2019

客户个人信息保护协议

供应商适用

LVMH
WATCHES & JEWELRY

目录

第 1 条：目的

本客户个人信息保护协议（本“协议”）由路威酩轩钟表珠宝商贸（上海）有限公司（“LVMH W&J”）和【插入供应商名称】（“供应商”）于【插入日期】订立。本协议并入《一般服务购买协议》，并构成该协议的一部分。如本协议与《一般服务购买协议》之间有任何冲突或不一致，以本协议所载条款和条件为准。

第 2 条：范围

本协议承认，供应商和 LVMH W&J（以下统称为“双方”）可讨论 LVMH W&J 客户的或与之相关的客户个人信息（定义见下文，下称“客户个人信息”）。本协议所载条文界定了在不同情况下供应商该如何保护客户个人信息，并包含 LVMH W&J 可就违规行为采取的救济、处罚和法律行动。

双方同意，保护客户个人信息符合其最佳利益，且本协议条款在双方之间建立了信任和保密关系。

即使本协议因任何原因终止或期满，本条规定仍然有效。

第 3 条：定义

“**客户**”指向 LVMH W&J 或其子公司（合称“LVMH W&J”）购买商品或服务以及通过任何渠道留下客户个人信息的人或组织。

“**生命周期管理**”指客户个人信息管理可能涉及以下一种或多种情况：客户个人信息的收集、存储、处理、分享、传输、披露和销毁。

“**供应商**”指向 LVMH W&J 提供产品或服务并获得报酬的个人或实体。供应商可适用于下列一种或多种情况：

1. “**客户个人信息委托管理**”。供应商代表 LVMH W&J 进行客户个人信息的生命周期管理。LVMH W&J 作为数据控制者，供应商作为数据处理者。
2. “**委托开发**”。供应商为 LVMH W&J 开发和/或运营数字渠道。
3. “**数据共同控制者**”。请参阅“数据共同控制者”的定义。

“个人信息”指以电子或任何其他方式记录并可单独或与其他信息相结合用于识别特定自然人身份或者反映特定自然人活动情况的各种信息。

注：个人信息包括姓名、出生日期、身份证号码、个人生物特征信息、居住地址、联系方式、通信记录及内容、账户密码、财产信息、信用信息、行踪轨迹、酒店住宿信息、健康及生理信息、交易信息等。

“客户个人信息”(“CPI”)指 LVMH W&J 的客户的个人信息。

除 LVMH W&J 和供应商作为数据共同控制者的情况外，客户个人信息归 LVMH W&J 独家所有。

“客户个人敏感信息”指一旦泄露、非法提供或滥用可能危及客户的人身和财产安全，极易导致个人名誉、身心健康受到损害或导致歧视性待遇等的客户个人信息。

注：个人敏感信息包括身份证号码、生物特征信息、银行账号、通信记录和内容、财产信息、信用信息、行踪轨迹、酒店住宿信息、健康及生理信息、交易信息、14 岁以下（含）儿童的个人信息等。

“同意”指客户通过书面声明或主动作出肯定性行动对其个人信息进行生命周期管理作出明确授权的行为。

注：肯定性行动包括客户主动作出声明（电子、纸质或口头形式）、主动勾选、主动点击“同意”、“注册”、“发送”、“拨打”等。

“数字渠道”指经 LVMH W&J 授权，供应商进行客户个人信息生命周期管理活动所使用的网络渠道/平台/场景/应用，如公司网站、客户数字卡、移动应用程序(苹果或安卓)、微信公众号、微信小程序、微博、天猫、京东等。

“数据共同控制者”指供应商作为数据控制者，拥有供应商收集并随后传输给 LVMH W&J 的个人信息并对该等个人信息进行生命周期管理。在个人信息传输给 LVMH W&J 后，该等信息可被视作客户个人信息，此时，LVMH W&J 和供应商成为数据共同控制者并共享客户个人信息的所有权。

“安全事件”指从可用性、完整性、保密性和可追溯性角度而言，影响或很可能影响客户个人信息安全的任何事件。

“数据泄露”指导致客户个人信息被意外或非法销毁、遗失、篡改、未经授权披露或访问的任何事件。数据泄露构成安全事件。

第 4 条：具体条文

客户个人信息的收集

适用范围

如属客户个人信息委托管理，供应商应遵守第 4 条第 1-4 款的要求；

如作为数据共同控制者，供应商应遵守第 4 条第 1-5 款的要求。

条款

1. 在就有关客户个人信息的类型、收集方式、收集频率、收集目的等取得 LVMH W&J 授权后，供应商方可收集客户个人信息。应当根据适用法律规定依法收集客户个人信息。因此，供应商不得
    a) 欺骗、哄骗或者强迫客户提供其个人信息。
    b) 隐瞒产品或服务的个人信息收集功能。
    c) 从非法来源获取个人信息。
    d) 获取适用法律不允许收集的个人信息。
    e) 从 LVMH W&J 或适用法律认为不合适的渠道收集个人信息。

    未经 LVMH W&J 的书面授权，供应商不得收集客户个人信息。如果供应商认为需要额外收集客户个人信息，应提前至少 1 周与 LVMH W&J 沟通， 并取得书面授权。LVMH W&J 不对因供应商非法收集客户个人信息而引起的任何法律纠纷负责。

    供应商收集客户个人信息时应遵循适用法律规定的最低收集原则，不得超出 LVMH W&J 授权的收集范围（客户个人信息的类型、收集方式、收集频率、收集目的等）。
2. 当供应商通过数字渠道或其他方式（如实体店线下收集渠道、商业活动）收集客户个人信息时，供应商应明确告知客户所提供的产品或服务的不同业务功能分别将收集的客户个人信息类型，以及客户个人信息的收集和使用规则，以获得客户的同意。告知客户的方式包括：
    a) 供应商有义务在本协议第 3 条定义的各数字渠道上发布及维护 LVMH W&J 提供的隐私政策。

i. LVMH W&J 提供的隐私政策应予以公布并易于获取，例如在数字渠道首页的显著位置插入链接。

ii. 隐私政策应作为一份独立文件，与用户协议分开。

iii. 除数字渠道外，在其他情况下，应当通过合同、链接、消息、电子邮件或其他方式向各客户交付隐私政策；如果成本过高或存在重大困难，可采用公告的形式发布隐私政策。

iv. LVMH W&J 提供的隐私政策发生变动时，供应商应就重新通知客户向 LVMH W&J 提供必要的协助，并在收集客户个人信息的各种情景下更新 LVMH W&J 提供的隐私政策。

b) 在无法告知客户隐私政策的情况下，供应商应通过发送邮件、打电话或推送通知的方式，告知客户所提供的产品或服务的不同业务功能分别将收集的客户个人信息类型，以及客户个人信息的收集和使用规则。

如果因处理所收集的个人信息而产生的信息被视作客户个人信息，应在客户的授权范围内处理新产生的客户个人信息。如超出客户的授权范围，供应商应：

a) 按照本协议第 4.2(a)、(b)条的规定通知客户并重新获得客户的同意。

b) 如适用，在 5 个工作日内通知 LVMH W&J 更新隐私政策。

3. 对于客户个人敏感信息的收集，客户的同意必须是自愿的、具体的、明确的，并以对收集的充分了解为基础。

业务功能是核心业务功能还是附加功能，应由供应商与 LVMH W&J 的 IS&T/法务部/事业部确认。

在通过主动提供或自动收集方式收集客户个人敏感信息之前，供应商应：

a) 告知客户所提供的产品或服务的核心业务功能，以及针对核心功能需要收集的客户个人敏感信息；明确告知客户由于拒绝提供同意而造成的影响（如，为客户提供的产品或服务可能无法正常使用）。应允许客户选择是否提供此类信息或同意自动收集。

b) 如产品或服务提供其他附加功能，当需要收集客户个人敏感信息时，供应商应在收集前逐一告知客户为执行附加功能而需要提供的客户个人敏感信息，允许客户自行选择是否逐一为各附加功能提供该等信息或同意自动收集。如果客户拒绝，可能无法提供相应的附加功能，但供应商不得因此停止提供核心业务功能，并应保证相应的服务质量。

注 1：通知方式可参考本协议第 4.2(a)(b)条。

注 2：功能接口是一种可用于通知客户业务功能及各项业务功能所需的客户个人信息的可选方法。供应商应在收集客户个人敏感信息之前（如产品安装过程中，或客户首次使用产品或服务时，或客户注册帐户时），主动为客户提供功能接口。

c) 供应商不得代表 LVMH W&J 收集或处理 18 岁以下未成年人的客户个人信息。如果供应商拥有该等客户个人信息，且该等客户个人信息是代表 LVMH W&J 收集的，则供应商应删除相应的客户个人信息。

4. 供应商只能通过数字渠道向通过数字渠道提交真实身份信息的客户提供产品和服务（如供应商应通过收集客户手机号码来部署客户身份验证机制，并发送验证码来验证手机号码的真实性）。如果供应商拒绝履行本协议规定的义务或未能作出更正，则其应自负费用承担适用法律（如《中华人民共和国网络安全法》）中规定的可能经济处罚。

5. 作为数据共同控制者，供应商应制定一套全面的隐私政策，且供应商的客户个人信息收集和后续处理活动应严格遵守该政策。供应商隐私政策的内容包括但不限于：

a) 供应商的基本信息，包括注册名称、注册地址、办公地址、负责人联系方式等。

b) 收集和处理客户个人信息的目的及该目的所涵盖的业务功能，如利用客户个人信息推送商业广告、利用客户个人信息形成直接的用户画像及其用途等。

c) 各业务功能分别收集的客户个人信息，客户个人信息处理规则（涵盖收集方法和频率、存储位置和期限以及拟收集的客户个人信息实际范围）。

d) 分享、传输和公开披露客户个人信息的目的、所涉及的客户个人信息的类型、接收客户个人信息的第三方类型以及相应法律责任。

e) 保障客户个人信息安全所遵循的基本原则、控制者的数据安全能力以及所采取的客户个人信息安全措施。

f) 个人数据主体的权利和实现该等权利的机制，如访问方法、更正方法、删除方法、账户关闭方法、撤销同意的方法、取得客户个人信息副本的方法以及阻止信息系统自动决策的方法等。

g) 提供客户个人信息之后可能面临的安全风险以及未能提供客户个人信息可能造成的影响。

h) 响应客户问询和投诉的渠道和机制、外部争议解决机构及其联系方式。

供应商的隐私政策应予以发布并易于获取，例如在在供应商网站首页、手机应用程序安装页面、社交媒体首页等显著位置插入链接；隐私政策应作为一份独立文件，与用户协议分开；应当通过合同、链接、消息、电子邮件或其他方式向各客户交付隐私政策；如果成本过高或存在重大困难，可采用公告的形式发布隐私政策；本条款中第 a)至 h)项所述事项如有变更，应及时更新隐私政策并重新通知客户。

供应商应了解违反上述要求的潜在后果（如因非法收集而被相关监管部门要求删除客户个人信息）。供应商应尽一切努力确保遵守适用法律的规定，并将因违反适用法律给 LVMH W&J 业务造成的任何潜在干扰降至最低。供应商应向 LVMH W&J 赔偿 LVMH W&J 因该等业务中断而产生的实际成本。

客户个人信息的存储

适用范围

如属客户个人信息委托管理，供应商应遵守第 4 条第 6-8 款的要求；

如为委托开发，供应商应遵守第 4 条第 9 款的要求；

如作为数据共同控制者，供应商应遵守第 4 条第 7 款的要求。

条款

6. 如果供应商向 LVMH W&J 提供的服务涉及和/或依赖于存储所收集的客户个人信息，则除非事先获得 LVMH W&J 的明确书面批准，供应商仅限在中国境内存储客户个人信息。

   供应商应遵循下列原则，确保有效实施数据最小化和有限保留：

   a) 请参阅《一般服务购买协议》附件五第 2.2 条（委托服务提供商处理个人数据）。

   b) 应从物理上分别存储客户个人信息和属于供应商、供应商的其他客户或任何第三方的其他数据。

7. 供应商应保持服务资源与客户数量的匹配程度，并按照 LVMH W&J 的服务质量要求，始终保持数据分析能力、系统维护能力和信息安全能力。

供应商应从管理和技术角度确定拟将采取的适当安全措施，以加强数据保护能力，并将发生潜在风险的可能性（如客户个人信息泄漏、销毁和丢失）和影响（如泄露客户个人信息可能损害客户的利益）限制在可接受的水平。

在任何情况下，安全措施应符合良好行业惯例的安全规定或市场上可用的先进技术标准。供应商应按 LVMH W&J 的要求，向其提供正式授权人员名单和审计记录。

供应商应了解违反上述要求的潜在后果（如因泄露客户个人信息导致数据不可用或不完整）。供应商应尽一切努力确保遵守适用法律的规定，并将因违反适用法律给 LVMH W&J 业务造成的任何潜在干扰降至最低。供应商应向 LVMH W&J 赔偿 LVMH W&J 因该等业务中断而产生的实际成本。

具体要求请参阅本协议附件 A。

了解更多要求，请参阅《一般服务购买协议》附件五第 1.1 条（一般安全义务）和第 2.4 条（处理的安全性和保密性）。

8. 如果供应商收到任何客户的个人信息相关请求或行使权利的请求，

   a) 请参阅《一般服务购买协议》附件五第 1.1 条（一般安全义务）。

   注 1：客户的权利包括：访问权、客户个人信息修正或删除权、限制（阻止）处理客户个人信息的权利权、反对基于画像作出决定的权利、数据迁移权、撤回同意权。

9. 供应商有义务为含有客户个人信息的系统取得信息安全技术网络安全保护 MLPS 2.0 认证。认证到期后，须更新证书。

客户个人信息的处理

适用范围

如属客户个人信息委托管理，供应商应遵守第 4 条第 10-18 款的要求；

如属委托开发，供应商应遵守第 4 条第 19 款的要求。

条款

10. 供应商应保存一份代表 LVMH W&J 开展的处理活动的登记册。请参阅《一般服务购买协议》附件五第 2.3 条（处理活动登记册）。

11. 客户个人信息的处理不得超出客户授权的范围。如果确有必要在上述范围之外处理客户个人信息，供应商应取得客户的同意（请参阅第 4.2 条和第 4.3 条）。

    在特定情况下，如果无需明确指明身份，供应商应开展间接用户画像，避免精确指向具体个人，如向客户推送商业广告等。

12. 如果供应商委托分包商处理客户个人信息，供应商应参阅《一般服务购买协议》附件五第 2.6 条（分包商）的相关规定。

    在任何情况下，供应商应始终就其分包商履行义务对 LVMH W&J 承担全部责任。

13. 如果供应商与第三方合并、被第三方合并或直接或间接受第三方控制，

    a) 则未经 LVMH W&J 事先书面授权，供应商不得向该第三方披露 LVMH W&J 的任何客户个人信息，并应按照 LVMH W&J 的要求直接向 LVMH W&J 交还该等客户个人信息或永久销毁其持有的全部客户个人信息。

    b) 但是，如果经 LVMH W&J 事先书面授权，供应商可继续处理客户个人信息，且处理客户个人信息时应始终遵守本协议及适用法律的规定。本协议中规定的供应商责任应由合并后的实体继承。

14. 对于安全事件，供应商应：

    a) 为响应安全事件制订一套应急计划，包括工作职责、事件响应策略和程序等。该应急计划应定期更新或根据相关法律法规的变化以及安全事件处置结果及时更新。

    b) 定期（至少一年一次）为供应商员工组织事件响应培训和应急演习，告知其工作职责以及应急响应策略和程序。

    c) 供应商应在 LVMH W&J 规定的期限内，起草、收集并提供遵守适用法律、良好行业惯例所需的或 LVMH W&J 要求的任何可用材料（包括但不限于相关记录、日志、文件、数据报告）。有关客户个人信息安全事件的材料应包含以下内容：

        i. 事件内容，包括但不限于发现事件的人员、事件汇报对象、时间和地点、所涉及的客户个人信息及客户数量、发生事件的系统名称、对其他相关系统的影响。

        ii. 对事件可能造成的影响的评估结果、为控制局面和消除隐患需采取的措施、相关责任人及其联系方式以及因事件导致的任何变更（补充、修改或删除）。

d) 更多要求及相关赔偿问题，请参阅《一般服务购买协议》附件五第 1.3 条（安全事件及数据泄露管理和通知）。

e) 恶意程序相关要求，请参阅《一般服务购买协议》附件五第 1.2 条（恶意程序）。

15. 根据适用法律的规定，供应商同意通过以下方式完善其组织管理：

a) 制定客户个人信息保护计划或政策，确保法定代表人或组织负责人全面负责监管客户个人信息的安全，包括提供人力、财力和物力履行客户个人信息的安全使命。

b) 指定一名人员和一个部门监督客户个人信息保护情况。

c) 如果供应商处理了超过 1,000,000 人的客户个人信息，或预计在未来 12 个月内将处理超过 1,000,000 人的客户个人信息，或供应商的主营业务涉及个人信息处理，且员工人数超过 200 人，则供应商应指定一名专职主管负责客户个人信息保护工作，并成立客户个人信息保护部门负责客户个人信息安全工作。

d) 客户个人信息保护主管和客户个人信息保护部门须履行的责任包括但不限于：

i. 计划和实施组织内部的客户个人信息安全工作，并直接负责客户个人信息安全工作。

ii. 制定、发布、实施并定期更新隐私政策及相关规范。

iii. 建立、保持并更新一份由供应商处理的客户个人信息清单（包括客户个人信息的类型、数量、来源、接收人等）和访问政策；

iv. 开展客户个人信息安全影响评估；

v. 组织客户个人信息安全培训；

vi. 在线发布产品或服务之前先对产品或服务进行测试，以避免非法收集和分享客户个人信息；

vii. 开展安全审计。

16. 供应商应建立客户个人信息安全影响评估制度，并定期开展客户个人信息安全影响评估（至少一年一次）。

a) 客户个人信息安全影响评估应重点评估处理活动是否符合客户个人信息安全基本原则以及客户个人信息处理活动对客户的合法权益造成的影响，包括但不限于：

i. 是否所有客户个人信息收集步骤均遵循了目的明确、同意选择、最低充分性等原则；

ii. 客户个人信息的处理是否可能对客户的合法权益造成不利影响，包括信息处理是否会危及人身和财产安全、损害个人信誉以及身心健康或导致歧视性待遇等;

iii. 客户个人信息安全措施的有效性；

iv. 匿名化或去标识化数据可能被用于重新标识客户的风险；

v. 安全事件可能对客户合法权益产生的不利影响。

b) 当法律法规提出新要求，或业务模式、信息系统和运营环境发生重大变化，或发生重大个人信息安全事件时，重新评估客户个人信息安全的影响。

c) 通过指定负责部门或系统，妥善保存客户个人信息安全影响评估报告，确保报告可供 LVMH W&J 或相关监管机构（如适用）进行审查。

17. 对于人员管理和培训，供应商应：

a) 与从事客户个人信息处理的相关人员（如销售经理、客户服务人员、大数据分析师、数据库管理员 等）签署保密协议，审查有权访问海量客户个人敏感信息的人员背景。

b) 告知从事个人信息处理的相关人员不同岗位应承担的安全责任，建立与安全事件相关的处罚机制。

c) 要求从事个人信息处理的相关人员在转岗或劳动合同终止时继续履行保密义务。

d) 规定有权访问客户个人信息的外部服务人员的安全要求，或与之签订保密协议并加以监督。

e) 定期（至少一年一次）或在隐私政策发生重大变更时对客户个人信息处理岗位的相关人员开展客户个人信息安全专业培训和评估，并保存培训记录（如签到表和培训内容）。

18. 除非与 LVMH W&J 另有明确约定，否则供应商不得向公众或任何第三方（包括分包商）披露、分享或传输客户个人信息。

对于 LVMH W&J 可能被要求或选择作出的任何披露/通知，供应商应向 LVMH W&J 提供一切合理的协助，包括但不限于：

a) 对于公开披露（向全部或特定群体公布）客户个人信息，供应商应协助 LVMH W&J 开展个人信息安全影响评估，以确保有效保护客户的权利。

b) 准确记录和保存客户个人信息的公开披露情况，包括公开披露的日期、规模、目的和范围。

c) 协助 LVMH W&J 告知客户被披露信息的目的和类型，并在 LVMH W&J 公开披露之前取得客户的同意。

19. 对于负责为 LVMH W&J 开发数字渠道的供应商，供应商应通过主动地将隐私保护嵌入到 IT 系统、网络基础设施和业务实践的设计和操作中“从设计着手保护隐私”（PbD）(参考附件 B)。供应商应确保将隐私保护的预防措施充分整合到为 LVMH W&J 提供的产品中。

对于系统的安全开发，供应商应 1)在设计系统的基础架构之前识别安全需求；2)定期对负责数字渠道的开发人员开展信息安全相关技术培训（如代码规范、常见软件漏洞等）；3)对拟将交付的系统执行代码审查和代码安全扫描，并生成测试报告。

客户个人信息的传输

适用范围

如属客户个人信息委托管理，供应商应遵守第 4 条第 20-22 款的要求；

如作为数据共同控制者，供应商应遵守第 4 条第 22 款的要求。

条款

20. 除非另有约定，供应商承诺仅在中国境内开展客户个人信息生命周期管理，且除非 LVMH W&J 事先明确书面批准，其承包商、国外关联实体或合作伙伴均不得向中国境外传输客户个人信息。了解更多要求，请参阅《一般服务购买协议》附件五第 2.7 条（个人数据的跨境传输）。

如果经 LVMH W&J 授权在中国境外对客户个人信息进行生命周期管理，供应商应：

a) 协助 LVMH W&J 开展客户个人信息跨境传输安全评估，并对评估结果的合法性和准确性负责。

b) 将所有客户个人信息跨境传输记录保留至少五年，包括 1)供应商在中国境外的法人实体的信息；2)跨境传输的时间；3)拟传输的客户个人信息的类型、数量和敏感性；及 4)适用法律（如《数据出境安全评估指南（草案）》）要求记录的其他信息。

c) 了解更多要求，请参阅《一般服务购买协议》附件五第 2.7 条（个人数据的国际传输）最后一段。

21. 如果供应商是海外组织/机构并经 LVMH W&J 授权委托处理客户个人信息，供应商应：

a) 确保签署本协议和履行本协议的规定义务不会违反供应商所在国家/地区的法律要求。

b) 当供应商所在国家或地区的法律环境发生变化且可能影响本协议的执行时，接收人应及时通知 LVMH W&J。

c) 遵守本协议上文第 4.20 条所载要求。

22. 在向 LVMH W&J 传输所收集和/或存储的客户个人信息时，供应商应：

a) 确保客户个人信息在存储、处理和传输阶段是完整、可用且最新的。

b) 负责向 LVMH W&J 安全传输客户个人信息，包括但不限于：对发送给 LVMH W&J 的、载有客户个人信息的文件进行加密、对便携式存储设备进行加密、使用可靠的传递渠道及指定专人负责快递。

c) 将向 LVMH W&J 传输的记录保留至少三年。记录的内容应包括：1)发送人的姓名；2)接收人的姓名；3)传输时间；4)传输方式和支持性安全措施；5)所传输的客户个人信息的类型、数量和敏感性；6)所涉及的客户数量。

客户个人信息的销毁

适用范围

如属客户个人信息委托管理，供应商应遵守第 4 条第 23-24 款的要求。

条款

23. 客户个人信息的存储期限于满足下列任一条件时期满：

a) 客户个人信息的存储不再符合收集客户个人信息的初始目的。

b) 供应商收到 LVMH W&J 的书面请求，要求删除所存储的客户个人信息。

c) LVMH W&J 规定的客户个人信息保留期已过。

如果客户个人信息的存储期满，供应商应参阅《一般服务采购协议》附件五第 2.8 条（个人数据的保留）和第 3 条（终止时处理）的相关要求。

24. 当供应商不再为 LVMH W&J 提供约定的产品/服务时，

a) 供应商应及时停止收集客户个人信息。

b) 供应商应至少提前两个月向 LVMH W&J 发出终止通知；供应商应继续遵守本协议的全部适用条款，直至以可互操作或可读格式向 LVMH W&J 交还供应商所拥有的全部客户个人信息并永久销毁供应商所拥有的客户个人信息的全部副本（硬拷贝或电子副本），包括备份数据，不考虑客户个人信息的存储方式和存储位置。

c) 如果因停止营业而终止，供应商应至少提前两个月向 LVMH W&J 发出终止通知；同时，供应商有义务以可互操作或可读格式交还客户个人信息，并销毁供应商所拥有的客户个人信息的全部副本（硬拷贝或电子副本），包括备份数据，不考虑客户个人数据的存储方式和存储位置。

审计与赔偿

适用范围

如属委托管理，供应商应遵守第 4 条第 25-27 款的要求；

如属委托开发，供应商应遵守第 4 条第 26-27 款的要求。

条款

25. 为证明供应商已遵守本协议和适用法律的规定，供应商应自费对与客户个人信息保护相关的安全政策、相关程序、安全措施的有效性进行定期内部审计（至少一年一次），并向 LVMH W&J 提交审计报告，或接受 LVMH W&J 指定的第三方审计。

    对于供应商开展的内部审计，供应商还应：

    a) 建立自动化审计系统，监控和记录客户个人信息的生命周期管理活动。

    b) 确保在审计过程中形成的记录能够为安全事件处理、事件响应和事件调查提供支持。

    c) 防止未经授权的访问、篡改或删除审计记录。

    d) 及时处理审计过程中发现的客户个人信息非法使用和滥用问题。

    对于 LVMH W&J 指定的第三方审计，详细要求请参阅《一般服务购买协议》附件五第 2.9 条“协作”。

26. LVMH W&J 保留开展其认为有用的任何检查的权利，以确认上述供应商义务得到履行。详细要求请参阅《一般服务购买协议》附件五第 3 条（审计）。

27. 赔偿问题请参阅《一般服务购买协议》附件五第 4 条（赔偿）。

第 5 条：适用法律

本协议的履行涉及客户个人信息的生命周期管理。客户个人信息的生命周期管理受适用法律约束。双方承认，其已知悉在法律项下其就相关客户个人信息保护活动的权利和义务。有关双方的义务，请参阅《一般服务购买协议》附件五第 2.1 条（双方关于适用数据保护法律的义务）。

本条列举了根据本协议规定适用于客户个人信息保护的相关法律、法规、规章、国家标准和指南，包括但不限于：

法律

《中华人民共和国密码法》，第三十五号主席令，2019 年 10 月 26 日

《中华人民共和国刑法修正案（九）》，2015 年 8 月 29 日

《中华人民共和国网络安全法》，2017 年 6 月 1 日

《中华人民共和国电子商务法》，2019 年 1 月 1 日

行政法规

《中华人民共和国计算机信息系统安全保护条例》，1994 年 2 月 18 日

《个人信息出境安全评估办法（征求意见稿）》

注：合同要求源自本办法征求意见稿。本办法生效后，供应商应确保遵守相关规定并承诺在相关实践中协助 LVMH W&J。

《儿童个人信息网络保护规定》，2019 年 10 月 1 号

《互联网个人信息安全保护指南》，2019 年 4 月 10 日

技术规范和标准

《信息安全技术 - 个人信息安全规范》

《信息安全技术 - 网络安全等级保护基本要求》，2019 年 12 月 1 日

因本协议产生的或与之相关的任何争议，均应提交至国家互联网信息办公室或当地法院，根据其届时有效的仲裁规则解决。仲裁裁决具有终局性，对双方具有约束力。

附件 A：数据安全要求

政策和标准

- 制定数据分类标准、相关数据安全政策和程序。

身份和访问管理

- 制定最少访问控制规则，保证供应商的人员和承包商仅能够访问其职责所需的最少客户个人信息，并将其最少数据操作许可（如读取、修改、删除、下载）严格限制在履行其职责所需的范围内；
- 为重要的客户个人信息操作（如批量修改、复制、下载 等）制定内部审批流程，应通过电子邮件获得 LVMH W&J 的最终批准；
- 确保由不同人员担任安全管理员、数据操作员和审计师；
- 明确规定和记录有权访问客户个人信息及相关信息系统的员工的责任、义务和基本信息；
- 建立相关机制，限制对包含客户个人信息的信息系统多次尝试进行未经授权的访问。

物理安全

- 只有数据安全政策中的授权人员可访问安装有信息系统的物理设备存储位置。
- 员工携带包含任何客户个人信息的设备和文件（包括电子邮件和/或电子邮件随附的文件）离开供应商的公司时，应获得许可。
- 在丢弃包含客户个人信息的文件或设备时，应采取措施擦除或物理销毁该文件或设备，以防止访问所包含的数据或随后恢复相关数据。

备份

- 供应商应制定满足客户个人信息备份、恢复和修复的安全要求的政策或标准，供内部参考。
- 供应商应确保客户个人信息备份免遭未经授权的访问，并向 LVMH W&J 提供有关客户个人信息备份的任何信息，包括但不限于客户个人信息的类型、数量、所涉及的客户数量、备份的存储位置、备份负责人、恢复测试和删除 等。

其他技术措施

- 如通过界面（如显示屏、纸张）显示个人信息，则须对拟将显示的客户个人信息采取去标识化处理等措施，以降低在展示期间泄露客户个人信息的风险。
- 对于已去标识化的客户个人信息，供应商应采取技术和管理措施，将去标识化的数据与可恢复用

于识别个人身份的信息分开存储，并确保在后续处理该等客户个人信息时无法重新标识相关个人。

- 对于客户个人敏感信息的存储，供应商应采取安全措施，包括加密和数据屏蔽或等效技术。
- 对于生物特征信息（如指纹、面部特征、声纹、虹膜等）的存储，供应商应在存储前采取技术措施（如采取技术措施和确保只存储生物特征信息摘要等）。

附件 B：供应商检查表（委托开发适用）

2019

Customer Personal Information Protection Agreement

FOR VENDOR USE

LVMH
WATCHES & JEWELRY

Contents

Article 1: Purpose

This Customer Personal Information Protection Agreement (this "Agreement"), is hereby incorporated into and made a part of that certain *General Service Purchase Agreement*, dated [INSERT DATE] by and between LVMH Watch & Jewellery (Shanghai) Commercial Co., Ltd.("LVMH W&J"), and [INSERT VENDOR NAME] ("Vendor"). In the event of a conflict or inconsistency between this Agreement and *General Service Purchase Agreement*, the terms and conditions set forth in this Agreement, shall govern and control.

Article 2: Scope

This Agreement acknowledges that Customer Personal Information (hereinafter defined and referred to as "CPI") of or regarding the Customer of LVMH W&J may be discussed between Vendor and LVMH W&J (hereinafter known collectively as the "Both Parties"). The provisions set forth in this Agreement define how Vendor protect CPI under different circumstances, and include the remedies, penalties and lawful action that LVMH W&J may take for violation actions.

Both Parties agree that it is in their best interests to protect the CPI, and that the terms of this Agreement create a bond of trust and confidentiality between them.

This article will remain in force after the termination or expiry of the Agreement for whatever reason.

Article 3: Definition

"Customer" means a person or organization that buys goods or services from LVMH W&J or its subsidiaries (collectively "LVMH W&J")as well as leaving CPI through any channels.

"Lifecycle Management" means management of CPI may involve one or more of the following situations: collection, storage, processing, sharing, transfer, disclosure and destruction of CPI.

"Vendor" means a person or entity that provide products or services to LVMH W&J and get paid. Vendor may be applicable in one or more of the following circumstances:

4. **"Commissioned Management of CPI"**. Vendor undertakes Lifecycle Management of CPI on behalf of LVMH W&J. LVMH W&J acts as the data controller, and vendor acts as data processor.

5. **"Commissioned Development"**. Vendor develops and/or operates Digital Channel for LVMH W&J.
6. **"Data Co-controllers"**. Refers to the definition of "Data Co-controller".

"Personal information" means all information that is recorded electronically or by other means and can be used solely or in combination with other information to identify a certain natural person or reflect the activities of a certain natural person.

Note: Personal information includes name, date of birth, ID number, personal biometric information, residential address, contact information, communication records and content, account password, property information, credit information, whereabouts, hotel accommodation information, health and physiological information, transaction information, etc.

"Customer Personal Information" ("CPI") means personal information of Customer of LVMH W&J. The ownership of CPI belongs solely to LVMH W&J except the circumstance when LVMH W&J and Vendor are Data Co-controller.

"Customer Personal Sensitive Information" means CPI whose leaked, illegal provided or abused may endanger Customer personal and property security and easily lead to damage of personal reputation and physical or mental health, or discriminatory treatment.

Note: Personal sensitive information includes ID number, biometric information, bank account number, communication records and content, property information, credit information, whereabouts, hotel accommodation information, health and physiological information, transaction information, and personal information of children at or under 14 years old.

"Consent" means behavior whereby a Customer grants a clear authorization on certain Lifecycle Management of personal information through written statement or proactive affirmative action.

Note: Affirmative actions include statement (in electronic, paper form or orally) proactively made by Customer and proactively checking or clicking on "Agree", "Sign up", "Send", "Dial", etc.

“Digital Channel” means network channels/platforms/scenarios/applications through which Vendor conduct Lifecycle Management activities of CPI with authorization of LVMH W&J. Such as company websites, customer digital card, Mobile APP (IOS or Android), WeChat official account, WeChat mini program, Weibo, T-mall, JD, etc.

“Data Co-controller” means Vendor acts as data controller who owns and manages the lifecycle of personal information collected by Vendor and later transferred to LVMH W&J. Such personal information can be regarded as CPI after the transmission to LVMH W&J, in which case LVMH W&J and Vendor become Data Co-controllers and share the ownership of CPI.

“Security Incident” means any event impacting or likely to impact the security of CPI in terms of availability, integrity, confidentiality and traceability.

“Data Breach” means any event leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to CPI. A Security Breach is a Security Incident.

Article 4: Provisions

Collection of CPI

Applicability

In the event of Commissioned Management of CPI, Vendor shall follow the requirements under Clause1-4 in Article 4;

In the event of Data Co-controller, Vendor shall follow the requirements under Clause 1-5 in Article 4.

Clauses

28. Vendor shall collect CPI after obtaining written authorization from LVMH W&J regarding types of CPI, methods of collection, frequency of collection, purpose of collection, *etc*. Collection of CPI should be legitimate according to applicable legislation. Therefore, Vendor shall not
    a) Cheat, trick or force Customer to provide his or her personal information.

b) Conceal the personal information collection function of a product or service.

c) Obtain personal information from illegal sources.

d) Obtain personal information that is not allowed to collect by Applicable Legislation.

e) Collect personal information from channels that are considered inappropriate by LVMH W&J or Applicable Legislation.

Vendor is not allowed to collect CPI without written authorization of LVMH W&J. If additional CPI collection is regarded as necessary by Vendor, Vendor shall communicate with LVMH W&J 1 week at least in advance and ask for written authorization. LVMH W&J shall not be responsible for any legal disputes arising from illegitimate collection by Vendor.

Collection of CPI by Vendor shall follow the minimum collection principle prescribed by the Applicable Legislation and shall not exceed the authorized scope (types of CPI, methods of collection, frequency of collection, purpose of collection, *etc*.) by LVMH W&J.

29. When Vendor collects CPI through Digital Channel or other methods (e.g. offline collection channels in physical stores, commercial activities), Vendor shall explicitly inform Customer of the types of CPI to be collected respectively by different business functions of the product or service provided, as well as the rules for collection and use of CPI so that to obtain Consent from Customer. Methods of informing Customer include:

a) Privacy policy provided by LVMH W&J Which Vendor shall be obligated to release and maintain on each Digital Channel defined in Article 3 in this Agreement.

i. The privacy policy provided by LVMH W&J shall be published and easily accessible, e.g. inserting links in prominent positions on the homepage of Digital Channel.

ii. The privacy policy shall be an independent document and separated from User Agreement.

iii. In other circumstances despite Digital Channel, privacy policy shall be delivered to each Customer by contract, link, message, email or other means; The privacy policy can be released in the form of announcement if the cost is too high or there is significant difficulty.

iv. When the privacy policy provided by LVMH W&J changes, Vendor shall provide necessary assistance with LVMH W&J in re-informing Customer and update the privacy policy provided by LVMH W&J in each scenario of collecting CPI.

b) Under the circumstance where privacy policy is not a feasible method to inform Customer, Vendor shall, send mails, make phone calls or push notifications to Customer regarding the types of CPI to be collected respectively by different business functions of the product or service provided, as well as the rules for collection and use of CPI.

In the case when the information generated by the processing of personal information collected can be regarded as CPI, processing of the newly generated CPI shall be within the range of authorization obtained from Customer. If it is beyond the range of Customer's authorization, Vendor shall

c) Inform Customer and re-obtain the Consent from Customer as per Article 4.2 (a), (b) in this Agreement.

d) Notify LVMH W&J within 5 working days to update privacy policy, if applicable.

30. For collection of Customer Personal Sensitive Information, Consent of Customer to be obtained must be voluntary, concrete, clear and based on full knowledge of the collection.

Whether a business function is core business function or additional function should be confirmed by Vendor with the IS&T/Legal/Business Unit of LVMH W&J.

Prior to the collection of Customer Personal Sensitive Information by means of proactive provision or automatic collection, Vendor shall:

a) Inform Customer of the core business functions of the products or services provided and the Customer Personal Sensitive Information which needs to be collected for the core function; clearly inform Customer of the impact caused by his/her refusal to provide Consent (e.g. normal function of products or services provided for Customer may fail). Customer shall be allowed to choose whether to provide such information or give Consent to automatic collection.

b) In the case when the product or service provides other additional functions, when Customer Personal Sensitive Information needs to be collected, Vendor shall, prior to collection, inform Customer of what Customer Personal Sensitive Information is required for fulfilling which

additional function, one by one, and allow Customer to choose, whether to provide such information to each additional function, one by one, or give Consent to automatic collection. In the case when Customer refuses, corresponding additional functions may not be provided, but Vendor shall not stop providing core business function on this ground and shall ensure corresponding service quality.

Note 1: Methods of inform may refer to Article 4.2(a)(b) in this Agreement.

Note 2: Functional interface is an optional method of informing Customer of business functions and the required CPI by each business function. Vendor shall provide a functional interface for Customer proactively before the collection of Customer Personal Sensitive Information, such as during the product installation process, or when Customer first uses the product or service, or when Customer registers an account.

c) Vendor shall not collect or process CPI of minors under 18 years old on behalf of LVMH W&J. If Vendor possess such CPI which has been collected on behalf of LVMH W&J, Vendor shall delete the according CPI.

31. Vendor shall only provide products and services through Digital Channel with Customers who has submitted authentic identity information through Digital Channel (e.g. Vendor shall deploy the authentication mechanism for Customer identity by collecting Customer cell phone number and send verification code to verify the authenticity of the number). Vendor shall bear potential financial penalty stipulated in Applicable Legislation (e.g. China Cybersecurity Law) at Vendor's own cost due to refusal to perform such obligation as per this Agreement or failure to make corrections.

32. Vendor, serving as Data Co-controller, shall establish a comprehensive privacy policy which the collection and the subsequent processing activities of CPI by Vendor are strictly subject to. Contents of Vendor's privacy policy include but are not limited to:

i) General information of Vendor, including registered name, registered address, office location, and contact information of the person in charge, *etc*.

j) Purpose for collection and processing of CPI, and the business functions covered by the purpose, e.g. using CPI to push commercial advertisements, using CPI to form direct user profiling and its uses, *etc*.

k) CPI respectively collected by each business function, CPI processing rules covering collection methods and frequency, storage area and storage period, as well as the actual range of CPI to be collected.

l) Purposes of sharing, transfer and public disclosure of CPI, types of CPI involved, types of a third party that receives CPI, and corresponding legal liability.

m) Basic principles of CPI security followed, data security capability of the controller, and CPI security measures adopted.

n) Rights of the personal data subject and the mechanism for the realization of such rights, e.g. access method, correction method, deletion method, account closing method, Consent withdrawal method, method for obtaining a duplicate of CPI, and method for restraining the automatic decision-making of information system, *etc*.

o) Possible security risks after CPI is provided, and possible impact if fail to provide CPI.

p) Channels and mechanisms for responding to inquiries and complaints from the Customer, and external dispute settlement agency and its contact information.

Vendor's privacy policy shall be published and easily accessible, e.g. inserting links in prominent positions on the Vendor's homepage of website, mobile application program installation page, social media homepage, *etc*.; The privacy policy should be an independent document and separated from User Agreement; The privacy policy should be delivered to each Customer by contract, link, message, email or other means; The privacy policy can be released in the form of announcement if the cost is too high or there is significant difficulty; In case of a change to the matters set forth in a) to h) in this clause, the privacy policy shall be updated promptly and Customer shall be re-informed.

Vendor shall be aware of potential consequences of violating requirements hereinabove (e.g. being requested by relevant regulatory departments to delete CPI due to illegitimate collection). Vendor shall make every effort to ensure the compliance with Applicable Legislation and minimize any possible disruption of LVMH W&J's business caused by the consequences upon violation of

Applicable Legislation. Vendor shall reimburse LVMH W&J for actual costs suffered by LVMH W&J arising out of such disruption of business.

Storage of CPI

Applicability

In the event of Commissioned Management of CPI, Vendor shall follow the requirements under Clause 6-8 in Article 4;

In the event of Commissioned Development, Vendor shall follow the requirements under Clause 9 in Article 4;

In the event of Data Co-controller, Vendor shall follow the requirements under Clause 7 in Article 4.

Clauses

33. If Vendor's service provided to LVMH W&J involves and/or depends on storing the collected CPI, Vendor shall store CPI exclusively within the territory of China unless with express prior written approval of LVMH W&J.

    Vendor shall ensure the effectively implement data minimization and limited retention by following the principles:

    a) Refer to 2.2 "Personal Data Processing entrusted to the Service Provider" in Attachment V of *General Service Purchase Agreement*.

    b) The storage of CPI shall be physically separated from other data belonging to Vendor, Vendor's other clients or any third parties.

34. Vendor shall maintain the matching degree between the service resources and the number of clients, and shall always maintain the data analysis capability, system maintenance capability and information security capability in line with the service quality required by LVMH W&J.

    Vendor shall determine appropriate security measures to be taken, from both management and technical perspectives, to enhance its data protection capability and limit the likelihood (e.g. leakage, destruction and loss of CPI) and impact (e.g. leakage of CPI may harm the interests of Customer) of potential risks to an acceptable level.

    In any case, security measures shall be in accordance with the security provisions of good industry practices or the advanced technical standards available in the market. Vendor shall be able to provide LVMH W&J with a list of duly authorized persons and audit trails in response to a request from the latter.

Vendor shall be aware of potential consequences of violating requirements hereinabove (e.g. lack of data availability and integrity due to leakage of CPI). Vendor shall make every effort to ensure the compliance with Applicable Legislation and minimize any possible disruption to LVMH W&J's business caused by the consequences upon violation of Applicable Legislation. Vendor shall reimburse LVMH W&J for actual costs suffered by LVMH W&J arising out of such disruption of business.

Detailed requirements refer to Appendix A of this Agreement.

More requirements refer to 1.1 "General security obligation" and 2.4 "Processing security and confidentiality"in Attachment V of *General Service Purchase Agreement.*

35. If Vendor receives any Customer's request with respect to their personal information or request on exercising their rights,

    a) Refer to 1.1 "General security obligation" in Attachment V of *General Service Purchase Agreement*.

    Note 1: Rights of Customer include the right to access, the right to obtain the rectification or deletion of CPI or to restrict (block) the processing of CPI, the right to object to decisions based on profiling, the right to data portability and the right to withdraw Consent.

36. Vendor is obligated to get Classified Protection of Cybersecurity (MLPS 2.0) certification for systems that contain CPI. Certification shall be updated if expired.

Processing of CPI

Applicability

In the event of Commissioned Management of CPI, Vendor shall follow the requirements under Clause 10-18 in Article 4;

In the event of Commissioned Development, Vendor shall follow the requirements under 19 in Article 4.

Clauses

37. Vendor shall keep a register of the processing activities carried out on behalf of LVMH W&J. Details requirements refer to 2.3 "Register of Processing activities" in Attachment V of *General Service Purchase Agreement.*

38. Processing of CPI shall not go beyond the authorized scope by Customer. In the event when it is indeed necessary to process CPI beyond the above scope, Vendor shall obtain Consent from Customer (refer to Article 4.2 and Article 4.3).

    Under specific circumstances, if clear identity directionality is not necessary, Vendor shall implement indirect user profiling to avoid pointing precisely to specific individuals, such as pushing commercial advertisement to Customer.

39. In the event when Vendor commission subcontractors in processing of CPI, Vendor shall refer to 2.6 "Subcontractor" in Attachment V of *General Service Purchase Agreement.*

    In any case, Vendor shall remain fully liable towards LVMH W&J for the performance of its subcontractor's obligations.

40. If Vendor merges with a third party, be merged by a third party or be directly or indirectly controlled by a third party,

    a) If Vendor has not obtained prior written authorization from LVMH W&J, Vendor shall not disclose any CPI of LVMH W&J to the third party and immediately return the CPI to LVMH W&J or destroy permanently all CPI that Vendor may hold as required by LVMH W&J.

    b) However, if prior written authorization from LVMH W&J is obtained, Vendor may continue the processing of the CPI and the processing shall remain compliant to this Agreement and to Applicable Legislation. Responsibility of Vendor defined in this Agreement shall be inherited by the merged entity.

41. With regards to Security Incident, Vendor shall:

    a) Develop a contingency plan for responding to Security Incident, including job responsibilities and incident response strategies and procedures. The contingency plan shall be updated regularly or update in a timely manner according to the changes to relevant laws and regulations as well as the disposal results of Security Incident.

    b) Organize incident response training and emergency drills for Vendor's employees regularly (at least once a year) to inform them of job responsibilities and emergency response strategies and procedures.

c) Vendor shall draft, collect and provide any available material (include but not limit to relevant records, logs, files, data reporting) required to comply with Applicable Legislation, good Industry practices or as otherwise required by LVMH W&J within the time period required by LVMH W&J. Relevant materials of CPI Security Incident shall include:

   i. Contents of the incident, including but not limited to: person who discover the incident, personnel to whom the incident is reported, time and place, what CPI and number of Customer involved, name of the system on which the incident occurs, impact on other connected systems.

   ii. Assessment result of the possible impact of the incident, what necessary measures to be taken to control the situation and eliminate hidden dangers, the according responsible personnel with the personnel's contact information and any changes made as a result of the incident (add, modify, or delete).

d) More requirements and related indemnification issues refer to 1.3 "Security Incident and Data Breach management and notification" in Attachment V of *General Service Purchase Agreement*.

e) Malicious program related requirements refer to 1.2 "Malicious Programs" in Attachment V of *General Service Purchase Agreement*.

42. In the light of Applicable Legislation, Vendor agrees to improve its management of organization through:

a) Developing CPI protection plan or policy to ensure legal representative or head of the organization assume total responsibility for overseeing the CPI security, including providing human, financial and material resources to fulfill the CPI security mission.

b) Designating a person and department to oversee CPI protection.

c) If Vendor processes CPI of over 1,000,000 people or expects to process CPI of over 1,000,000 people in the next 12 months or Vendor's the main business involves personal information processing, and the number of employees is more than 200, Vendor shall appoint a full-time officer in charge of CPI protection and establish a CPI protection department to be responsible for CPI security work.

d) Responsibilities that the CPI protection officer and CPI protection department shall perform include but are not limited to:

i. Plan and implement the CPI security work within the organization and be directly responsible for CPI security work.

ii. Develop, issue, implement and regularly update privacy policy and related regulations.

iii. Establish, maintain and update a list of CPI processed by Vendor (including CPI type, amount, source, recipient, *etc*.) and a policy on authorized access;

iv. Conduct CPI security impact assessment.

v. Organize CPI security training.

vi. Test the products or services before they are published online, to avoid illegitimate collection and sharing of CPI.

vii. Conduct security audits.

43. Vendor shall establish a CPI security impact assessment system and carry out a CPI security impact assessment regularly (at least once a year).

a) The CPI security impact assessment shall focus on assessing the compliance of processing activities with the basic principles for CPI security, and the impact of CPI processing activities on the legitimate rights and interests of Customer, including but not limited to:

i. Whether all CPI collection steps follows the principles of clear purpose, Consent selection, minimum but adequacy, *etc*.;

ii. Whether CPI processing may adversely affect the legitimate rights and interests of Customer, including whether the processing will endanger the personal and property safety, damage personal reputation and physical and mental health or lead to discriminatory treatment, *etc*.;

iii. Effectiveness of CPI security measures;

iv. The risk that anonymized or de-identified data can be used to re-identify Customer;

v. Possible adverse impact of a security incident on legitimate rights and interests of Customer.

b) Re-assess the CPI security impact when there are new requirements in laws and regulations, or major changes in business models, information systems and operating environments, or major CPI security incidents.

c) Properly keep CPI security impact assessment reports by assigning responsible department or system, to ensure that the reports are available for review by LVMH W&J or relevant regulatory body if applicable.

44. With regards to personnel management and training, Vendor shall:

a) Sign a non-disclosure agreement with relevant personnel (such as sales manager, customer service, big data analyst, database administrator, *etc*.) engaged in CPI processing and review the background of personnel who have access to large amounts of Customer Personal Sensitive Information.

b) Inform relevant personnel engaged in personal information processing of the security responsibilities of different roles and build a punishment mechanism associated with Security Incident.

c) Require relevant personnel engaged in personal information processing to continue to perform the non-disclosure obligation when transferred to other positions or when employment contract is terminated.

d) Define the security requirements of CPI for external service personnel who have access to CPI, or sign a confidentiality agreement with them and supervise them

e) Conduct professional training and assessment on CPI security for relevant personnel in CPI processing positions on a regular basis (at least once a year) or in case of major changes in privacy policy and keep training records (such as sign-in form and training content).

45. Vendor shall not disclose, share or transfer CPI to public or any third party including sub-contractors unless expressly otherwise agreed with LVMH W&J.

Vendor shall provide all reasonable assistance to LVMH W&J with respect to any disclosure/notification that the latter may be required to or elect to make, including but not limited to:

a) In the case of publicly disclosure (publishing to all or certain groups) of CPI, Vendor shall assist LVMH W&J in conducting personal information security impact assessment to ensure effective protection of the rights of Customer.

b) Accurately record and preserve the public disclosure of CPI, including date, scale, purpose and scope of the public disclosure.

c) Assist LVMH W&J in informing Customer of the purpose and types of disclosed information, and obtained Consent from Customer before the public disclosure by LVMH W&J.

46. For Vendor responsible of developing Digital Channel for LVMH W&J, Vendor should take account of "Privacy by Design" (PbD) (refer to Appendix B) by proactively embedding privacy protection into the design and operation of IT systems, networked infrastructure, and business practices. Vendor should make sure that preventative measures of privacy protection are fully integrated components in the product provided for LVMH W&J.

    With regards to security development of system, Vendor shall 1) identify security requirements before designing the architecture of system, 2) conduct regular information security-related technical training for developers responsible for Digital Channel (such as code specification, common software vulnerabilities, *etc*.), 3) performs code reviews and code security scans on systems to be delivered and generates test reports.

Transfer of CPI

Applicability

In the event of Commissioned Management of CPI, Vendor shall follow the requirements under Clause20-22 in Article 4;

In the event of Data Co-controller, Vendor shall follow the requirements under Clause22 in Article 4.

Clauses

47. Unless expressly otherwise agreed, Vendor undertakes to keep the Lifecycle Management of CPI exclusively in the territory of China and no CPI is transferred outside the territory of China by its own sub-contractors, foreign affiliated entity or partners unless with express prior written approval of LVMH

W&J. More requirements refer to 2.7 “International transfers of Personal Data” Attachment V of *General Service Purchase Agreement*.

In the case when Vendor’s Lifecycle Management of CPI outside the territory of China has been authorized by LVMH W&J, Vendor shall

a) Assist LVMH W&J in conducting security assessment of CPI cross-border transfer and be responsible for the legitimacy and accuracy of the assessment results.

b) Keep a record for all the cross-border transfer of CPI for at least 5 years including 1) information of Vendor’s legal entity located outside the territory of China, 2) time of cross-border transfer, 3) types, amount and sensitivity of CPI to be transferred and 4) other information required to be recorded according to Applicable Legislation such as Guidelines for data cross-border transfer security assessment (Draft).

c) More requirements refer to the last paragraph in 2.7 “International transfers of Personal Data” in Attachment V of *General Service Purchase Agreement.*

48. In the case when Vendor is a foreign organization/institution and commission processing has been authorized by LVMH W&J, Vendor shall:

a) Ensure that the signing of this Agreement and the performance of the obligations stipulated by this Agreement will not violate the legal requirements of the country/region where Vendor locates.

b) When changes in the legal environment of the country or region where Vendor locates may affect the execution of this Agreement, the recipient shall promptly notify LVMH W&J.

c) Comply with requirements as per Article 4.20in this Agreement hereinbefore.

49. In the event of transferring collected or/and stored CPI to LVMH W&J, Vendor shall:

a) Ensure CPI is kept complete, available and up to date during the stages of storage, processing and transfer.

b) Be responsible for secure transfer of CPI to LVMH W&J, including but not limited to: encryption of files containing CPI sent to LVMH W&J, encryption of portable storage devices, using reliable delivery channels and designating specific personnel responsible of express delivery.

c) Keep records of every transfer to LVMH W&J for at least three years. Content of records shall include: 1) name of sender, 2) name of receiver, 3) time of transfer, 4) method of transfer and supporting security measures, 5) types, amount and sensitivity of transferred CPI, 6) amount of Customer that involved.

Destruction of CPI

Applicability

In the event of Commissioned Management of CPI, Vendor shall follow the requirements under Clause 23-24 in Article 4.

Clauses

50. The CPI storage period expires if any of the following conditions is met:

    a) Storage of CPI no longer fulfils the original purpose of collecting CPI.

    b) Vendor has received written request from LVMH W&J claiming to delete the stored CPI.

    c) The CPI retention period specified by LVMH W&J has expired.

    If the CPI storage period expires, Vendor shall refer to 2.8 “Conservation of Personal Data”and Article 3 “Handling upon Termination” in Attachment V of *General Service Purchase Agreement.*

51. When Vendor ceases providing the agreed products/services for LVMH W&J,

    d) Vendor shall discontinue collection of any CPI in a timely manner.

    e) Vendor shall sent the termination notice to LVMH W&J two months in advance at least; Vendor shall continue to comply with all the applicable clauses in this Agreement until all CPI that Vendor may have in its possession has been returned in an interoperable or readable format to LVMH W&J and all (hard or electronic) copies (including backup data) of the CPI have been destroyed permanently that Vendor may have in its possession, regardless how and where the CPI is stored.

    f) If the ceasing is caused by ceasing of business operation, Vendor shall send the termination notice to LVMH W&J two months in advance at least; Vendor shall also be obligated to return the CPI in an interoperable or readable format and to destroy all (hard or electronic) copies

(including backup data) of the CPI permanently that Vendor may have in its possession, regardless how and where the CPI is stored.

Audit &Indemnification

Applicability

In the event of Commission Management, Vendor shall follow the requirements under Clause 25-27 in Article 4;

In the event of Commissioned Development, Vendor shall follow the requirements under Clause 26-27 in Article 4.

Clauses

52. In order to demonstrate the compliance of Vendor with this Agreement and Applicable Legislation, Vendor shall conduct regular internal(at least once a year) audit at its cost on related security policies, related procedures, effectiveness of security measures associated with CPI protection and submit the audit report to LVMH W&J, or accept third-party audit designated by LVMH W&J.

    With regards to internal audit conducted by Vendor, Vendor shall also

    e) Establish an automated audit system, to monitor and record the Lifecycle Management activities of CPI.

    f) Ensure the records formed during the audit process are able to provide support for Security Incident disposal, incident response and incident investigation.

    g) Prevent unauthorized access, tampering or deletion of audit records.

    h) Promptly handle illegal use and abuse of CPI discovered during the audit.

    With regards to third-party audit designated by LVMH W&J, details requirements refer to 2.9 “Collaboration” in Attachment V of *General Service Purchase Agreement*.

53. LVMH W&J reserves the right to carry out any checks it deems useful in order to confirm that these obligations of Vendor hereinbefore are being fulfilled. Details requirements refer to 3. “AUDIT” in Attachment V of *General Service Purchase Agreement.*

54. Indemnification issues refer to Article 4 “Indemnification” in Attachment V of *General Service Purchase Agreement.*

Article 5: Applicable Legislation

Performance of this Agreement entails the Lifecycle Management of CPI, which is subject to Applicable Legislation. Both Parties acknowledge they are aware of their rights and obligations under this Legislation and in relation with CPI protection activities. Obligations of both Parties refer to 2.1 “Obligation of the Parties regarding Applicable Data Protection Legislation” in Attachment V of *General Service Purchase Agreement.*

This article outlines relevant laws, regulations, rules, national standards and guidelines applicable to the protection of CPI in accordance with this Agreement, including but not limited to：

Laws

Code law of the People's Republic of China (President's Order No. 35), 26th October,2019

Amendment to Criminal Law (ix)，29th August,2015

China Cybersecurity Law，1st June,2017

The E-Commerce Law of The People's Republic of China，1st January, 2019

Administrative regulations

Regulations of The People's Republic of China on The Security Protection of Computer Information Systems，18th February,1994

Measures for Personal Information Cross-Border Transfer Security Assessment (Draft)

Note: Contractual requirements are derived from this draft version of Measures. When related Measures come into effect, Vendor shall ensure its compliance and undertakes to assist LVMH W&J in related practices.

Regulations on Children’s Personal Information Network Security Protection,1stOctober, 2019

Guidelines for Internet Personal Information Security Protection,10thApril, 2019

Technical specifications and standards

Information Technology - Personal Information Security Specification

Information Technology – Baseline for Classified Protection of Cybersecurity (MLPS 2.0),1st December,2019

Any disputes arising out of or in connection with this Agreement shall be submitted to Cyberspace Administration of China or local court in accordance with its arbitral rules then in force. The arbitration award shall be final and have binding force upon the Parties.

Appendix A: Data Security Requirements

Policy and standard

- Develop data classification standard, relevant data security policy and procedure.

Identity and access management

- Set up the minimum access control rules to guarantee Vendor's personnel and contractors can only access the minimum CPI required by their duties, and only have the minimum data operation permission (e.g. read, modify, delete, download) within a strict limit of what is needed to perform their duties;
- Set up internal approval process for important operation of CPI, such as batch modification, copy, download, *etc*., which should obtain LVMH W&J's final approval through Email.
- Ensure the roles of security administrator, data operator and auditor are assumed by different persons;
- Responsibilities, obligations and basic information of employees who have access to CPI and related information systems shall be clearly defined and recorded.
- Mechanisms should be established to limit repeated attempts to gain unauthorized access to the information system that contains CPI.

Physical security

- Only authorized personnel in the data security policy may access the physical equipment storage location where the information system is installed.
- Permission should be obtained by employees to leave the company of Vendor with equipment and documents containing any CPI, including e-mails and/or documents attached to e-mails.
- When discarding a file or device containing CPI, measures should be taken to erase or physically destroy it to prevent access to the contained data or subsequent recovery.

Backup

- Vendor shall develop a policy or standard which addresses the security requirements for backup, recovery and restoration of CPI for internal reference.
- Vendor shall keep backup of CPI from unauthorized access and provide LVMH W&J with any information related to the backup of CPI, including but not limited to: types, amount of CPI, amount of Customer involved, storage location of backup, responsible personnel for backup, recovery testing and deletion, *etc*.

Other technical measures

- In the case that personal information is displayed through interface (e.g. display screen, paper), measures such as de-identification for the CPI to be displayed are necessary to reduce the risk of leakage of CPI during the exhibition.
- For the de-identified CPI, Vendor shall take technical and management measures to store de-identified data separately from the information that can be restored to identify individuals and ensure no possibility of re-identifying individuals in the subsequent processing of such CPI.
- For the storage of Customer Personal Sensitive Information, Vendor shall adopt security measures, including encryption and data masking, or equivalent technologies.
- For the storage of biometric information (e.g. fingerprints, facial features, voice prints, iris, *etc*.), Vendor shall take technical measures before storage (e.g. take technical measures and ensure only the abstract of biometric information is stored).

Appendix B: Checklist for Vender (applicable to Commissioned Development)