客户个人数据）用于与产品改进和新提供商产品及服务开发相关的目的。

关于产品的用途、如何处理个人数据以及数据存储位置的更多详细信息，将在适用的产品文件和安全指南中提供。

7. 个人数据的保留期限或用于确定该期限的标准（如果无法保留）

上述个人数据应在客户根据本协议使用 SaaS 软件期间进行处理，并遵守本附录第 9 条的规定。

8. 对于向（分）处理者的传输，还需说明处理的事项、性质和期限

就标准合同条款而言，向分处理者的传输应以本附录规定的相同方式进行。

9. 说明，客户和提供商的承诺。

本协议、本附录和提供商的任何相关 SaaS 软件文档中的任何处理描述均应被客户和提供商视为说明。提供商应按照客户就客户个人数据提出的书面和文件化的说明行事，除非提供商认为此类说明 (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 SaaS 软件进行重大变更，和/或 (3) 不符合本协议条款或提供商关于在本附录项下出售的 SaaS 软件的文件。在任何此类情况下，提供商应立即就其无法遵守此类说明通知客户。

附件 II - 关于技术和组织措施的声明

提供商在根据本附录处理客户个人数据时，将采用安全网站（定义见附录第 3(a) 条）上规定的适当技术和组织措施。客户同意，提供商可以改变为保护客户个人数据而采取的措施，前提是该措施不显著降低本附录中约定的数据保护的总体水平。