客户数据处理附录

当 HP 为了提供 HP 与客户之间签订的适用协议（以下简称“服务协议”）中约定的服务而处理客户个人数据时，本数据处理附录（以下简称“DPA”）和适用附件将适用。本附录中未明确定义的大写、粗体或斜体术语应具有服务协议中规定的含义。如果服务协议中与个人数据处理相关的条款与本 DPA 发生冲突，应以本 DPA 为准。

1 定义

1.1 **“CCPA”**指《2018 年加州消费者隐私方案》，不时修订的《加州隐私法案》（“CPRA”）、《加州民法典 1798.100》等，以及不时修订和补充的任何相关法规；

1.2 **“客户”**指 HP 服务的最终用户客户；

1.3 **“客户个人数据”**指客户作为数据控制者并且在服务提供过程中由作为数据处理者的 HP 或其次级处理者处理的个人数据；

1.4 **“数据控制者”**指单独或与其他实体共同决定处理个人数据的目的和方法的自然人或法人、公共机关、代理商或任何其他实体，包括依据 CCPA 定义的“企业”；

1.5 **“数据处理者”**指任何以数据控制者名义，或依照另一个以数据控制者名义行事的数据处理者的指示处理个人数据的任何自然人或法人、公共机关、代理商或任何其他实体；

1.6 **“数据保护和隐私法律”**指相关司法管辖区可能存在的与个人数据和隐私的处理、安全、保护和保留相关的所有现行和未来的适用法律和法规，包括但不限于 CCPA、GDPR、PIPL、中华人民共和国保护个人信息的任何适用法规和国家标准、《英国通用数据保护条例》、《英国 2018 年数据保护法》、电子通信领域关于个人数据处理和隐私保护的 2002/58/EC 指令、执行上述指令的任何国家法律或法规，以及挪威、冰岛、列支敦士登和瑞士的任何数据保护法及对此类法律和法规的任何修订或替代；

1.7 **“数据主体”**应具有适用的数据保护和隐私法律赋予“数据主体”一词的含义，并且至少应包括与个人数据相关的所有已识别或可识别的自然人；

1.8 **“EU”**指“欧盟”及该政治联盟的全体成员国；

1.9 **“欧洲国家/地区”**是指欧盟成员国、挪威、冰岛、列支敦士登和瑞士；

1.10 **“欧美批准的适足性机制”**指根据适用的数据保护和隐私法律批准的将个人数据从欧洲国家/地区转移到美国的任何适足性机制；

1.11 **“欧盟标准合同条款”**指 2021 年 6 月 4 日委员会实施决议（EU）2021/914 或后续针对瑞士进行任何必要修订的决议中预见的将个人数据从数据控制者转移到数据处理者以及从数据处理者转移到数据处理者的欧盟标准合同条款；

1.12 **“GDPR”**指在处理个人数据和此类数据的自由移动方面对自然人提供保护的通用数据保护条例 (EU) 2016/679；

1.13 **“HP Group”**指 HP Inc.（1501 Page Mill Road, Palo Alto, CA 94304）及其拥有多数股权和控制权的所有子公司，无论其注册成立或运营所在的司法管辖区为何；

1.14 **“个人数据”**指与已识别或可识别身份的个人相关的任何信息，或者适用的数据保护和隐私法律另行定义的任何信息。可识别身份个人指可以直接或间接被识别身份的个人，特别是通过参考其姓名、身份证号码、位置数据、在线标识符等标识符，或参考一个或多个特定于该个人的身体、生理、遗传、心理、经济、文化或社会身份的因素而被识别的个人；

1.15 **“个人数据事故”**应具有适用的数据保护和隐私法律对“安全事故”、“安全漏洞”或“个人数据泄露”术语所赋予的含义，但是应包括 HP 意识到客户个人数据已经被或可能被未经授权的个人以未经授权的方式访问、披露、修改、丢失、销毁或使用的任何情况；

1.16 **“PIPL”**指《中华人民共和国个人信息保护法》；

1.17 **“处理”**、**“正在处理”**或**“已处理”**指对个人数据执行的任何操作或一套操作，不论是否以自动手段执行，包括但不限于访问、收集、记录、组织、构造、保留、储存、改编或更改、检索、查阅、使用、披露、通过传输方式披露、传播或提供、对齐、合并、限制、清除和销毁个人数据，以及适用数据保护和隐私法律中的任何同等定义，但此等定义应凌驾于本定义之上；

1.18 **“对处理者有约束力的公司规则”**指针对数据处理者的有约束力的公司规则，这些规则已获得欧盟特定隐私权机关的批准；

1.19 **“相关国家/地区”**指除欧洲国家和根据 GDPR 第 45 条或瑞士法律或英国同等法律规定具有适足性裁决的其他国家/地区以外的所有国家/地区，包括美国，只要任何此类适足性裁决仅限于要求使用欧美批准的适足性机制；

1.20 **“销售”**应具有 CCPA 中规定的含义；

1.21 **“共享”**应具有 CCPA 中规定的含义；

1.22 **“服务”**指 HP 根据服务协议提供的服务，包括产品和支持；

1.23 **“服务协议”**指 HP 与客户之间就从 HP 购买服务而签订的协议；以及

1.24 **“次级处理者”**指任何以代表数据控制者行事的数据处理者的名义处理个人数据的任何自然人或法人、公共机关、代理商或任何其他实体。

2 适用范围和法律遵守

2.1 本 DPA 适用于 HP 在提供服务时对客户个人数据的处理，以及当 HP 代表作为数据控制者的客户以数据处理者身份行事时。所有各方均应遵守适用的数据保护和隐私法，第 2.1 节中的任何内容均不会修改适用于任何一方根据缔约方协议使用或以其他方式处理个人数据的权利的任何限制。

2.2 本 DPA 的附件 1 中列出了数据主体的类别、处理的客户个人数据类型和处理目的。HP 应在服务协议有效期内（或适用法律要求的更长时间内）处理客户的个人数据。

2.3 客户在使用 HP 的服务时，应全权负责遵守所有适用的数据保护和隐私法律，以确保 HP 根据服务处理的客户个人数据的准确性、质量和合法性。客户应进一步确保其向 HP 提供的有关客户个人数据处理的指示将遵守所有适用的数据保护和隐私法律，并且不得使 HP 违反其在适用数据保护和隐私法律下的义务。

2.4 如果客户使用服务来处理本 DPA 未明确涵盖的任何类别的个人数据，客户应自行承担风险，HP 不对与此类使用相关的任何潜在不合规情况负责。

2.5 如果 HP 向客户披露任何 HP 员工个人数据，或者 HP 员工直接向客户提供个人数据，客户通过处理这些数据来管理其对服务的使用，此时客户应根据其隐私政策和适用的数据保护和隐私法律处理该个人数据。只有在出于合同管理、服务管理或者客户的合理背景筛查验证或安全目的的合法情况下，HP 才应进行此类披露。

3 数据处理者的义务

3.1 尽管服务协议中有任何相反规定，但就客户个人数据而言，HP 仍应：

3.1.1 仅根据客户的书面指示（服务协议中规定或缔约方另行约定的具体指示或一般性指示）处理客户个人数据。在不限制上述内容一般性的情况下，在 CCPA 适用于客户

个人数据的范围内，HP 不得以不符合 CCPA 的方式：出售或共享客户个人数据；不得出于执行服务的特定商业目的或以其他方式履行协议义务的目的（其目的属于缔约方直接业务关系范围）之外的任何目的保留、使用或披露客户个人数据。或将客户个人数据与来自任何其他来源的个人数据相结合。在 CPPA 适用于客户个人数据的范围内，如果 HP 无法履行 CCPA 规定的与客户个人数据相关的义务，则 HP 应通知客户。尽管有上述规定，HP 仍可根据适用法律的要求处理客户个人数据。在这种情况下，除非法律禁止，否则 HP 应在 HP 处理数据之前采取合理的措施将此类要求告知客户；

3.1.2 确保只有在保护和处理个人数据方面接受过适当培训并且肯定会尊重客户个人数据机密性的授权人员才能访问这些数据；

3.1.3 实施适当的技术和组织措施，以防止出现未经授权或非法的破坏、丢失、篡改、未经授权的披露或访问客户个人数据。这些措施应适用于客户个人数据的任何未经授权或非法处理、意外丢失、破坏、损坏或被盗可能导致的损害，并考虑到要保护的客户个人数据的性质；

3.1.4 不得无故拖延，并在法律允许的范围内，将数据主体试图根据适用数据保护和隐私法律行使其权利而提出的任何请求通知客户，并在客户发出书面请求并支付费用的情况下，根据处理的性质，通过实施适当的技术和组织措施，在可能的情况下协助客户履行响应此类请求的义务；

3.1.5 在客户发出书面请求并支付费用的情况下，应根据处理的性质和 HP 可获得的信息，协助客户履行其在 GDPR 第 32 至 36 条或适用数据保护和隐私法律下同等条款下的义务，协助客户履行客户在 PIPL 下的义务； 以及 CPRA 规定的义务；

3.1.6 按照客户发出的书面要求，在服务结束后删除或向客户归还任何客户个人数据，除非适用法律要求存储客户个人数据，否则由 HP 在删除或归还客户个人数据之间进行选择。

4 次级处理

4.1 客户授权 HP 为提供服务或履行附件 1 的“处理活动”一节中确定的其他目的，将客户个人数据转给 HP Group 成员和作为次级处理者的第三方或者向其提供客户个人数据的访问权（并允许次级处理者依照第 4.1 条的规定执行相同行动）。HP 应继续对其次级处理者遵守本 DPA 义务的行为负责。HP 应确保 HP 将客户个人数据转给的任何次级处理者与 HP

签订书面协议，要求次级处理者遵守不低于本 DPA 中规定的保护性条款。HP 应向客户提供服务协议所涵盖服务的最新次级处理者列表。

4.2 HP 可以在没有正当理由的情况下随时指定新的次级处理者，但必须提前十（10）天通知客户并且客户在该期限内没有正当合理地反对此类变更。正当合理的反对必须包含与次级处理者不遵守适用的数据保护和隐私法律有关的合理且有据可查的理由。如果 HP 有理由相信此类反对正当合理，则 HP 应避免在处理客户个人数据时使用此类次级处理者。在这种情况下，HP 应尽合理的努力（i）向客户提供 HP 服务变更，或（ii）建议客户变更服务的配置或使用方式，以避免被反对的次级处理者处理客户个人数据。如果 HP 无法在九十（90）天内的合理期限内提供此类变更，客户可以通过向 HP 提供书面通知，终止 HP 在不使用受到反对的次级处理者情况下无法提供的服务。如果 PIPL 适用，HP 应请求客户事先授权指定新的次级处理者。客户必须在十（10）天内回应 HP 的请求。如果客户反对变更，HP 应避免使用此类次级处理者处理客户个人数据。在这种情况下，HP 应尽合理的努力（i）向客户提供 HP 服务变更，或（ii）建议客户变更服务的配置或使用方式，以避免被反对的次级处理者处理客户个人数据。如果 HP 无法在九十（90）天内的合理期限内提供此类变更，客户可以通过向 HP 提供书面通知，终止 HP 在不使用受到反对的次级处理者情况下无法提供的服务。

5 个人数据事故

5.1 如果 HP 发现涉及客户个人数据的任何个人数据事故，HP 应立即通知客户，不得无故拖延，并在合理期限内采取客户合理要求的措施来补救个人数据事故，并提供客户可能合理要求的进一步信息。HP 有权针对根据本附录第 5.1 条提供的协助收取管理费，除非客户证明由于 HP 未能遵守本 DPA 才需要此类协助。

6 客户个人数据的跨国转移

6.1 HP 可以将客户个人数据转移到最初收集数据的国家/地区之外，但是所提供的服务必须需要此类转移，并且此类转移符合适用的数据保护和隐私法律，包括但不限于完成数据保护和隐私法律要求的任何事先评估。

6.2 欧洲特定条款

6.2.1 对于将客户个人数据从欧洲国家/地区转移到相关国家/地区的情况，HP 提供下列转移机制，这些转移机制应按照第 6.2.2 条规定的优先顺序用于任何此类转移，并符合适用的数据保护和隐私法律：

6.2.1.1 如适用，对 HP 作为处理者有约束力的公司规则：HP 已采用对处理者有约束力的公司规则，且该规则已涵盖所处理的客户个人数据。HP 应维护此类对 HP 处理者有约束力的公司规则，并在对 HP 处理者有约束力的公司规则不再是有效的转移机制时立即通知客户。单击以下链接可了解对 HP 处理者有约束力的公司规则：https://www.hp.com/uk-en/bcr-pages.html?jumpid=in_R11928_/us/en/corp/privacy-central/binding-corporate-rules。

6.2.1.2 欧美批准的适足性机制；依据欧美批准的适足性机制进行的任何转移都必须按照该机制的规则进行，包括在需要时对位于美利坚合众国的将出于服务目的处理客户个人数据的 HP 附属公司进行注册或认证。

6.2.1.3 欧盟标准合同条款，即数据控制者转移至数据处理者（附件 2）或数据处理者转移至数据处理者（附件 3）（如适用）。

6.2.2 如果服务由多个转移机制覆盖，则客户个人数据的转移将按照以下优先顺序使用单一转移机制：1）对 HP 处理者有约束力的公司规则；2）欧美批准的适足性机制；3）欧盟标准合同条款。

6.3 其他规定的转移机制

6.3.1 在不影响上述第 6.1 条规定普遍性的情况下，缔约方同意使用附件 4（英国）和 5（阿根廷）中提到的转移机制将个人数据从有关国家/地区转移到相关国家/地区。

6.4 中国特定条款

6.4.1 如果 HP 将在中国收集或生成的任何客户个人数据从中华人民共和国转移到中国以外的国家或地区，HP 提供下列转移机制：

6.4.1.1 安全评估：如果国家互联网信息办公室（CAC）进行的安全评估适用于客户个人数据的转移，则客户应申请安全评估并遵守相关要求，HP 应在客户要求且缔约方视为必要时提供协助。

6.4.1.2 标准合同（附件 6）：如果安全评估不适用，客户必须与客户个人数据的接收者签订 CAC 发布的标准合同。

6.4.2 如果数据控制者将中华人民共和国的个人数据转移至中国以外国家或地区的数据处理者，数据控制者应负责征得数据主体的同意。

7 审计

7.1 在客户发出书面请求时，HP 应向客户提供所有必要信息，以证明履行了适用数据保护和隐私法律规定的义务，但 HP 没有义务提供商业机密信息。HP 应在不超过每年一次且费用由客户承担的情况下，进一步允许并协助客户或其授权的第三方审计人员（不得是 HP 的竞争对手）进行审计和检查。任何此类审计的范围，包括保密条件，应在开始前由缔约方共同商定。 为确保客户有权采取合理且适当的措施来停止和补救 HP 未经授权使用客户个人数据，缔约方将确认并制定相互认可的必要补救计划，以解决任何涉及此类未经授权使用客户个人数据的任何审核结果。

附件列表

附件 1——处理详情
附件 2——欧盟标准合同条款（数据控制者转移至数据处理者）
附件 3——欧盟标准合同条款（数据处理者转移至数据处理者）
附件 4——国际数据转移协议（IDTA）（英国）
附件 5——标准合同条款（阿根廷）
附件 6——个人信息跨境转移标准合同（中国）

附件 1

处理详情

HP 可能会定期更新此附件 1，以反映处理活动的变更。

数据主体的类别

- 客户的员工、客户代理和分包商。

个人数据的类型

HP 在其提供服务时处理的客户个人数据由作为数据控制者的客户根据适用的工作说明书和/或采购/变更单确定和控制，但可能包括以下示例：

- *联系数据*——例如姓名、工作或个人电话号码、工作或个人电子邮件地址和办公地址；
- *安全凭据数据*——例如员工身份或名牌编号；
- *产品使用数据*——例如打印的页面、发起打印作业的设备类型、打印模式、使用的介质、墨水或碳粉品牌、打印的文件类型（.pdf、.jpg 等）、用于打印的应用程序（Word、Excel、Adobe Photoshop 等）、文件大小、时间戳以及打印机耗材的使用和状态；
- *性能数据*——使用的打印事件、功能和警报，例如“墨水不足”警告、使用照片卡、传真、扫描、嵌入式 Web 服务器，以及依产品而异的其他技术信息；
- *设备数据*——有关计算机、打印机和/或设备的信息，例如操作系统、内存量、地理区域、语言、时区、型号、首次启动日期、设备使用年数、设备制造日期、浏览器版本、计算机制造商、连接端口、保修状态、唯一设备标识符、广告标识符和依产品而异的其他技术信息；
- *应用程序数据*——与 HP 应用程序相关的信息，例如位置、语言、软件版本、数据共享选择和更新详情；以及
- 数据主体面对面、在线或通过电话或邮件与服务中心、帮助台或其他客户支持渠道互动时提供的其他个人数据，以促进 HP 服务的交付和响应客户和/或数据主体的查询；或（ii）HP 收到的设备上的个人数据。

处理活动

HP 将使用根据服务协议处理的客户个人数据来管理与客户的关系并向客户提供服务。HP 可能会处理客户个人数据以执行以下操作：

- 提供系列管理服务，例如托管打印服务和设备即服务；

- 维护准确的联系和注册数据，以提供全面的支持和维护服务，包括金牌服务和延长保修支持以及辅助维修和退货；
- 为访问门户网站提供便利，确保能查看和管理数据、管理设备、订购和完成产品或服务订单，以便管理帐户和安排发货和交付；
- 改进产品、解决方案、服务和支持的性能和运行，包括保修支持以及及时的固件和软件更新和警报，以确保设备或服务的持续运行；
- 向客户提供有关服务的管理沟通。管理沟通的示例可能包括对客户查询或请求的回应、产品使用或性能报告、服务完成或保修相关的沟通、安全召回通知或与合并、收购或剥离相关的适用公司更新；
- 维护 HP 网站、产品、功能和服务的完整性和安全性，防止和检测可能危及客户信息的安全威胁、欺诈或其他犯罪或恶意活动；
- 验证客户身份，包括在提供 HP 远程维护服务时要求提供来电者姓名和员工身份证明或名牌号码；
- 遵守适用的法律、法规、法院指令、政府和执法部门的要求，保护员工和其他客户并解决纠纷；以及
- 提供量身定制的体验，个性化服务和沟通并提出建议；以及
- 擦除退回给 HP 的设备中的数据。

附件 2

欧盟标准合同条款（数据控制者转移至数据处理者）

第一节

第 1 条

目的和适用范围

(a) 本标准合同条款旨在确保在将个人数据转移到第三国时符合欧洲议会的第（EU）2016/679 号条例和理事会 2016 年 4 月 27 日关于在处理个人数据方面和保护自然人以及此类数据的自由流动的要求（通用数据保护条例）。

(b) 缔约方：

(i) 转移个人数据的自然人或法人、公共当局、机构或其他团体（以下简称“实体”），如附件 I.A 中所列（以下简称“数据出口方”），以及

(ii) 直接或通过另一个同为本条款缔约方的中间实体，从数据出口方接收个人数据（如附件 I.A 中所列）的第三国实体，（以下简称“数据进口方”）

已就这些标准合同条款（以下简称：“条款”）达成一致。

(c) 本条款适用于个人数据的转移，如附件 I.B 中规定。

(d) 本条款的附录包含条款中提及的附件，是本条款不可或缺的部分。

第 2 条

条款的效力和不可更改性

(a) 本条款规定了适当的保障措施，包括根据第 (EU) 2016/679 号条例的第 46(1) 条和第 46(2) (c) 条的规定可执行的数据主体权利和有效的法律救济措施以及从控制者向处理者和/或从处理者到处理者的数据转移，标准合同条款应符合第 (EU) 2016/679 号条例的第 28(7) 条的规定，除非选择适当的模块或在附录中添加或更新信息外，均不得修改。这并不妨碍缔约方将本条款中规定的标准合同条款纳入更广泛的合同中和/或添加其他条款或额外保障措施，但它们不得直接或间接地与本条款相矛盾或损害数据主体的基本权利或自由。

(b) 本条款不影响数据出口方根据第 (EU) 2016/679 号条例所承担的义务。

第 3 条

第三方受益人

(a) 数据主体可以作为第三方受益人，可对数据出口方和/或数据进口方援引和执行本条款，但以下情况除外：

(i) 第 1、2、3、6、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) (a) 款不影响数据主体根据第 (EU) 2016/679 号条例所享有的权利。

第 4 条

释义

(a) 如果本条款使用第 (EU) 2016/679 号条例中定义的术语，则这些术语应与该条例中的含义相同。

(b) 本条款应根据第 (EU) 2016/679 号条例的规定进行理解和解释。

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

第 5 条

等级制度

如果本条款与在本条款达成一致或签订之时已存在的缔约方相关协议的规定发生冲突，则以本条款为准。

第 6 条

转移说明

附件 I.B 中详细说明了转移的详细信息，尤其是转移的个人数据的类别和转移的目的。

第二节——各方的义务

第 8 条

数据保护保障措施

数据出口方保证已尽合理努力确定数据进口方能够通过实施适当的技术和组织措施来履行其在本条款下的义务。

8.1 指示

(a) 数据进口方应仅根据数据出口方的书面指示处理个人数据。数据出口方可以在整个合同期间发出此类指示。

(b) 数据进口方如不能按照指示执行，应立即通知数据出口方。

8.2 目的限制

除非数据出口方有进一步的指示，否则数据进口方应仅出于转移的特定目的处理个人数据，如附件 I.B 中所述。

8.3 透明度

数据出口方必须应要求免费向数据主体提供本条款的副本，包括缔约方编写的附录。在保护商业机密或其他机密信息（包括附件 II 中描述的措施和个人数据）的必要范围内，数据出口方可以在共享副本之前屏蔽本条款的附录的部分文本，但应提供有意义的摘要，以帮助数据主体了解其内容或行使其权利。缔约方应按要求在不泄露修订信息的范围内尽可能向数据主体提供修订的理由。本条款不影响数据出口方根据第 (EU) 2016/679 号条例第 13 条和第 14 条所承担的义务。

8.4 准确度

如果数据进口方发现其收到的个人数据不准确或已过时，应立即通知数据出口方。在这种情况下，数据进口方应配合数据出口方对数据进行删除或更正。

8.5 处理期限和数据的删除或归还

数据进口方只能在附件 I.B 中指定的期限内处理数据。在终止提供处理服务时，数据进口方应根据数据出口方的选择，删除代表数据出口方处理的所有个人数据，并向数据出口方证明其已删除此类数据，或者将其代表数据出口方处理的个人数据归还给数据出口方并删除现有副本。在删除或归还数据之前，数据进口方应继续确保遵守本条款。如果适用于数据进口方的当地法律禁止归还或删除个人数据，则数据进口方保证将继续确保遵守本条款，并且只会在当前法律要求的范围和期限内处理数据。这不影响第 14 条，特别是第

14(e) 条规定的要求，即数据进口方在整个合同期间都有义务在合理认为其受到或已经受到与第 14(a) 条的要求有冲突的法律或惯例约束时通知数据出口方。

8.6 处理的安全性

(a) 数据进口方和传输过程中的数据出口方应实施适当的技术和组织措施以确保数据的安全，包括防止安全漏洞，导致的意外或非法破坏、丢失、篡改、未经授权的披露或获取该数据（以下简称“个人数据泄露”）。在评估适当的安全水平时，缔约方应适当考虑最新技术水平、实施成本及处理的性质、范围、背景和目的以及处理给数据主体带来的风险。缔约方应特别考虑在不妨碍实现处理目的的情况下包括在传输过程中对数据进行加密或假名化处理。在假名化的情况下，用于将个人数据还原到特定数据主体的附加信息应尽可能由数据出口方独家控制。在履行本款规定的义务时，数据进口方至少应实施附件 II 中规定的技术和组织措施。数据进口方应进行定期检查，以确保这些措施继续提供适当的安全水平。

(b) 数据进口方只有在合同的实施、管理和监控绝对必要的范围内，才能授予其人员访问个人数据的权限，并且应确保被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) 如果数据进口方根据本条款处理的个人数据发生个人数据泄露，数据进口方应采取适当措施解决该泄露事件，包括减轻其不利影响的措施。数据进口方还应在知悉违规行为后立即通知数据出口方，不得无故拖延。此类通知应包含可以获取更多信息的联络人的详细信息、对泄露事件性质的描述（在可能的情况下，包括相关的数据主体和个人数据记录的类别和大致数量）、可能的后果以及为解决泄露事件而采取或建议采取的措施，应包括在适当情况下减轻其可能的不利影响而采取的措施。在不可能同时提供所有信息的情况下，初始通知应包含当时可获得的信息，并且在获得进一步信息后应及时提供，不得无故拖延。

(d) 数据进口方应与数据出口方合作并协助数据出口方履行其根据第（EU）2016/679 号条例所承担的义务，特别是在结合考虑处理的性质和数据进口方可获得的信息后通知主管监管机构和受影响的数据主体。

8.7 敏感数据

如果转移的数据涉及包含种族或族裔血统、政治观点、宗教或哲学信仰或工会成员身份的个人数据、能够唯一识别自然人身份的基因数据或生物特征数据、有关健康或个人性生活或性取向的数据或与刑事定罪和犯罪有关的数据（以下简称“敏感数据”），数据进口方应当应用附件 I.B 中描述的具体限制和/或其他保障措施。

8.8 后续转移

数据进口方应仅根据数据出口方的书面指示向第三方披露个人数据。此外，数据只能披露给位于欧盟以外的在适当模块下受本条款约束或同意受本条款约束的第三方（与数据进口方在同一国家/地区或在另一个第三国，以下简称“后续转移”），或者：

(a) 后续转移指转移到受益于根据第 (EU) 2016/679 号条例第 45 条（涵盖后续转移）作出的充分性决定的国家或地区；

(b) 第三方根据第 (EU) 2016/679 号条例的第 46 条或第 47 条规定确保为有关处理提供适当的保障措施；

(c) 后续转移是指在特定的行政、监管或司法程序中建立、行使或维护法律诉求所必需的；或

(d) 为了保护数据主体或其他自然人的切身利益，有必要进行后续转移。

对于任何后续转移，数据进口方都必须遵守本条款下的所有其他保障措施，特别是目的限制。

8.9 文档记录和合规性

(a) 数据进口方应及时、充分地处理数据出口方就根据本条款进行的处理提出的询问。

(b) 缔约方应能够证明遵守本条款。特别是，数据进口方应保留代表数据出口方进行的处理活动有关的相应文件。

(c) 数据进口方应向数据出口方提供所有必要信息，以证明其遵守本条款中规定的义务，并应数据出口方的要求，允许并协助以合理的时间间隔或在有不合规迹象的情况下对本条款所涵盖的处理活动进行审计。在决定进行审核或审计时，数据出口方应考虑数据进口方持有的相关证明。

(d) 数据出口方可以选择自己进行审计或委托独立审计人员进行审计。审计可能包括对数据进口方的场所或物理设施的检查，并应在合理的通知下在合适时进行。

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

第 9 条

使用次级处理者

(a) 一般书面授权数据进口方拥有数据出口方的一般性授权，可以聘用商定清单中的次级处理者。如果该清单中增加或替换了某些次级处理者，数据进口方应至少提前 90 天以书面形式专门将此变更告知数据出口方，使数据出口方在数据进口方聘用次级处理者之前有足够的时间反对此类变更。数据进口方应向数据出口方提供必要的信息，使数据出口方能够行使反对权。

(b) 如果数据进口方聘用次级处理者（代表数据出口方）执行特定处理活动，则应通过书面合同的形式聘请，该合同应实际规定与数据进口方在本条款下所受约束相同的数据保护义务，包括数据主体的第三

方受益人权利。缔约方同意，遵守本条款，即代表数据进口方将履行第 8.8 条规定的义务。数据进口方应确保次级处理者承担本条款规定的数据进口方应承担的义务。

(c) 数据出口方如有要求，数据进口方应按要求向数据出口方提供此类次级处理者协议和任何后续修订的副本。在保护商业机密或其他机密信息（包括个人数据）所必需的范围内，数据进口方可以在提供副本之前编辑协议部分文本。

(d) 对于次级处理者履行其与数据进口方签订的合同的义务，数据进口方应就此向数据出口方承担全部责任。如果次级处理者未能履行其在该合同下的义务，数据进口方应通知数据出口方。

(e) 数据进口方应与次级处理者商定第三方受益人条款，根据该条款，如果数据进口方实际消失、在法律上不复存在或破产的情况下，数据出口方有权终止次级处理者合同并指示次级处理者删除或归还个人数据。

第 10 条

数据主体权利

(a) 若数据进口方收到数据主体的任何请求，应当及时通知数据出口方。除非得到数据出口方的授权，否则不应自行回应该请求。

(b) 数据进口方有义务协助数据出口方回应数据主体根据第 (EU) 2016/679 号条例行使其权利而提出的请求。在这方面，缔约方应在附件 II 中列出适当的技术和组织措施，同时考虑到提供协助的处理的性质，以及所需协助的范围和程度。

(c) 在履行 (a) 和 (b) 款规定的义务时，数据进口方应遵守数据出口方的指示。

第 11 条

救济

(a) 数据进口方应通过单独通知或在其网站上以透明且易于访问的格式告知数据主体授权处理投诉的联络点。数据进口方应及时处理数据主体提起的任何投诉。

(b) 如果数据主体与其中一方就本条款的遵守情况发生争议，该方应尽最大努力及时友好地解决问题。缔约方应就此类争议相互通报，并在适当情况下合作解决这些争议。

(c) 当数据主体依据第 3 条规定行使第三方受益权，数据进口方应当接受数据主体的以下决定：

(i) 根据第 13 条向其常住地或工作地所在成员国的监管机构或主管监管机构提出投诉；

(ii) 将争议提交第 18 条指定的主管法院。

(d) 缔约方接受数据主体可以由非营利机构、组织或协会根据第 (EU) 2016/679 号条例第 80(1) 条规定的

条件作为代表。

(e) 数据进口方应遵守根据适用欧盟或成员国法律作出的具有约束的决定。

(f) 数据进口方同意，数据主体的选择不会减损其依据适用法律寻求救济的实质和程序权利。

第 12 条

责任

(a) 任何一方均应对另一方因违反本条款而给另一方造成的任何损害承担责任。

(b) 数据进口方或其次级处理者因违反本条款规定的第三方受益人权利而给数据主体造成的任何重大或非重大损害，数据进口方应对数据主体承担责任，且数据主体有权获得赔偿。

(c) 尽管有（b）款的规定，但对数据出口方或数据进口方（或其次级处理者）因侵犯本条款规定的第三方受益人权利而给数据主体造成的任何重大或非重大损害，数据出口方应对数据主体承担责任，且数据主体有权获得赔偿。这不影响数据出口方的责任，如果数据出口方是以控制者名义行事的处理者，则不影响控制者在第 (EU) 2016/679 号或或 (EU) 2018/1725 号条例（视情况而定）下的责任。

(d) 缔约方同意，如果数据出口方根据 (c) 款对数据进口方（或其次级处理者）造成的损害承担责任，则有权向数据进口方追要与数据进口方所应承担的损害对应部分的赔偿。

(e) 如果超过一方对因违反本条款而对数据主体造成的任何损害负责，则所有责任方应承担连带责任，数据主体有权对其中任何一方提起诉讼。

(f) 缔约方同意，如果一方根据（e）款承担责任，则有权向另一方/其他方追要与其承担损害责任相对应部分的赔偿。

(g) 数据进口方不得以次级处理者的行为来规避自己的责任。

第 13 条

监管

(a) 如果数据出口方在欧盟成员国设立：负责监督数据出口方遵守第（EU）2016/679 号条例关于数据转移的监管机构（如附件 I.C 所示）应作为主管监管机构。

如果数据出口方未在欧盟成员国设立，但根据第（EU）2016/679 号条例的第 3（2）条属于其适用领土范围，且已根据第（EU）2016/679 号条例第 27（1）条指定代表：第（EU）2016/679 号条例第 27(1) 条所指的代表所在成员国的监管机构（如附件 I.C 所示）应作为主管监管机构。

如果数据出口方未在欧盟成员国设立，但根据第（EU）2016/679 号条例的第 3（2）条属于其适用领土范围，且根据第（EU）2016/679 号条例第 27（2）条无需指定代表：因为数据主体接受货物或服

务或其行为受到监视，其个人数据根据本条款被转移，那么其所在的一个成员国的监控机构（如附件 I.C 所示）应作为主管监管机构。

(b) 数据进口方同意，在任何旨在确保遵守本条款的程序中服从主管监管机构的管辖并与之合作。特别是，数据进口方同意回应查询、提交审计并遵守监管机构采取的措施，包括救济和赔偿措施。它应向监管机构提供书面确认书，表明已采取必要的措施。

第三节——当公共当局提出查阅数据请求的情况下当地的法律和义务

第 14 条

影响遵守本条款的地方法律和惯例

(a) 缔约方保证，他们没有理由认为适用于数据进口方处理个人数据的目的地第三国法律和惯例（包括披露个人数据的任何要求或向公共机关授予访问权限的措施）会阻止数据进口方履行其在本条款下的义务。这一保证所基于的理解是：尊重基本权利和自由本质，并且如果法律和惯例不超过民主社会中为保障第 (EU) 2016/679 号条例第 23(1) 条所列目标之一所必需和相称的范围，则该法律和惯例与本条款不矛盾。

(b) 帝约方声明，在提供 (a) 款中的保证时，他们特别考虑了以下内容：

(i) 转移的具体情况，包括处理链的长度、涉及的参与者数量和使用的渠道传输；后续转移；接收者的类型；处理的目的；转移的个人数据的类别和格式；进行转移的经济部门；转移的数据的存储位置；

(ii) 目的地第三国中与转移的具体情况相关的法律和惯例，包括要求向公共当局披露数据或授予此类机构访问权限的法律和惯例，以及适用限制和保障措施；

(iii) 为补充本条款下的保障措施而实施的任何相关合同、技术或组织保障措施，包括在传输过程中采取的措施以及在目的地国家/地区处理个人数据时采取的措施。

(c) 数据进口方保证，在根据（b）款进行评估时，已尽最大努力向数据出口方提供相关信息，并同意继续与数据出口方合作以确保遵守本条款。

(d) 缔约方同意根据 (b) 款规定的评估记录在案，并应要求将其提供给主管监管机构。

(e) 数据进口方同意，在就本条款达成一致之后、合同存续期间，如果有理由认为其受到或已经受到与（a）款要求有冲突的法律或惯例的约束，包括在第三国法律发生变更或采取措施（例如披露请求）表明此

类法律或惯例在实践中的应用不符合 (a) 款的要求之后，应将此类情况通知数据出口方。

(f) 在根据（e）款发出通知后，或者如果数据出口方有理由认为数据进口方无法再履行本条款规定的义务，则数据出口方应立即确定适当的措施（例如技术或组织措施，以确保安全性和保密性）供数据出口方和/或数据进口方采用以解决这种情况。如果数据出口方认为无法保障此类转移，或者如果主管监管机构指示暂停数据转移，则数据出口方应暂停数据转移。在这种情况下，只要涉及根据本条款处理个人数据，那么数据出口方便有权终止合同。如果合同涉及多方（超过两方），除非各方另有约定，否则数据出口方只能对相关方行使终止权。如果根据本条款终止合同，则应条款 16(d) 和（e）将适用。

第 15 条

在公共当局提出查阅数据请求的情况下数据进口方的义务

15.1 通知

(a) 数据进口方同意，在出现以下情况时立即通知数据出口方，并在可能的情况下通知数据主体（如有必要，请求数据出口方的帮助）：

(i) 从包括司法当局在内的公共当局收到，依据目的地国家/地区的法律要求披露依据本条款转移的个具有法律约束力的请求；此类通知应包括有关所请求的个人数据、发出请求的机构、请求的法律提供回应的信息；或

(ii) 获悉公共当局根据目的地国家/地区的法律，直接获取依据本条款转移的个人数据；此类通知应包可获得的所有信息。

(b) 如果目的地国家/地区法律禁止数据进口方通知数据出口方和/或数据主体，数据进口方同意尽最大努力获取禁令豁免，以期尽可能多地交流信息。数据进口方同意将其最大努力的记录在案，以便应数据出口方的要求出示。

(c) 在目的地国家/地区法律允许的情况下，数据进口方同意在合同期限内定期向数据出口方尽可能详细地提供有关所收到请求的信息（特别是请求的数量、请求的数据类型、发出请求的机构、请求是否受到质疑以及此类质疑的结果等）。

(d) 数据进口方同意在合同期限内根据 (a) 至 (c) 款保存信息，并应要求将其提供给主管监管机构。

(e) (a) 至（c）款不影响数据进口方在无法遵守本条款时根据条款 14(e) 和 16 及时通知数据出口方的义务。

15.2 合法性审查和数据最小化

(a) 数据进口方同意审查披露请求的合法性，特别是它是否属于发出请求的公共当局的权力范围内，并且如果在经过仔细评估后，数据进口方有合理理由相信根据目的地国家/地区的法律、国际法规定的适用义务和国际礼让原则可以得出该请求不合法的结论，则对该请求提出质疑。在同等条件下，数据进口方应当寻求申诉的可能性。在对请求提出质疑时，数据进口方应寻求临时措施，以期在法院就安庆作出决定前，暂停请求的效力。在适用的程序规则要求披露所请求的个人数据之前，不得披露此类消息。这些要求不影响数据进口方根据第 14(e) 条所承担的义务。

(b) 数据进口方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，向数据出口方提供文件。它还应根据要求将其提供给主管监管机构。

(c) 数据进口方同意根据对请求的合理解释，在回应披露请求时提供允许的最低量信息。

第四节——最后条款

第 16 条

违反条款和终止

(a) 如果数据进口方无法遵守本条款，无论原因为何，均应及时通知数据出口方。

(b) 如果数据进口方违反本条款或无法遵守本条款，数据出口方应暂停向数据进口方转移个人数据，直至再次确保合规或终止合同。这不影响条款 14(f)。

(c) 只要涉及根据本条款处理个人数据，如果出现以下情况，则数据出口方就有权终止合同：

(i) 数据出口方已根据（b）款暂停向数据进口方转移个人数据，但数据进口方在合理时间内及暂停后一个月内仍未遵守本条款；

(ii) 数据进口方严重或持续违反本条款；或

(iii) 数据进口方未能遵守主管法院或监管机构对其作出的有关本条款义务的具有约束力的决定。

在这种情况下，应将此类违规行为通知主管监管机构。如果合同涉及多方（超过两方），除非各方另有约定，否则数据出口方只能对相关方行使终止权。

(d) 根据（c）款终止合同前转移的个人数据应按数据出口方的选择立即归还给数据出口方或全部删除。此规定同样适用于数据的任何副本。数据进口方应向数据出口方证明数据已删除。在删除或归还数据之前，数据进口方应继续确保遵守本条款。如果适用于数据进口方的当地法律禁止归还或删除已转移的个人数据，则数据进口方保证将继续确保遵守本条款，并且只会在当前法律要求的范围和期限内处理数据。

(e) 如果 (i) 欧盟委员会根据第 (EU) 2016/679 号条例的第 45(3) 条作出决定，且决定涵盖本条款适用的个人数据转移，则任何一方均可撤销其受本条款约束的协议；或者 (ii) 第 (EU) 2016/679 号条例成为个人数据转移的目的地国家/地区法律框架的一部分。这不影响第 (EU) 2016/679 号条例规定的适用于相关处理的其他义务。

第 17 条

管辖法律

本条款应受欧盟成员国之一的法律管辖，但该法律必须允许第三方受益权。缔约方同意以法国的法律作为管辖法律。

第 18 条

选择法院和管辖权

(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) 缔约方同意由法国法院管辖。

(c) 数据主体还可以向其常住地所在成员国的法院对数据出口方和/或数据进口方提起法律诉讼。

(d) 缔约方同意接受此类法院的管辖。

附录

附件 I

A. 缔约方名单

数据出口方：[*数据出口方、其数据保护官和/或欧盟代表（如适用）的身份和详细联系方式*]

姓名：请参阅协议中的客户名称

地址：请参阅协议中的客户地址

联系人的姓名、职务及详细联系方式：请参阅协议中客户联系人的姓名、职位和详细联系方式

与根据本条款转移数据相关的活动： 同协议

签名和日期：同协议

角色（控制者/处理者）：控制者

数据进口方：[*数据进口方（包括负责数据保护的所有联系人）的身份和详细联系方式*]

姓名： 请参阅协议中的 HP 名称

地址：请参阅协议中的 HP 地址

联系人的姓名、职务及详细联系方式：Zoe McMahon，DPO，https://www.hp.com/us-en/privacy/
ww-privacy-form.html

与根据本条款转移数据相关的活动：同协议

签名和日期：同协议

角色（控制者/处理者）：处理者

B. 转移说明

个人数据被转移的数据主体的类别

请参阅附件 1。

所转移个人数据的类别

请参阅附件 1。

转移的敏感数据（如适用）和充分考虑到数据性质和所涉及风险的适用限制或保障措施，例如严格的目的限制、访问限制（包括仅限受过专业培训的员工访问）、保留数据访问记录、后续转移限制或其他安全措施。

请参阅附件 1。

转移频率（例如，数据是一次性转移还是连续转移）。

请参阅附件 1。

处理的性质

请参阅附件 1。

数据转移和进一步处理的目的

请参阅附件 1。

个人数据的保留期限，如果没有保留期限，则为用于确定该期限的标准

请参阅协议和 DPA。

对于到（次级）处理者的转移，还应指定处理的主题、性质和持续时间

标的物：请参阅附件 1。

性质：请参阅附件 1。

处理的持续时间：等同合同有效期。

C. 主管监管机构

Commission Nationale de l'informatique et des Libertés (CNIL)

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

为保护客户数据，HP 遵守一套稳健的信息安全控制措施，包括政策、实践、程序和组织架构，以保护其自身信息和客户信息（包括 HP 的客户和数据处理附录中定义的个人数据）的机密性、完整性和可用性。以下概述了 HP 在整个公司实施的技术/组织安全措施。

1. 安全策略

HP 致力于维护旨在保护 HP 和客户数据的全球适用的政策、标准和程序。HP 安全策略的细节属于保密信息，用于保护 HP 数据和系统的完整性。但是，我们的主要策略摘要如下。

2. 信息安全组织

HP 设立了一个信息安全组织，负责指导和管理组织的信息安全策略和控制措施。HP 还部署了信息安全框架/管理系统，以确保符合 HP 的安全政策和控制措施，并确认遵守其客户的安全要求。该框架的结构与 NIST 网络安全框架保持一致，每年审查一次。

3. 资产管理

HP 制定了一个用于识别技术信息资产的流程，通过此流程，HP 可以识别其负责的所有资产并对关键资产进行分类。HP 还为每种信息分类类型（包括那些包含个人数据的资产）建立一套书面处理程序。处理程序中说明了存储、传输、通信、访问、记录、保留、销毁、处置、事故管理和**信息泄露**通知。

4. 访问控制

最小权限原则用于提供逻辑访问控制。通过唯一的用户 ID 和密码提供用户访问权限。HP 的密码策略定义了复杂性、强度、有效性和密码历史的相关控制。访问权限会定期审查，并在人员调离岗位时撤销。

用户帐户创建和删除程序，在实施缔约方同意的前提下，将被实现，以授予和撤销协议期间使用的客户端系统访问权限。

5. 人员培训

HP 员工必须完成 Integrity at HP 培训，该培训旨在确保员工熟悉用于管理 HP 的道德行为、卓越和合规期望的项目、政策和资源。Integrity at HP 提供安全和数据隐私模块，员工还需要参加年度“进修”课程。HP 员工还必须完成每年更新的专门安全意识培训，该培训重点关注基本安全政策，并强调员工在事故管理、数据隐私和信息安全方面的责任。

6. 第三方和分包商

HP 制定了适当的流程来甄选能够遵守全面合同安全要求的分包商。

对于适用的供应商（处理/存储/传输 HP 数据和 HP 拥有的客户自有数据或有权访问 HP 网络的供应商），HP 网络安全部门将执行风险评估以验证是否制定了信息安全计划。适足的计划必须包括物理、技术和管理保障。完成此评估后，供应商才能访问 HP 信息。

7. 系统安全

根据政策，HP 内部的系统和支持软件的开发遵循安全的开发方法，以确保整个系统/软件生命周期的安全。软件开发生命周期定义了启动、开发/采集、实施、操作和处置要求。评估包括模块、库、服务和离散组件在内的所有系统组件，以确定它们对整体系统安全状态的影响。

HP 定义了保护应用服务交易的控制措施。这些控制措施包括：验证和确认用户凭据、强制要求数字签名和加密、实施安全通信协议、在适当的网络安全区域内的服务器上存储在线交易详细信息。

定期执行内部漏洞扫描。

8. 物理和环境安全

HP 设施使用各种物理和电子访问控制和监控功能实现保护。根据设施的不同，这可能包括安保、电子访问控制和闭路电视 (CCTV)。

所有 HP 人员均已注册，并且必须携带适当的身份名牌。

设施具有所需的基础设施支持，可在需要时提供温度控制和备用电源，通过 UPS 和/或柴油发电机来支持关键服务。

9. 运营管理

HP 为技术基础设施定义了一套最低强化要求，包括工作站、服务器和网络设备。工作站/服务器映像包含预强化的操作系统。强化要求因操作系统类型和实施的适用控制而异。

HP 已在网络内部署了网络入侵检测/预防系统 (NIDS/NIPS)，并提供 24*7 的监控和管理。

HP 安全政策和标准要求对介质进行安全处理。

10. 加密技术

HP 定义了一套强大的加密流程，以确保信息资产的机密性、完整性和可用性。批准的协议要求对某些资产进行加密，包括那些包含个人数据的资产。

11. 信息安全事故管理

HP 遵循已制定的网络事故管理层流程，该流程涉及目的、范围、角色、职责、管理承诺、组织协调、实施程序和合规性检查。HP 每年都会审查和更新此流程。

HP 拥有一支受过事故响应和危机管理培训的网络安全人员组成的网络事故响应团队，负责对流程和任何事故或事件定期进行公开审查。

12. 业务连续性管理

HP 制定了一项全球运营连续性计划。该计划通过一组协作、标准化和内部记录的规划流程，采用涉及全公司范围的整体式方法来实现端到端的连续性。

HP 定期执行其业务连续性计划以确保其有效性。HP 目前至少每年测试和更新所有计划一次，并确保对业务连续性计划涉及的人员进行培训。

对于向（次级）处理者的转移，还应描述（次级）处理者为能够向控制者提供帮助以及为数据出口方将数据从处理者转移到次级处理者提供帮助而采取的具体技术和组织措施

次级处理者仅处理：姓名、企业电子邮件地址、企业电话号码、企业地址。转移这些数据的目的是为了完成合同。

对于 HP 而言，上述所有技术和组织措施都在遵循合作伙伴行为准则和合同条款的前提下传递给次级处理者。次级处理者必须承诺遵守 HP 的要求。

附件 3

欧盟标准合同条款（数据处理者转移至数据处理者）

第一节

第 1 条

目的和适用范围

(a) 本标准合同条款旨在确保在将个人数据转移到第三国时符合欧洲议会的第 (EU) 2016/679 号条例和理事会 2016 年 4 月 27 日关于在处理个人数据方面和保护自然人以及此类数据的自由流动的要求（通用数据保护条例）https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN - ntr1-L_2021199EN.01003701-E0001。

(b) 缔约方：

(i) 转移个人数据的自然人或法人、公共当局、机构或其他团体（以下简称“实体”），如附件 I.A 中所列（以下简称“数据出口方”），以及

(ii) 直接或通过另一个同为本条款缔约方的中间实体，从数据出口方接收个人数据（如附件 I.A 中所列）的第三国实体，（以下简称“数据进口方”）

已就这些标准合同条款（以下简称：“条款”）达成一致。

(c) 本条款适用于个人数据的转移，如附件 I.B 中规定。

(d) 本条款的附录包含条款中提及的附件，是本条款不可或缺的部分。

第 2 条

条款的效力和不可更改性

(a) 本条款规定了适当的保障措施，包括根据第 (EU) 2016/679 号条例的第 46(1) 条和第 46(2) (c) 条的规定可执行的数据主体权利和有效的法律救济措施以及从控制者向处理者和/或从处理者到处理者的数据转移，标准合同条款应符合第 (EU) 2016/679 号条例的第 28(7) 条的规定，除非选择适当的模块或在附录中添加或更新信息外，均不得修改。这并不妨碍缔约方将本条款中规定的标准合同条款纳入和/或添加其他条款或额外保障措施，但它们不得直接或间接地与本条款相矛盾或损害数据主体的基本权利或自由。

(b) 本条款不影响数据出口方根据第 (EU) 2016/679 号条例所承担的义务。

第 3 条

第三方受益人

(a) 数据主体可以作为第三方受益人，可对数据出口方和/或数据进口方援引和执行本条款，但以下情况除外：

(i) 第 1、2、3、6、7 条；

(ii) 第 8 条——第 8.1(a)、(c) 和 (d) 条以及第 8.9(a)、(c)、(d)、(e)、(f) 和 (g) 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) (a) 款不影响数据主体根据第 (EU) 2016/679 号条例所享有的权利。

第 4 条

释义

(a) 如果本条款使用第 (EU) 2016/679 号条例中定义的术语，则这些术语应与该条例中的含义相同。

(b) 本条款应根据第 (EU) 2016/679 号条例的规定进行理解和解释。

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

第 5 条

等级制度

如果本条款与在本条款达成一致或签订之时已存在的缔约方相关协议的规定发生冲突，则以本条款为准。

第 6 条

转移说明

附件 I.B 中详细说明了转移的详细信息，尤其是转移的个人数据的类别和转移的目的。

第二节——各方的义务

第 8 条

数据保护保障措施

数据出口方保证已尽合理努力确定数据进口方能够通过实施适当的技术和组织措施来履行其在本条款下的义务。

8.1 指示

(a) 数据出口方已通知数据进口方应作为处理者根据控制者的指示行事，数据出口方应在处理前向数据进口方提供该等指示。

(b) 数据进口方应仅根据数据出口方传达给数据进口方的来自控制者的书面指示和数据出口方的任何附加书面指示处理个人数据。此类附加指示不得与控制者的指示相冲突。控制者或数据出口方可能会在整个合同期间就数据处理提供进一步的书面指示。

(c) 数据进口方如不能按照指示执行，应立即通知数据出口方。如果数据进口方无法按照控制者的指示执行，数据出口方应当立即通知控制者。

(d) 数据出口方保证，已要求数据进口方承担与控制者和数据出口方之间的合同或欧盟或成员国法律规定的其他法律行为中列出的相同数据保护义务。

8.2 目的限制

数据进口方应仅出于附件 I.B 中规定的特定转移目的处理个人数据，除非数据进口方收到数据出口方传达的来自控制者的进一步指示，或者数据出口方有进一步指示。

8.3 透明度

数据出口方必须应要求免费向数据主体提供本条款的副本，包括缔约方编写的附录。在保护商业机密或其他机密信息（包括个人数据）的必要范围内，数据出口方可以在共享副本之前编辑附录的部分文本，但应提供有意义的摘要，以帮助数据主体了解其内容或行使其权利。缔约方应按要求在不泄露修订信息的范围内尽可能向数据主体提供修订的理由。

8.4 准确度

如果数据进口方发现其收到的个人数据不准确或已过时，应立即通知数据出口方。在这种情况下，数据进口方应配合数据出口方对数据进行更正或删除。

8.5 处理期限和数据的删除或归还

数据进口方只能在附件 I.B 中指定的期限内处理数据。在终止提供处理服务时，数据进口方应根据数据出口方的选择，删除代表控制者处理的所有个人数据，并向数据出口方证明其已删除此类数据，或者将其代表数据出口方处理的个人数据归还给数据出口方并删除现有副本。在删除或归还数据之前，数据进口方应继续确保遵守本条款。如果适用于数据进口方的当地法律禁止归还或删除个人数据，则数据进口方保证将继续确保遵守本条款，并且只会在当前法律要求的范围和期限内处理数据。这不影响第 14 条，特别是第 14(e) 条规定的要求，即数据进口方在整个合同期间都有义务在合理认为其受到或已经受到与第 14(a) 条的要求有冲突的法律或惯例约束时通知数据出口方。

8.6 处理的安全性

(a) 数据进口方和过程中传输的数据出口方应实施适当的技术和组织措施以确保数据的安全，包括防止安全漏洞，导致意外或非法破坏、丢失、篡改、未经授权的披露或获取该数据（以下简称“个人数据泄露”）。在评估适当的安全水平时，应适当考虑最新技术水平、实施成本及处理的性质、范围、背景和目的以及处理给数据主体带来的风险。缔约方应特别考虑在不妨碍实现处理目的的情况下包括在传输过程中对数据进行加密或假名化处理。在假名化的情况下，用于将个人数据还原到特定数据主体的附加信息应尽可能由数据出口方或控制者独家控制。在履行本款规定的义务时，数据进口方至少应实施附件 II 中规定的技术和组织措施。数据进口方应进行定期检查，以确保这些措施继续提供适当的安全水平。

(b) 数据进口方只有在合同的实施、管理和监控绝对必要的范围内，才能授予其人员访问数据的权限，并且应确保被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) 如果数据进口方根据本条款处理的个人数据发生个人数据泄露，数据进口方应采取适当措施解决该泄露事件，包括减轻其不利影响的措施。数据进口方还应在知悉违规行为后立即通知数据出口方，在适当和可行时还应通知控制者。此类通知应包含可以获取更多信息的联络人的详细信息、对泄露事件性质的描述（在可能的情况下，包括相关的数据主体和个人数据记录的类别和大致数量）、可能的后果以及为解决数据泄露而采取或建议采取的措施，包括减轻其可能的不利影响的措施。在不可能同时提供所有信息的情况下，初始通知应包含当时可获得的信息，并且在获得进一步信息后应及时提供，不得无故拖延。

(d) 数据进口方应与数据出口方合作并协助数据出口方履行其根据第（EU）2016/679 号条例所承担的义务，特别应帮助数据出口方通知其控制者，使控制者能够在结合考虑处理的性质和数据进口方拥有的信息后，通知主管监管机构和受影响的数据主体。

8.7 敏感数据

如果转移的数据涉及包含种族或族裔血统、政治观点、宗教或哲学信仰或工会成员身份的个人数据、能够唯一识别自然人身份的基因数据或生物特征数据、有关健康或个人性生活或性取向的数据或与刑事定罪和犯罪有关的数据（以下简称“敏感数据”），数据进口方应当应用附件 I.B 中载明的具体限制和/或其他保障措施。

8.8 后续转移

数据进口方应仅根据数据出口方传达给数据进口方的来自控制者的书面指示向第三方披露个人数据。此外，数据只能披露给位于欧盟 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&from=EN - ntr6-L_2021199EN.01003701-E0006 以外的在适当模块下受本条款约束或同意受本条款约束的第三方（与数据进口方在同一国家/地区或在另一个第三国，以下简称“后续转移”），或者：

(i) 后续转移指转移到受益于根据第 (EU) 2016/679 号条例第 45 条（涵盖后续转移）作出的充分性决定的国家或地区；

(ii) 第三方根据第 (EU) 2016/679 号条例的第 46 或 47 条确保适当的保障措施；

(iii) 后续转移是指在特定的行政、监管或司法程序中建立、行使或维护法律诉求所必需的；或

(iv) 为了保护数据主体或其他自然人的切身利益，有必要进行后续转移。

对于任何后续转移，数据进口方都必须遵守本条款下的所有其他保障措施，特别是目的限制。

8.9 文档记录和合规性

(a) 数据进口方应及时、充分地处理数据出口方或控制者就根据本条款进行的处理提出的询问。

(b) 缔约方应能够证明遵守本条款。特别是，数据进口方应保留代表控制者进行的处理活动有关的相应文件。

(c) 数据进口方应向数据出口方提供证明其遵守本条款中所规定义务的所有必要信息，数据出口方应将此类信息提供给控制者。

(d) 数据进口方应允许并协助数据出口方以合理的时间间隔或在有不合规迹象的情况下对本条款涵盖的处理活动进行审计。如果数据出口方要求对控制者的指示进行审计，则这一要求同样适用。在决定进行审计时，数据出口方应考虑数据进口方持有的相关证明。

(e) 如果审计根据控制者的指示进行，则数据出口方应将结果提供给控制者。

(f) 数据出口方可以选择自己进行审计或委托独立审计人员进行审计。审计可能包括对数据进口方的场所或物理设施的检查，适当情况下应事先发出合理通知。

(g) 缔约方应根据要求向主管监管机构提供 (b) 和 (c) 款中提及的信息，包括任何审计结果。

第 9 条

使用次级处理者

(a) “一般书面授权”：数据进口方拥有控制者的一般性授权，可以聘用商定清单中的次级处理者。如果

该清单中增加或替换了某些次级处理者，数据进口方应至少提前 10 天以书面形式专门将此变更告知控制者，使控制者在数据进口方聘用次级处理者之前有足够的时间反对此类变更。数据进口方应向控制者提供必要的信息，使控制者能够行使反对权。数据进口方应将聘用次级处理者的情况通知数据出口方。

(b) 如果数据进口方聘用次级处理者（代表控制者）执行特定处理活动，则应通过书面合同的形式聘请，该合同应实际规定与数据进口方在本条款下所受约束相同的数据保护义务，包括数据主体的第三方受益人权利。缔约方同意，遵守本条款，即代表数据进口方将履行第 8.8 条规定的义务。数据进口方应确保次级处理者承担本条款规定的数据进口方应承担的义务。

(c) 数据出口方或控制者如有要求，数据进口方应按要求提供此类次级处理者协议和任何后续修订的副本。在保护商业机密或其他机密信息（包括个人数据）所必需的范围内，数据进口方可以在提供副本之前编辑协议部分文本。

(d) 对于次级处理者履行其与数据进口方签订的合同的义务，数据进口方应就此向数据出口方承担全部责任。如果次级处理者未能履行其在该合同下的义务，数据进口方应通知数据出口方。

(e) 数据进口方应与次级处理者商定第三方受益人条款，根据该条款，如果数据进口方实际消失、在法律上不复存在或破产的情况下，数据出口方有权终止次级处理者合同并指示次级处理者删除或归还个人数据。

第 10 条

数据主体权利

(a) 数据进口方在收到数据主体的任何请求时，均应立即将其通知数据出口方，适当情况下还应通知控制者。除非获得控制者的授权，否则不得回应该请求。

(b) 在适当的情况下，数据进口方应与数据出口方合作，协助控制者履行其义务，回应数据主体根据第 (EU) 2016/679 号条例或第 (EU) 2018/1725 号条例（视情况而定）行使其权利而提出的请求。在这方面，缔约方应在附件 II 中列出适当的技术和组织措施，同时考虑到提供协助的处理的性质，以及所需协助的范围和程度。

(c) 在履行 (a) 和 (b) 款规定的义务时，数据进口方应遵守数据出口方传达的来自控制者的指示。

第 11 条

救济

(a) 数据进口方应通过单独通知或在其网站上以透明且易于访问的格式告知数据主体授权处理投诉的联络点。数据进口方应及时处理数据主体提起的任何投诉。

(b) 如果数据主体与其中一方就本条款的遵守情况发生争议，该方应尽最大努力及时友好地解决问题。缔约方应就此类争议相互通报，并在适当情况下合作解决这些争议。

(c) 当数据主体依据第 3 条规定行使第三方受益权，数据进口方应当接受数据主体的以下决定：

(i) 根据第 13 条向其常住地或工作地所在成员国的监管机构或主管监管机构提出投诉；

(ii) 将争议提交第 18 条指定的主管法院。

(d) 缔约方接受数据主体可以由非营利机构、组织或协会根据第 (EU) 2016/679 号条例第 80(1) 条规定的条件作为代表。

(e) 数据进口方应遵守根据适用欧盟或成员国法律作出的具有约束的决定。

(f) 数据进口方同意，数据主体的选择不会减损其依据适用法律寻求救济的实质和程序权利。

第 12 条

责任

(a) 任何一方均应对另一方因违反本条款而给另一方造成的任何损害承担责任。

(b) 数据进口方或其次级处理者因违反本条款规定的第三方受益人权利而给数据主体造成的任何重大或非重大损害，数据进口方应对数据主体承担责任，且数据主体有权获得赔偿。

(c) 尽管有（b）款的规定，但对数据出口方或数据进口方（或其次级处理者）因侵犯本条款规定的第三方受益人权利而给数据主体造成的任何重大或非重大损害，数据出口方应对数据主体承担责任，且数据主体有权获得赔偿。这不影响数据出口方的责任，如果数据出口方是以控制者名义行事的处理者，则不影响控制者在第 (EU) 2016/679 号或或 (EU) 2018/1725 号条例（视情况而定）下的责任。

(d) 缔约方同意，如果数据出口方根据 (c) 款对数据进口方（或其次级处理者）造成的损害承担责任，则有权向数据进口方追要与数据进口方所应承担的损害对应部分的赔偿。

(e) 如果超过一方对因违反本条款而对数据主体造成的任何损害负责，则所有责任方应承担连带责任，数据主体有权对其中任何一方提起诉讼。

(f) 缔约方同意，如果一方根据（e）款承担责任，则有权向另一方/其他方追要与其承担损害责任相对应部分的赔偿。

(g) 数据进口方不得援引次级处理者的行为来规避自己的责任。

第 13 条

监管

(a) 如果数据出口方在欧盟成员国设立：负责监督数据出口方遵守第（EU）2016/679 号条例关于数据转移的监管机构（如附件 I.C 所示）应作为主管监管机构。

如果数据出口方未在欧盟成员国设立，但根据第（EU）2016/679 号条例的第 3（2）条属于其适用领土范围，且已根据第（EU）2016/679 号条例第 27（1）条指定代表：第（EU）2016/679 号条例第 27(1) 条所指的代表所在成员国的监管机构（如附件 I.C 所示）应作为主管监管机构。

如果数据出口方未在欧盟成员国设立，但根据第（EU）2016/679 号条例的第 3（2）条属于其适用领土范围，且根据第（EU）2016/679 号条例第 27（2）条无需指定代表：因为数据主体接受货物或服务或其行为受到监视，其个人数据根据本条款被转移，那么其所在的一个成员国的监控机构（如附件 I.C 所示）应作为主管监管机构。

(b) 数据进口方同意，在任何旨在确保遵守本条款的程序中服从主管监管机构的管辖并与之合作。特别是，数据进口方同意回应查询、提交审计并遵守监管机构采取的措施，包括救济和赔偿措施。它应向监管机构提供书面确认书，表明已采取必要的措施。

第三节——当公共当局提出查阅数据请求的情况下当地的法律和义务

第 14 条

影响遵守本条款的地方法律和惯例

(a) 缔约方保证，他们没有理由认为适用于数据进口方处理个人数据的目的地第三国法律和惯例（包括披露个人数据的任何要求或向公共机关授予访问权限的措施）会阻止数据进口方履行其在本条款下的义务。这一保证所基于的理解是：尊重基本权利和自由本质，并且如果法律和惯例不超过民主社会中为保障第 (EU) 2016/679 号条例第 23(1) 条所列目标之一所必需和相称的范围，则该法律和惯例与本条款不矛盾。

(b) 缔约方声明，在提供 (a) 款中的保证时，他们特别考虑了以下内容：

(i) 转移的具体情况，包括处理链的长度、涉及的参与者数量和使用的渠道传输；后续转移；接收者的类型；处理的目的；转移的个人数据的类别和格式；进行转移的经济部门；转移的数据的存储位置；

(ii) 目的地第三国中与转移的具体情况相关的法律和惯例，包括要求向公共当局披露数据或授予此类机构访问权限的法律和惯例，以及适用限制和保障措施；

(iii)为补充本条款下的保障措施而实施的任何相关合同、技术或组织保障措施，包括在传输过程中采取的措施以及在目的地国家/地区处理个人数据时采取的措施。

(c) 数据进口方保证，在根据（b）款进行评估时，已尽最大努力向数据出口方提供相关信息，并同意继续

与数据出口方合作以确保遵守本条款。

(d) 缔约方同意根据 (b) 款规定的评估记录在案，并应要求将其提供给主管监管机构。

(e) 数据进口方同意，在就本条款达成一致之后、合同存续期间，如果有理由认为其受到或已经受到与 (a) 款要求有冲突的法律或惯例的约束，包括在第三国法律发生变更或采取措施（例如披露请求）表明此类法律或惯例在实践中的应用不符合 (a) 款的要求之后，应将此类情况通知数据出口方。数据出口方应将通知转发给控制者。

(f) 在根据 (e) 款发出通知后，或者如果数据出口方有理由认为数据进口方无法再履行本条款规定的义务，则数据出口方应立即（在适当的情况下，与控制者协商）确定适当的措施（例如技术或组织措施，以确保安全性和保密性）供数据出口方和/或数据进口方采用以解决这种情况。如果数据出口方认为无法保障此类转移，或者如果控制者或主管监管机构指示暂停数据转移，则数据出口方应暂停数据转移。在这种情况下，只要涉及根据本条款处理个人数据，那么数据出口方便有权终止合同。如果合同涉及多方（超过两方），除非各方另有约定，否则数据出口方只能对相关方行使终止权。如果根据本条款终止合同，则应条款 16(d) 和 (e) 将适用。

第 15 条

在公共当局提出查阅数据请求的情况下数据进口方的义务

15.1 通知

(a) 数据进口方同意，在出现以下情况时立即通知数据出口方，并在可能的情况下通知数据主体（如有必要，请求数据出口方的帮助）：

(i) 从包括司法当局在内的公共当局收到，依据目的地国家/地区的法律要求披露依据本条款转移的个人数据的具有法律约束力的请求；此类通知应包括有关所请求的个人数据、发出请求的机构、请求的法律依据和所提供回应的信息；或

(ii) 获悉公共当局根据目的地国家/地区的法律，直接获取依据本条款转移的个人数据；此类通知应包括进口方可获得的所有信息。

数据出口方应将通知转发给控制者。

(b) 如果目的地国家/地区法律禁止数据进口方通知数据出口方和/或数据主体，数据进口方同意尽最大努力获取禁令豁免，以期尽可能多地交流信息。数据进口方同意将其最大努力的记录在案，以便应数据出口方的要求出示。

(c) 在目的地国家/地区法律允许的情况下，数据进口方同意在合同期限内定期向数据出口方尽可能详细地提供有关所收到请求的信息（特别是请求的数量、请求的数据类型、发出请求的机构、请求是否受

到质疑以及此类质疑的结果等）。数据出口方应将信息转发给控制者。

(d) 数据进口方同意在合同期限内根据 (a) 至 (c) 款保存信息，并应要求将其提供给主管监管机构。

(e) (a) 至 (c) 款不影响数据进口方在无法遵守本条款时根据条款 14(e) 和 16 及时通知数据出口方的义务。

15.2 合法性审查和数据最小化

(a) 数据进口方同意审查披露请求的合法性，特别是它是否属于发出请求的公共当局的权力范围内，并且如果在经过仔细评估后，数据进口方有合理理由相信根据目的地国家/地区的法律、国际法规定的适用义务和国际礼让原则可以得出该请求不合法的结论，则对该请求提出质疑。在同等条件下，数据进口方应当寻求申诉的可能性。在对请求提出质疑时，数据进口方应寻求临时措施，以期在法院就安庆作出决定前，暂停请求的效力。在适用的程序规则要求披露所请求的个人数据之前，不得披露此类消息。这些要求不影响数据进口方根据第 14(e) 条所承担的义务。

(b) 数据进口方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，向数据出口方提供文件。它还应根据要求将其提供给主管监管机构。数据出口方应将评估结果提供给控制者。

(c) 数据进口方同意根据对请求的合理解释，在回应披露请求时提供允许的最低量信息。

第四节——最后条款

第 16 条

违反条款和终止

(a) 如果数据进口方无法遵守本条款，无论原因为何，均应及时通知数据出口方。

(b) 如果数据进口方违反本条款或无法遵守本条款，数据出口方应暂停向数据进口方转移个人数据，直至再次确保合规或终止合同。这不影响条款 14(f)。

(c) 只要涉及根据本条款处理个人数据，如果出现以下情况，则数据出口方就有权终止合同：

(i) 数据出口方已根据（b）款暂停向数据进口方转移个人数据，但数据进口方在合理时间内及暂停后一个月内仍未遵守本条款；

(ii) 数据进口方严重或持续违反本条款；或

(iii) 数据进口方未能遵守主管法院或监管机构对其作出的有关本条款义务的具有约束力的决定。

在这种情况下，应将此类违规行为通知主管监管机构和控制者。如果合同涉及多方（超过两方），

除非各方另有约定，否则数据出口方只能对相关方行使终止权。

(d) 根据（c）款终止合同前转移的个人数据应按数据出口方的选择立即归还给数据出口方或全部删除。此规定同样适用于数据的任何副本。数据进口方应向数据出口方证明数据已删除。在删除或归还数据之前，数据进口方应继续确保遵守本条款。如果适用于数据进口方的当地法律禁止归还或删除已转移的个人数据，则数据进口方保证将继续确保遵守本条款，并且只会在当前法律要求的范围和期限内处理数据。

(e) 如果 (i) 欧盟委员会根据第 (EU) 2016/679 号条例的第 45(3) 条作出决定，且决定涵盖本条款适用的个人数据转移，则任何一方均可撤销其受本条款约束的协议；或者 (ii) 第 (EU) 2016/679 号条例成为个人数据转移的目的地国家/地区法律框架的一部分。这不影响第（EU）2016/679 号条例规定的适用于相关处理的其他义务。

第 17 条

管辖法律

本条款应受欧盟成员国之一的法律管辖，但该法律必须允许第三方受益权。缔约方同意以法国的法律作为管辖法律。

第 18 条

选择法院和管辖权

(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) 缔约方同意由法国法院管辖。

(c) 数据主体还可以向其常住地所在成员国的法院对数据出口方和/或数据进口方提起法律诉讼。

(d) 缔约方同意接受此类法院的管辖。

附录

附件 I

A. 缔约方名单

数据出口方：[*数据出口方、其数据保护官和/或欧盟代表（如适用）的身份和详细联系方式*]

姓名：请参阅协议中的客户名称

地址：请参阅协议中的客户地址

联系人的姓名、职务及详细联系方式：请参阅协议中客户联系人的姓名、职位和详细联系方式

与根据本条款转移数据相关的活动： 同协议

签名和日期：同协议

角色（控制者/处理者）：处理者

数据进口方：[*数据进口方（包括负责数据保护的所有联系人）的身份和详细联系方式*]

姓名：请参阅协议中的 HP 名称

地址：请参阅协议中的 HP 地址

联系人的姓名、职务及详细联系方式：Zoe McMahon，DPO，https://www.hp.com/us-en/privacy/
ww-privacy-form.html

与根据本条款转移数据相关的活动：同协议

签名和日期：同协议

角色（控制者/处理者）：处理者

B. 转移说明

个人数据被转移的数据主体的类别

请参阅附件 1

所转移个人数据的类别

请参阅附件 1。

转移的敏感数据（如适用）和充分考虑到数据性质和所涉及风险的适用限制或保障措施，例如严格的目的限制、访问限制（包括仅限受过专业培训的员工访问）、保留数据访问记录、后续转移限制或其他安全措施。

请参阅附件 1。

转移频率（例如，数据是一次性转移还是连续转移）。

请参阅附件 1。

处理的性质

请参阅附件 1。

数据转移和进一步处理的目的

请参阅附件 1。

个人数据的保留期限，如果没有保留期限，则为用于确定该期限的标准

请参阅协议和 DPA。

对于到（次级）处理者的转移，还应指定处理的主题、性质和持续时间

标的物：见协议 1。

性质：见协议 1。

处理的持续时间：等同合同有效期。

C. 主管监管机构

Commission Nationale de l'informatique et des Libertés (CNIL)

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

为保护客户数据，HP 遵守一套稳健的信息安全控制措施，包括政策、实践、程序和组织架构，以保护其自身信息和客户信息（包括 HP 的客户和数据处理附录中定义的个人数据）的机密性、完整性和可用性。以下概述了 HP 在整个公司实施的技术/组织安全措施。

1. 安全策略

HP 致力于维护旨在保护 HP 和客户数据的全球适用的政策、标准和程序。HP 安全策略的细节属于保密信息，用于保护 HP 数据和系统的完整性。但是，我们的主要策略摘要如下。

2. 信息安全组织

HP 设立了一个信息安全组织，负责指导和管理组织的信息安全策略和控制措施。HP 还部署了信息安全框架/管理系统，以确保符合 HP 的安全政策和控制措施，并确认遵守其客户的安全要求。该框架的结构与 NIST 网络安全框架保持一致，每年审查一次。

3. 资产管理

HP 制定了一个用于识别技术信息资产的流程，通过此流程，HP 可以识别其负责的所有资产并对关键资产进行分类。HP 还为每种信息分类类型（包括那些包含个人数据的资产）建立一套书面处理程序。处理程序中说明了存储、传输、通信、访问、记录、保留、销毁、处置、事故管理和信息泄露通知。

4. 访问控制

最小权限原则用于提供逻辑访问控制。通过唯一的用户 ID 和密码提供用户访问权限。HP 的密码策略定义了复杂性、强度、有效性和密码历史相关控制。访问权限会定期审查，并在人员调离岗位时撤销。

用户帐户创建和删除程序，在实施缔约方同意的前提下，将被实现，以授予和撤销协议期间使用的客户端系统访问权限。

5. 人员培训

HP 员工必须完成 Integrity at HP 培训，该培训旨在确保员工熟悉用于管理 HP 的道德行为、卓越和合规期望的项目、政策和资源。Integrity at HP 提供安全和数据隐私模块，员工还需要参加年度“进修”课程。HP 员工还必须完成每年更新的专门安全意识培训，该培训重点关注基本安全政策，并强调员工在事故管理、数据隐私和信息安全方面的责任。

6. 第三方和分包商

HP 制定了适当的流程来甄选能够遵守全面合同安全要求的分包商。

对于适用的供应商（处理/存储/传输 HP 数据和 HP 拥有的客户自有数据或有权访问 HP 网络的供应商），HP 网络安全部门将执行风险评估以验证是否制定了信息安全计划。适足的计划必须包括物理、技术和管理保障。完成此评估后，供应商才能访问 HP 信息。

7. 系统安全

根据政策，HP 内部的系统和支持软件的开发遵循安全的开发方法，以确保整个系统/软件生命周期的安全。软件开发生命周期定义了启动、开发/采集、实施、操作和处置要求。评估包括模块、库、服务和离散组件在内的所有系统组件，以确定它们对整体系统安全状态的影响。

HP 定义了保护应用服务交易的控制措施。这些控制措施包括：验证和确认用户凭据、强制要求数字签名和加密、实施安全通信协议、在适当的网络安全区域内的服务器上存储在线交易详细信息。

定期执行内部漏洞扫描。

8. 物理和环境安全

HP 设施使用各种物理和电子访问控制和监控功能实现保护。根据设施的不同，这可能包括安保、电子访问控制和闭路电视 (CCTV)。

所有 HP 人员均已注册，并且必须携带适当的身份名牌。

设施具有所需的基础设施支持，可在需要时提供温度控制和备用电源，通过 UPS 和/或柴油发电机来支持关键服务。

9. 运营管理

HP 为技术基础设施定义了一套最低强化要求，包括工作站、服务器和网络设备。工作站/服务器映像包含预强化的操作系统。强化要求因操作系统类型和实施的适用控制而异。

HP 已在网络内部署了网络入侵检测/预防系统 (NIDS/NIPS)，并提供 24*7 的监控和管理。

HP 安全政策和标准要求对介质进行安全处理。

10. 加密技术

HP 定义了一套强大的加密流程，以确保信息资产的机密性、完整性和可用性。批准的协议要求对某些资产进行加密，包括那些包含个人数据的资产。

11. 信息安全事故管理

HP 遵循已制定的网络事故管理流程，该流程涉及目的、范围、角色、职责、管理层承诺、组织协调、实施程序和合规性检查。HP 每年都会审查和更新此流程。

HP 拥有一支受过事故响应和危机管理培训的网络安全人员组成的网络事故响应团队，负责对流程和任何事故或事件定期进行公开审查。

12. 业务连续性管理

HP 制定了一项全球运营连续性计划。该计划通过一组协作、标准化和内部记录的规划流程，采用涉及全公司范围的整体式方法来实现端到端的连续性。

HP 定期执行其业务连续性计划以确保其有效性。HP 目前至少每年测试和更新所有计划一次，并确保对业务连续性计划涉及的人员进行培训。

对于向（次级）处理者的转移，还应描述（次级）处理者为能够向控制者提供帮助以及为数据出口方将数据从处理者转移到次级处理者提供帮助而采取的具体技术和组织措施

次级处理者仅处理：姓名、企业电子邮件地址、企业电话号码、企业地址。转移这些数据的目的是为了完成合同。

对于 HP 而言，上述所有技术和组织措施都在遵循合作伙伴行为准则和合同条款的前提下传递给次级处理者。次级处理者必须承诺遵守 HP 的要求。

附件 4

国际数据转移协议 (IDTA)（英国）

第 1 部分：表

表 1：缔约方及签名

起始日期	同协议	
缔约方	**出口方（发送受限转移）**	**进口方（接收受限转移）**
缔约方详细资料	法定全名：请参阅协议中的客户法定全名 商号（如果不同）：请参阅协议中的客户商号 主要地址（如果是公司注册地址）：请参阅协议中的客户主要地址 官方注册号（如有）（公司编号或类似标识符）：请参阅协议中的客户官方注册号	法定全名：请参阅协议中的 HP 法定全名 商号（如果不同）：请参阅协议中的 HP 商号 主要地址（如果是公司注册地址）：请参阅协议中的 HP 主要地址 官方注册号（如有）（公司编号或类似标识符）：请参阅协议中的 HP 官方注册号
主要联系人	全名（可选）：请参阅协议 职务：请参阅协议 联系方式，包括电子邮件地址：请参阅协议	全名（可选）：请参阅协议 职务：请参阅协议 联系方式，包括电子邮件地址：请参阅协议
进口方数据主体联系		HP 隐私办公室 https://www.hp.com/us-

方式		en/privacy/ ww-privacy-form.html
确认各方同意受本 IDTA 约束的签名	上述**出口方**代表签名 签名：请参阅协议签名日期：请参阅协议全名：请参阅协议职务：请参阅协议	上述**进口方**的代表签名 签名：请参阅协议 签名日期：请参阅协议 全名：请参阅协议 职务：请参阅协议

表 2：转移详情

监管 IDTA 的英国法律：	☒英格兰和威尔士 ☐北爱尔兰 ☐苏格兰
缔约方提出法律主张的主要地点	☒英格兰和威尔士 ☐北爱尔兰 ☐苏格兰
出口方的身份	关于转移的数据的处理： ☒出口方是控制者 ☐出口方是处理者或次级处理者
进口方的身份	关于转移的数据的处理： ☐进口方是控制者

	☒进口方是出口方的处理者或次级处理者 ☐ 进口方**不是**出口方的处理者或次级处理者（并且进口方受第三方控制者的指示）
英国 GDPR 是否适用于进口方	☐英国 GDPR 适用于进口方处理转移数据 ☒英国 GDPR 不适用于进口方处理转移数据
关联协议	**如果进口方是出口方的处理者或次级处理者**——载明了处理者或次级处理者处理转移数据指示的缔约方协议： 协议名称：如果适用，请参阅协议 协议日期：如果适用，请参阅协议 协议各方：如果适用，请参阅协议 参考号（如有）：如果适用，请参阅协议 **其他协议**——缔约方之间规定与转移数据相关的额外义务的任何协议，例如数据共享协议或服务协议： 协议名称：如果适用，请参阅协议 协议日期：如果适用，请参阅协议 协议各方：如果适用，请参阅协议 参考号（如有）如果适用，请参阅协议**如果出口方是处理者或次级处理者**——出口方与缔约方之间载明了出口方处理所转移数据指示的协议： 协议名称：如果适用，请参阅协议 协议日期：如果适用，请参阅协议 协议各方：如果适用，请参阅协议 参考号（如有）：如果适用，请参阅协议

期限	进口方可以在以下时段内处理转移的数据： ☒关联协议的有效期 ☐适用期： ☐（仅当进口方是控制者或不是出口方的处理者或次级处理者时）不超过目的所需的时间。
在期限结束前终止 IDTA	☒除非违反 IDTA 或经缔约方同意，否则缔约方不得在期限结束前终止 IDTA。 ☐缔约方可以通过以下方式在期限结束前终止 IDTA： 提前 个月发出书面通知，如第 29 节所述。（如何在不违反本 IDTA 的情况下终止本 IDTA）。
在获得批准的 IDTA 发生变更时终止 IDTA	哪一方可以依据第 29.2 节的规定终止 IDTA： ☒进口方 ☒出口方 ☐任意一方
进口方可以进一步转移已转移的数据吗？	☒进口方可以根据第 16.1 节（关于转移已转移的数据）将已转移数据转移给另一个组织或个人（不同的法律实体）。 ☐根据第 16.1 节（关于转移已转移的数据），进口方不得将已转移的数据转移给另一个组织或个人（不同的法律实体）。
进口方可以对已转移的数据进行转移时的具体限制	进口方只能根据第 16.1 节对已转移的数据进行转移： ☐如果出口方发出书面转移指示。 ☐接收方：

	☐转移给如下授权接收者（或授权接收者的类别）： ☒没有具体限制。
审查日期	☐无需审查，因为这是一次性转移，进口方不保留任何已转移的数据 首次审查日期： 缔约方必须按以下频率审查安全要求： ☐每 个月一次 ☐每季度一次 ☐每 6 个月一次 ☐每年一次 ☐每 年一次） ☒每次转移的数据、目的、进口方信息、TRA 或风险评估发生变化时

表 3：转移的数据

转移的数据	根据本 IDTA 发送给进口方的个人数据，包括： ☒提及的关联协议更新信息时，转移数据的类别将自动更新。 ☐提及的关联协议更新信息时，转移数据的类别不会自动更新。缔约方必须根据第 5.3 节就变更达成一致。
特殊类别的个人数据以及刑事定罪和罪行	转移的数据包括与以下各项相关的数据： ☐种族 ☐政治倾向 ☐宗教或哲学信仰

	☐工会会员 ☐遗传数据 ☐用于唯一识别自然人身份的生物特征数据 ☐身体或心理健康 ☐性生活或性取向 ☐刑事定罪和罪行 ☒以上皆非 ☐载于： 和： ☒提及的关联协议更新信息时，特殊类别和犯罪记录数据的类别将自动更新。 ☐提及的关联协议更新信息时，特殊类别和犯罪记录数据的类别不会自动更新。缔约方必须根据第 5.3 节就变更达成一致。
相关数据主体	转移的数据的数据主体是： ☒提及的关联协议更新信息时，数据主体的类别将自动更新。 ☐提及的关联协议更新信息时，数据主体的类别不会自动更新。缔约方必须根据第 5.3 节就变更达成一致。
用途	☐进口方可以出于以下目的处理转移的数据： ☐进口方可以出于协议规定的目的处理转移的数据。 在这两种情况下，与上述目的一致的任何其他目的。 ☒提及的关联协议更新信息时，目的将自动更新。

	□提及的关联协议更新信息时，目的不会自动更新。缔约方必须根据第 5.3 节就变更达成一致。

表 4：安全要求

传输的安全性	HP 定义了保护应用服务交易的控制措施。这些控制措施包括：验证和确认用户凭据、强制要求数字签名和加密、实施安全通信协议、在适当的网络安全区域内的服务器上存储在线交易详细信息。
存储的安全性	HP 的网络安全部门/组织和 HP 的法律部门为每种信息分类类型建立一套书面处理程序，并与负责数据隐私的部门一起处理任何相关事宜。处理程序说明：存储、传输、通信、访问、记录、保留、销毁、处置、事故管理泄露通知。 HP 信息技术部有一套用于识别技术信息资产的流程。 HP 识别其负责的所有资产，并对关键资产进行分类。 维护 HP 拥有的并由服务提供商从外部管理的信息资产和系统的记录。 还实施了书面服务器退役、孤立介质和旧介质流程，以确保对不可移除介质进行适当的管理和处置。
处理的安全性	根据政策，HP 内部的系统和支持软件的开发遵循安全的开发方法，以确保整个系统/软件生命周期的安全。软件开发生命周期定义了启动、开发/采集、实施、操作和处置要求。评估包括模块、库、服务和离散组件在内的所有系统组件，以确定它们对整体系统安全状态的影响。 HP 对系统应用程序和设备实施日志记录机制。HP 为包括但不限于电子邮件、办公生产力套件和 Internet 浏览器的操作软件的安装、配置、升级、测试和安全补丁制定了稳健的程序。 内部漏洞扫描每季度执行一次，在任何重大变更之后也执行一次。
组织安全措施	为了保护组织和客户的个人数据，HP 为包括工作站、服务器和网络设备在内的技术基础设施定义了一套最低限度的强化要求。工作站/服务器映像包含预强化的操作系统。强化要求因操作系统类型和实施的适用控制而异。 具有外部连接的系统将受到强化措施和防火墙的保护。面向外部的系统将

	放置在非军事区 (DMZ) 或其他类似配置中，以保护内部 HP 系统。 关键网络区域处于逻辑隔离状态。 远程访问 HP 内部网络上的设备（电子邮件系统除外）时需要使用 HP 标准 VPN 解决方案。 网络入侵检测/预防系统 (NIDS/NIPS) 放置在网络中的战略位置，并受到 24*7 的监控和管理。所有具有日志记录功能的设备，例如操作系统、数据库、应用程序、防火墙、路由器和交换机，都需要按照 HP 的日志记录和审计标准进行配置。 HP 安全政策和标准要求对介质进行安全处理。
技术安全最低要求	开发人员必须遵循为系统定义的代码标准和测试指南，以符合应用程序安全要求。源代码保护要求能够防止未经授权的访问。 执行初步测试并安排非生产补丁测试。发布来自非生产测试的反馈，安排并实施生产环境的实施。
安全要求更新	☒提及的关联协议更新信息时，安全要求将自动更新。 ☐提及的关联协议更新信息时，安全要求不会自动更新。缔约方必须根据第 5.3 节就变更达成一致。

第 2 部分：额外的保护条款

额外的保护条款：	
(i) 额外的技术安全保护	
(ii) 额外的组织保护	

(iii) 额外的合同保护	

第 3 部分：商业条款

商业条款	

第 4 部分：强制性条款

强制性条款	第 4 部分：已批准 IDTA 的强制性条款是 ICO 发布的模板 IDTA A.1.0，于 2022 年 2 月 2 日根据《2018 年数据保护法》第 s119A 条提交议会，并根据这些强制性条款的第 5.4 节进行了修订。

附件 5

标准合同条款（阿根廷）

根据《数据处理附录》第 6.3.1 条的规定，最初在阿根廷共和国收集的客户个人数据可能会应服务的需要转移到第三国。

如果前款所述的转移意味着将客户个人数据转移到被认为不能提供阿根廷适用数据保护和隐私法律所规定的适当保护程度的国家/地区，则应对转移应用附件 2 中包含的欧盟标准合同条款和下文规定的修改。

1. 第 1 条 (a)、(c) 和 (e) 项应替换如下：

   (a) *“个人数据”*、*“敏感数据”*、*“处理/正在处理”*、*“控制者”*、*“处理者”*、*“数据主体”和“监管机构”*的含义与《阿根廷第 25.326 号数据保护法》、第 1558/2001 号监管法令及其补充条例（不时修订或替换）中规定的含义相同；

   (c) *“数据进口方”*指位于阿根廷境外的从数据出口方接收个人数据以根据本协议的条款进行处理的服务提供商；

   (e) *“适用的数据保护法”*是指《阿根廷第 25,326 号数据保护法》及其配套法规（不时修订或替换）。

2. 第 4 条 (f) 项应替换如下：

   (f) 数据主体已被告知或将在转移之前或之后尽快被告知，其数据可能被转移到无法提供《阿根廷第 25,326 号数据保护法》及其配套法规（不时修订或更换）所规定的适当保护程度的第三国。

3. 第 7 条第 1 小节 (b) 项应替换如下：

   (b) 将争议提交阿根廷共和国的司法和行政管辖区域。

4. 第 9 条应替换如下：

本协议应受阿根廷共和国法律的管辖，特别是第 25,326 号法律、阿根廷数据保护局颁布的法规和处置方法（不时修订或替换）。

附件 5：个人信息出境标准合同（中国）

为了确保境外接收方处理个人信息的活动达到中华人民共和国相关法律法规规定的个人信息保护标准，明确个人信息处理者和境外接收方个人信息保护的权利和义务，经缔约方协商一致，订立本合同。

个人信息处理者：_____

地址：_____

联系方式：_____

联系人：_____职务：_____

境外接收方：_____

地址：_____

联系方式：_____

联系人：_____职务：_____

个人信息处理者与境外接收方依据本合同约定开展个人信息出境活动，与此活动相关的商业行为，缔约方【已】/【约定】于____年__月__日订立_____（商业合同，如有）。

本合同正文根据《个人信息出境标准合同办法》的要求拟定，在不与本合同正文内容相冲突的前提下，缔约方如有其他约定可在附录二中详述，附录构成本合同的组成部分。

第一条 定义

在本合同中，除上下文另有规定外：

（一）“个人信息处理者”是指在个人信息处理活动中自主决定处理目的、处理方式的，向中华人民共和国境外提供个人信息的组织、个人。

（二）“境外接收方”是指在中华人民共和国境外自个人信息处理者处接收个人信息的组织、个人。

（三）个人信息处理者或者境外接收方单称“一方”，合称“缔约方”。

（四）“个人信息主体”是指个人信息所识别或者关联的自然人。

（五）“个人信息”是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

（六）“敏感个人信息”是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

（七）“监管机构”是指中华人民共和国省级以上网信部门。

（八）“相关法律法规”是指《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国民法典》《中华人民共和国民事诉讼法》《个人信息出境标准合同办法》等中华人民共和国法律法规。

（九）本合同其他未定义术语的含义与相关法律法规规定的含义一致。

第二条 个人信息处理者的义务

个人信息处理者应当履行下列义务：

（一）按照相关法律法规规定处理个人信息，向境外提供的个人信息仅限于实现处理目的所需的最小范围。

（二）向个人信息主体告知境外接收方的名称或者姓名、联系方式、附录一“个人信息出境说明”中处理目的、处理方式、个人信息的种类、保存期限，以及行使个人信息主体权利的方式和程序等事项。向境外提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

（三）基于个人同意向境外提供个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

（四）向个人信息主体告知其与境外接收方通过本合同约定个人信息主体为第三方受益人，如个人信息主体未在 30 日内明确拒绝，则可以依据本合同享有第三方受益人的权利。

（五）尽合理地努力确保境外接收方采取如下技术和管理措施（综合考虑个人信息处理目的、个人信息的种类、规模、范围及敏感程度、传输的数量和频率、个人信息传输及境外接收方的保存期限等可能带来的个人信息安全风险），以履行本合同约定的义务：

（如加密、匿名化、去标识化、访问控制等技术和管理措施）

_____

（六）根据境外接收方的要求向境外接收方提供相关法律规定和技术标准的副本。

（七）答复监管机构关于境外接收方的个人信息处理活动的询问。

（八）按照相关法律法规对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。重点评估以下内容：

1．个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性。

2．出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险。

3．境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全。

4．个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等。

5．按照本合同第四条评估当地个人信息保护政策和法规对合同履行的影响。

6．其他可能影响个人信息出境安全的事项。

保存个人信息保护影响评估报告至少 3 年。

（九）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（十）对本合同义务的履行承担举证责任。

（十一）根据相关法律法规要求，向监管机构提供本合同第三条第十一项所述的信息，包括所有合规审计结果。

第三条 境外接收方的义务

境外接收方应当履行下列义务：

（一）按照附录一“个人信息出境说明”所列约定处理个人信息。如超出约定的处理目的、处理方式和处理的个人信息种类，基于个人同意处理个人信息的，应当事先取得个人信息主体的单独同意；涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。

（二）受个人信息处理者委托处理个人信息的，应当按照与个人信息处理者的约定处理个人信息，不得超出与个人信息处理者约定的处理目的、处理方式等处理个人信息。

（三）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（四）采取对个人权益影响最小的方式处理个人信息。

（五）个人信息的保存期限为实现处理目的所必要的最短时间，保存期限届满的，应当删除个人信息（包括所有备份）。受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销或者终止的，应当将个人信息返还个人信息处理者或者予以删除，并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

（六）按下列方式保障个人信息处理安全：

1．采取包括但不限于本合同第二条第五项的技术和管理措施，并定期进行检查，确保个人信息安全。

2．确保授权处理个人信息的人员履行保密义务，并建立最小授权的访问控制权限。

（七）如处理的个人信息发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问，应当开展下列工作：

1．及时采取适当补救措施，减轻对个人信息主体造成的不利影响。

2．立即通知个人信息处理者，并根据相关法律法规要求报告监管机构。通知应当包含下列事项：

⑴ 发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问的个人信息种类、原因和可能造成的危害。

⑵ 已采取的补救措施。

⑶ 个人信息主体可以采取的减轻危害的措施。

⑷ 负责处理相关情况的负责人或者负责团队的联系方式。

3．相关法律法规要求通知个人信息主体的，通知的内容包含本项第 2 目的事项。受个人信息处理者委托处理个人信息的，由个人信息处理者通知个人信息主体。

4．记录并留存所有与发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问有关的情况，包括采取的所有补救措施。

（八）同时符合下列条件的，方可向中华人民共和国境外的第三方提供个人信息：

1．确有业务需要。

2．已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向第三方提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外。

3．基于个人同意处理个人信息的，应当取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，应当取得书面同意。

4．与第三方达成书面协议，确保第三方的个人信息处理活动达到中华人民共和国相关法律法规规定的个人信息保护标准，并承担因向中华人民共和国境外的第三方提供个人信息而侵害个人信息主体享有权利的法律责任。

5．根据个人信息主体的要求向个人信息主体提供该书面协议的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对该书面协议相关内容进行适当处理。

（九）受个人信息处理者委托处理个人信息，转委托第三方处理的，应当事先征得个人信息处理者同意，要求该第三方不得超出本合同附录一“个人信息出境说明”中约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督。

（十）利用个人信息进行自动化决策的，应当保证决策的透明度和结果公平、公正，不得对个人信息主体在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人信息主体

进行信息推送、商业营销的，应当同时提供不针对其个人特征的选项，或者向个人信息主体提供便捷的拒绝方式。

（十一）承诺向个人信息处理者提供已遵守本合同义务所需的必要信息，允许个人信息处理者对必要数据文件和文档进行查阅，或者对本合同涵盖的处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利。

（十二）对开展的个人信息处理活动进行客观记录，保存记录至少 3 年，并按照相关法律法规要求直接或者通过个人信息处理者向监管机构提供相关记录文件。

（十三）同意在监督本合同实施的相关程序中接受监管机构的监督管理，包括但不限于答复监管机构询问、配合监管机构检查、服从监管机构采取的措施或者作出的决定、提供已采取必要行动的书面证明等。

第四条 境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响

（一）缔约方应当保证在本合同订立时已尽到合理注意义务，未发现境外接收方所在国家或者地区的个人信息保护政策和法规（包括任何提供个人信息的要求或者授权公共机关访问个人信息的规定）影响境外接收方履行本合同约定的义务。

（二）缔约方声明，在作出本条第一项的保证时，已经结合下列情形进行评估：

1．出境的具体情况，包括个人信息处理目的、传输个人信息的种类、规模、范围及敏感程度、传输的规模和频率、个人信息传输及境外接收方的保存期限、境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生个人信息安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况。

2．境外接收方所在国家或者地区的个人信息保护政策和法规，包括下列要素：

⑴该国家或者地区现行的个人信息保护法律法规及普遍适用的标准。

⑵ 该国家或者地区加入的区域性或者全球性的个人信息保护方面的组织，以及所作出的具有约束力的国际承诺。

⑶)该国家或者地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。

3．境外接收方安全管理制度和技术手段保障能力。

（三）境外接收方保证，在根据本条第二项进行评估时，已尽最大努力为个人信息处理者提供了必要的相关信息。

（四）缔约方应当记录根据本条第二项进行评估的过程和结果。

（五）因境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，境外接收方应当在知道该变化后立即通知个人信息处理者。

（六）境外接收方接到所在国家或者地区的政府部门、司法机构关于提供本合同项下的个人信息要求的，应当立即通知个人信息处理者。

第五条 个人信息主体的权利

缔约方约定个人信息主体作为本合同第三方受益人享有以下权利：

（一）个人信息主体依据相关法律法规，对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理，有权要求查阅、复制、更正、补充、删除其个人信息，有权要求对其个人信息处理规则进行解释说明。

（二）当个人信息主体要求对已经出境的个人信息行使上述权利时，个人信息主体可以请求个人信息处理者采取适当措施实现，或者直接向境外接收方提出请求。个人信息处理者无法实现的，应当通知并要求境外接收方协助实现。

（三）境外接收方应当按照个人信息处理者的通知，或者根据个人信息主体的请求，在合理期限内实现个人信息主体依照相关法律法规所享有的权利。

境外接收方应当以显著的方式、清晰易懂的语言真实、准确、完整地告知个人信息主体相关信息。

（四）境外接收方拒绝个人信息主体的请求的，应当告知个人信息主体其拒绝的原因，以及个人信息主体向相关监管机构提出投诉和寻求司法救济的途径。

（五）个人信息主体作为本合同第三方受益人有权根据本合同条款向个人信息处理者和境外接收方的一方或者缔约方主张并要求履行本合同项下与个人信息主体权利相关的下列条款：

1．第二条，但第二条第五项、第六项、第七项、第十一项除外。

2．第三条，但第三条第七项第 2 目和第 4 目、第九项、第十一项、第十二项、第十三项除外。

3．第四条，但第四条第五项、第六项除外。

4．第五条。

5．第六条。

6．第八条第二项、第三项。

7．第九条第五项。

上述约定不影响个人信息主体依据《中华人民共和国个人信息保护法》享有的权益。

第六条 救济

（一）境外接收方应当确定一个联系人，授权其答复有关个人信息处理的询问或者投诉，并应当及时处理个人信息主体的询问或者投诉。境外接收方应当将联系人信息告知个人信息处理者，并以简洁易懂的方式，通过单独通知或者在其网站公告，告知个人信息主体该联系人信息，具体为：

联系人及联系方式（办公电话或电子邮箱）_____

（二）一方因履行本合同与个人信息主体发生争议的，应当通知另一方，缔约方应当合作解决争议。

（三）争议未能友好解决，个人信息主体根据第五条行使第三方受益人的权利的，境外接收方接受个人信息主体通过下列形式维护权利：

1．向监管机构投诉。

2．向本条第五项约定的法院提起诉讼。

（四）缔约方同意个人信息主体就本合同争议行使第三方受益人权利，个人信息主体选择适用中华人民共和国相关法律法规的，从其选择。

（五）缔约方同意个人信息主体就本合同争议行使第三方受益人权利的，个人信息主体可以依据《中华人民共和国民事诉讼法》向有管辖权的人民法院提起诉讼。

（六）缔约方同意个人信息主体所作的维权选择不会减损个人信息主体根据其他法律法规寻求救济的权利。

第七条 合同解除

（一）境外接收方违反本合同约定的义务，或者境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，个人信息处理者可以暂停向境外接收方提供个人信息，直到违约行为被改正或者合同被解除。

（二）有下列情形之一的，个人信息处理者有权解除本合同，并在必要时通知监管机构：

1．个人信息处理者根据本条第一项的规定暂停向境外接收方提供个人信息的时间超过 1 个月。

2．境外接收方遵守本合同将违反其所在国家或者地区的法律规定。

3．境外接收方严重或者持续违反本合同约定的义务。

4．根据境外接收方的主管法院或者监管机构作出的终局决定，境外接收方或者个人信息处理者违反了本合同约定的义务。

在本项第 1 目、第 2 目、第 4 目的情况下，境外接收方可以解除本合同。

（三）经缔约方同意解除本合同的，合同解除不免除其在个人信息处理过程中的个人信息保护义务。

（四）合同解除时，境外接收方应当及时返还或者删除其根据本合同所接收到的个人信息（包括所有备份），并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

第八条 违约责任

（一）缔约方应就其违反本合同而给对方造成的损失承担责任。

（二）任何一方因违反本合同而侵害个人信息主体享有的权利，应当对个人信息主体承担民事法律责任，且不影响相关法律法规规定个人信息处理者应当承担的行政、刑事等法律责任。

（三）缔约方依法承担连带责任的，个人信息主体有权请求任何一方或者缔约方承担责任。一方承担的责任超过其应当承担的责任份额时，有权向另一方追偿。

第九条 其他

（一）如本合同与缔约方订立的任何其他法律文件发生冲突，本合同的条款优先适用。

（二）本合同的成立、效力、履行、解释、因本合同引起的缔约方间的任何争议，适用中华人民共和国相关法律法规。

（三）发出的通知应当以电子邮件、电报、电传、传真（以航空信件寄送确认副本）或者航空挂号信发往（具体地址）_____或者书面通知取代该地址的其它地址。如以航空挂号信寄出本合同项下的通知，在邮戳日期后的__天应当视为收讫；如以电子邮件、电报、电传或者传真发出，在发出以后的__个工作日应当视为收讫。

（四）缔约方因本合同产生的争议以及任何一方因先行赔偿个人信息主体损害赔偿责任而向另一方的追偿，缔约方应当协商解决；协商解决不成的，任何一方可以采取下列第__种方式加以解决（如选择仲裁，请勾选仲裁机构）：

1．仲裁。将该争议提交

□中国国际经济贸易仲裁委员会

□中国海事仲裁委员会

□北京仲裁委员会（北京国际仲裁中心）

□上海国际仲裁中心

□其他《承认及执行外国仲裁裁决公约》成员的仲裁机构_____

按其届时有效的仲裁规则在（仲裁地点）_____进行仲裁；

2．诉讼。依法向中华人民共和国有管辖权的人民法院提起诉讼。

（五）本合同应当按照相关法律法规的规定进行解释，不得以与相关法律法规规定的权利、义务相抵触的方式解释本合同。

（六）本合同正本一式__份，缔约方各执__份，其法律效力相同。

本合同在_____（地点）签订

个人信息处理者：_____

____年__月__日

境外接收方：_____

____年__月__日

附录 I

个人信息出境说明

根据本合同向境外提供个人信息的详情约定如下：

（一）处理目的：

（二）处理方式：

（三）出境个人信息的规模：

（四）出境个人信息种类（参考 GB/T 35273《信息安全技术个人信息安全规范》和相关标准）：

（五）出境敏感个人信息种类（如适用，参考 GB/T35273《信息安全技术 个人信息安全规范》和相关标准）：（六）境外接收方只向以下中华人民共和国境外第三方提供个人信息（如适用）：

（七）传输方式：

（八）出境后保存期限：

（ 年 月 日至 年 月 日）

（九）出境后保存地点：

（十）其他事项（视情况填写）：

附录 II

缔约方约定的其他条款（如需要）

附件 III

技术和组织措施

1. 组织

HP 设立了一个信息安全组织，负责指导和管理组织的信息安全策略和控制措施。HP 还部署了信息安全框架/管理系统，以确保符合 HP 的安全政策和控制措施，并确认遵守其客户的安全要求。该框架的结构与 NIST 网络安全框架保持一致，每年审查一次。

2. 资产管理

HP 制定了一个用于识别技术信息资产的流程，通过此流程，HP 可以识别其负责的所有资产并对关键资产进行分类。HP 还为每种信息分类类型（包括那些包含个人数据的资产）建立一套书面处理程序。处理程序中说明了存储、传输、通信、访问、记录、保留、销毁、处置、事故管理和信息泄露通知。

3. 访问控制

最小权限原则用于提供逻辑访问控制。通过唯一的用户 ID 和密码提供用户访问权限。HP 的密码策略定义了复杂性、强度、有效性和密码历史相关控制。访问权限会定期审查，并在人员调离岗位时撤销。

用户帐户创建和删除程序，在实施缔约方同意的前提下，将被实现，以授予和撤销协议期间使用的客户端系统访问权限。

4. 人员培训

HP 员工必须完成 Integrity at HP 培训，该培训旨在确保员工熟悉用于管理 HP 的道德行为、卓越和合规期望的项目、政策和资源。Integrity at HP 提供安全和数据隐私模块，员工还需要参加年度“进修”课程。HP 员工还必须完成每年更新的专门安全意识培训，该培训重点关注基本安全政策，并强调员工在事故管理、数据隐私和信息安全方面的责任。

5. 第三方和分包商

HP 制定了适当的流程来甄选能够遵守全面合同安全要求的分包商。

对于适用的供应商（处理/存储/传输 HP 数据和 HP 拥有的客户自有数据或有权访问 HP 网络的供应商），HP 网络安全部门将执行风险评估以验证是否制定了信息安全计划。适足的计划必须包括物理、技术和管理保障。完成此评估后，供应商才能访问 HP 信息。

6. 系统安全

根据政策，HP 内部的系统和支持软件的开发遵循安全的开发方法，以确保整个系统/软件生命周期的安全。软件开发生命周期定义了启动、开发/采集、实施、操作和处置要求。评估包括模块、库、服务和离散组件在内的所有系统组件，以确定它们对整体系统安全状态的影响。

HP 定义了保护应用服务交易的控制措施。这些控制措施包括：验证和确认用户凭据、强制要求数字签名和加密、实施安全通信协议、在适当的网络安全区域内的服务器上存储在线交易详细信息。

定期执行内部漏洞扫描。

7. 物理和环境安全

HP 设施使用各种物理和电子访问控制和监控功能实现保护。根据设施的不同，这可能包括安保、电子访问控制和闭路电视 (CCTV)。

所有 HP 人员均已注册，并且必须携带适当的身份名牌。

设施具有所需的基础设施支持，可在需要时提供温度控制和备用电源，通过 UPS 和/或柴油发电机来支持关键服务。

8. 运营管理

HP 为技术基础设施定义了一套最低强化要求，包括工作站、服务器和网络设备。工作站/服务器映像包含预强化的操作系统。强化要求因操作系统类型和实施的适用控制而异。

HP 已在网络内部署了网络入侵检测/预防系统 (NIDS/NIPS)，并提供 24*7 的监控和管理。

HP 安全政策和标准要求对介质进行安全处理。

9. 加密技术

HP 定义了一套强大的加密流程，以确保信息资产的机密性、完整性和可用性。批准的协议要求对某些资产进行加密，包括那些包含个人数据的资产。

10. 信息安全事故管理

HP 遵循已制定的网络事故管理流程，该流程涉及目的、范围、角色、职责、管理层承诺、组织协调、实施程序和合规性检查。HP 每年都会审查和更新此流程。

HP 拥有一支受过事故响应和危机管理培训的网络安全人员组成的网络事故响应团队，负责对流程和任何事故或事件定期进行公开审查。

12. 业务连续性管理

HP 制定了一项全球运营连续性计划。该计划通过一组协作、标准化和内部记录的规划流程，采用涉及全公司范围的整体式方法来实现端到端的连续性。

HP 定期执行其业务连续性计划以确保其有效性。HP 目前至少每年测试和更新所有计划一次，并确保对业务连续性计划涉及的人员进行培训。