2019

客户个人信息保护政策

供应商管理适用

LVMH
WATCHES & JEWELRY

目录

第 1 章：目标

供应商客户个人信息保护政策（本“政策”）在保护客户个人信息方面为供应商管理提供了指南。本政策包括个人信息保护标准，以确保 LVMH, Watch & Jewelry（“LVMH W&J”）的所有供应商在 LVMH W&J 的监督下达到保护客户个人信息的目标，并履行《客户个人信息保护协议——供应商适用》(“协议”)中规定的合同义务。

第 2 章：范围

本政策适用于 LVMH 中国钟表珠宝部门，包括采购部、事业部、安全团队和法务部。

第 3 章：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。

“供应商履行”指供应商履行客户个人信息保护。

“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 章：治理和责任

4.1 采购部

采购部负责：1)参与供应商准入，确保供应商的资质符合 LVMH W&J 的要求；2)审核供应商的年度审计结果和质量控制。

4.2 事业部

与缔约供应商往来的事业部负责：1)负责供应商管理；2)作为 LVMH W&J 与供应商的内部联系人；3)及时向供应商传达安全团队提出的客户个人信息保护要求；4)监督并对供应商履行负责；5)报告供应商违反内部信息安全政策及本政策的情况。

4.3 安全团队

安全团队负责：1)开发和维护包含客户个人信息保护策略、政策和相关程序（包括本政策）的信息安全程序；2)制定具体项目的客户个人信息保护安全目标和要求；3)从客户个人信息保护角度为供应商准入作出贡献；4)在签署协议期间与供应商合作；5)指导和监督供应商保护客户个人信息的履行；6)在必要时与相关外

部监管机构保持联络。

4.4 法务部

法务部负责：1)审查与供应商签订的合同/协议；2)从法律合规的角度支持签署协议；3)就任何合同纠纷提供法律咨询。

第 5 章：供应商管理

5.1 供应商准入

根据安全团队制定的总体客户个人信息保护策略，安全团队负责结合考虑业务情形和拟将收集的客户个人信息的性质（须与事业部保持一致），为涉及缔约承包商的具体项目制定客户个人信息保护整体目标（如客户个人信息准入管理的控制力度和传输/存储的技术措施等）。安全团队还负责根据内部供应商安全政策开发供应商评估系统，并制定【供应商信息安全评估】和清单。

在与任何供应商签约之前，事业部应牵头进行客户个人信息安全影响评估，以评估和处理客户个人信息处理活动中的安全风险。详细信息请参阅《客户个人信息保护政策——雇员管理适用》。

5.1.1 准入评估

在供应商准入阶段，采购部和事业部必须在下单或与任何供应商签订合同之前牵头开展供应商资格验证。事业部必须根据【供应商信息安全评估】填写清单。签约风险根据对供应商规定的保密性、完整性、可用性和可跟踪性要求相关的标准确定。

准入评估结果必须阐明供应商是否有能力实现安全团队制定的客户个人信息保护目标，以及 LVMH W&J 是否能接受引入供应商所带来的数据安全风险。必须向安全团队传达准入评估结果。安全团队应从客户个人信息保护角度对供应商准入提出建议，优先选择具有以下特征的供应商：

- 有能力确保客户个人信息的安全。
- 首选在中国境内存储和处理客户个人信息。
- 愿意在保护客户个人信息和处理安全事件方面提供专用资源。

关于准入评估中发现的风险，安全团队应考虑任何经济可行的补充控制措施，以减轻该等风险带来的任何潜在后果。在与供应商签署协议期间，将由安全团队负责执行该等补充控制措施。

5.1.2 供应商尽职调查

事业部必须与采购部合作开展供应商尽职调查。作为尽职调查的一部分，安全团队负责规划供应商信息安

全尽职调查。安全尽职调查可以在供应商的经营场所，由安全团队或法务部指定的第三方进行。安全尽职调查也可以通过事业部要求供应商根据安全团队起草的证据收集清单提供证据的方式来开展。

尽职调查的内容包括但不限于：

- 声誉
- 负责人员的专业经验和素质
- 有效的信息安全相关认证（如 ISO/IEC 27001、ISO/IEC 27018、ISO/IEC 29151、安全产品认证）
- 办公室和设施的物理安全性
- 信息安全事件历史
- 违规历史

安全团队可根据业务需要和供应商的实际情况调整安全尽职调查的内容。安全尽职调查的结果应报告给事业部和采购部。事业部和采购部必须根据安全尽职调查结果和其他尽职调查项目检查供应商资质的真实性。此外，如果供应商使用分包商支持与 LVMH W&J 的业务关系，LVMH W&J 要求供应商自行开展尽职调查项目，以审查分包商的资质。

5.2 授予协议

法务部、采购部、事业部和安全团队必须审核与供应商签订的合同和协议。法务部仅限参与有关合同法律方面的问题讨论。

安全团队已为特定类型的供应商起草 LVMH W&J 标准供应商客户个人信息保护协议模板（协议），并建议将草案作为最终版。

如果使用 LVMH W&J 的协议模板，

- 安全团队必须根据 1)具体项目的客户个人信息保护目标和要求；2)供应商类型；3)供应商的实际情况；和 4)拟执行的补充控制措施等，调整协议。安全团队必须确保协议条款包含全部必要安全措施，以保障客户个人信息的保密性、可用性和完整性。
- 事业部可以在协议中输入与具体条款有关的业务事项。该等业务事项必须包含业务的重要性、供应商的重要性和客户个人信息的性质（客户个人信息的数量、客户数量、客户个人信息敏感性）。
- 本协议中任何法律条款的变更均须经法务部最终批准。此外，法务部必须不断跟踪与个人信息保护相关法律的发展变化，并与安全团队合作不断更新协议。法务部必须确保协议包含适用法律规定的所有适用保护要求。

如果由供应商起草协议模板，则供应商的模板必须交由法务部、事业部、安全团队和采购部审查，以确保

在相关程度内其中所载权利和义务与协议所载权利和义务相同，尤其包括确保保护客户个人信息、遵守适用法律的义务和审计权利。如果供应商的模板未达到前述要求，法务部必须与供应商协商该等要求，并对相关条款作必要修订。

在法务部批准后，方可代表 LVMH W&J 与供应商签署协议。事业部组织代表 LVMH W&J 签署协议。必须由事业部与供应商和/或供应商的分包商签署协议和《保密协议》。协议所载条款和条件优先于供应商的安全文件。

安全团队的负责人员必须记录和保存供应商名单、所提供的服务和合同信息。

5.3 签署协议

为了履行协议并行使 LVMH W&J 的合同权利，相关部门有义务参与客户个人信息的生命周期管理。

5.3.1 客户个人信息的收集

如属客户个人信息委托管理，在委托供应商收集客户个人信息之前，

- 事业部必须与安全团队协商，起草并向供应商发送书面批准（作为购买协议的一部分，或通过电子邮件或其他可记录的传输形式发送），指明授权收集客户个人信息的范围（即客户个人信息的类型、收集方式、收集频率、收集目的等），收集应当遵循适用法律规定的最低收集原则。
- 事业部还必须明确需要收集客户个人信息的核心/附加业务功能，并在书面批准中指明该等信息。
- 事业部必须向供应商发送隐私政策，并就如何在各数字渠道发布和保持隐私政策作出指示。如果隐私政策有更新，事业部必须及时向供应商发送最新版的隐私政策。

如属客户个人信息委托管理和数据共同控制者，

- 事业部负责对供应商收集客户个人信息活动的合法性进行监督（如供应商是否在 LVMH 授权的范围之外收集了客户个人信息、供应商是否从非法渠道购买了客户个人信息），并立即向安全团队和法务部报告任何违约行为。

5.3.2 客户个人信息的存储

如属客户个人信息委托管理，

- 默认情况下，供应商只允许在中国境内存储客户个人信息。如确实需要在中国境外存储、处理客户个人信息，事业部应向供应商出具书面批准（更多信息请参阅本政策“*5.3.4 客户个人信息的传输*”）。
- 在选择 LVMH W&J 的阿里云平台（请参阅 LVMH 集团的原则）之前
    - 如果供应商对客户个人信息以及供应商网站上托管的全部数据提供 SAAS 服务，则事业部必须要求供应商提供客户个人信息保护政策和机制以及相关证书（如 MLPS、ISO/IEC 27001、ISO/IEC

27018、ISO/IEC 29151、安全产品认证）。

如属客户个人信息委托管理和数据共同控制者，

- 事业部必须要求供应商提供：1)数据安全政策和标准的相关文件；2)身份和访问管理相关政策；3)有权访问客户个人信息的员工名单；4)备份政策和标准；5)供应商为保护所存储的客户个人信息所采取的每一项安全措施的记录；6)记录该等安全措施发生任何重大变更的文件；7)年度测试和审计报告；和 8)协议第 4 条第 7 款所述的其他材料（如适用）；9)提供与 CSL 相关的认证；10)访问日志管理机制。
- 安全团队必须审核上述文件，识别可能导致违反协议的任何可能风险。安全团队应：1)提出强化数据保护措施，并由事业部和供应商协商；2)针对被视作重大和重要的风险，考虑采取补充控制措施。

5.3.3 客户个人信息的处理

如属客户个人信息委托管理，

- 事业部必须要求供应商提供：1)客户个人信息保护计划或政策；2)客户个人信息保护相关角色和责任的清单；3)供应商的安全联系人员的联系方式；4)客户个人信息安全影响评估报告；5)人员管理和培训记录；6)安全事件的事件响应计划；7)处理活动登记册；8)协议第 4 条第 10-18 款中提到的其他材料（如适用）。
- 安全团队必须审核上述文件，识别可能导致违反协议的任何可能风险。针对被视作重大和重要的风险，安全团队应当考虑采取补充控制措施。
- 如果供应商提议在处理客户个人信息时使用分包商，在作出决定之前，事业部必须就分包商可能给客户个人信息的处理带来的任何潜在风险咨询安全团队。如果事业部批准使用分包商，则分包商必须签署载有（在相关的范围内）与协议条款条件相同的条款和条件的合同/协议，以管控分包商的处理活动。在此情况下，必须取得安全团队的建议和法务部的批准。事业部必须起草聘用分包商的书面批准并发送给供应商。
- 如果供应商与第三方合并、被第三方兼并或直接或间接受第三方控制，则事业部必须决定是否继续委托管理客户个人信息。在作出决定之前，事业部必须就潜在风险咨询安全团队。如需停止客户个人信息委托管理，事业部必须立即通知供应商，且供应商不得向该第三方披露 LVMH W&J 的任何客户个人信息，且需在事业部规定的时限内向 LVMH W&J 交还客户个人信息，或永久销毁供应商持有的全部客户个人信息；如果可继续委托管理客户个人信息，则事业部必须向供应商出具书面批准，并要求供应商继续遵守协议。
- 如果发生任何实际的或合理怀疑的安全事件或数据泄露，事业部必须：1) 与供应商的安全联系人保持

密切沟通，并在内部事件响应流程结束后立即向 LVMH W&J 管理层和安全团队报告该事件；2)要求供应商遵守协议中有关“未经事先书面同意，供应商不得将任何数据通知任何第三方，包括相关客户”的条款；3)必要时配合 LVMH W&J 公关团队进行相关的公开披露工作；4)事件发生后，要求供应商按照协议提供安全事件登记册；安全团队必须：1)必要时，从安全团队指派负责人或委托第三方调查机构进行调查；2)监督供应商的补救措施，以减轻安全事件的影响；3)必要时，CISO 必须配合相关监管机构的调查和约谈；如对安全事件所导致的损失/费用的厘定有争议，根据 LVMH W&J 关于合同管理的法律事务相关规定，法务部和事业部应参与调查和谈判，以减轻 LVMH W&J 的损失。

5.3.4 客户个人信息的传输

如属客户个人信息委托管理，

- 默认情况下，供应商只允许在中国境内进行客户个人信息的生命周期管理。如果在签署协议期间，因供应商自身的技术和服务问题，供应商提议跨境传输客户个人信息，则事业部必须与安全团队共同决定是否有必要进行跨境传输、拟传输哪些客户个人信息、跨境传输的潜在风险等，以及如不进行跨境传输，则在拒绝供应商提议的情况下业务将受到哪些影响等。法务部负责就合规问题发表意见。
- 如果确实需要跨境传输，应符合《一般服务购买协议》附件五第 2.7 条（个人数据的国际传输）所述的跨境传输条件。在跨境传输之前，事业部有权审查供应商起草的客户个人信息安全评估报告，并在向供应商发出书面批准之前与安全团队协商。

如属客户个人信息委托管理和数据共同控制者，在供应商向 LVMH W&J 传输所收集和/或存储的客户个人信息时，

- 事业部必须指派一名负责收集客户个人信息的人员。事业部必须检查供应商是否对电子邮件或便携式存储设备发送的文件进行了加密处理、供应商是否采用了可靠的交付渠道以及所收到的客户个人信息是否完整有效，以确保客户个人信息的安全传输。

5.3.5 客户个人信息的销毁

客户个人信息的存储期期满后，事业部必须确保供应商已停止收集客户个人信息，并已交还和/或销毁供应商所持有的全部客户个人信息。如有必要，安全团队有权从安全团队指派一位负责人进行现场审计，检查确认供应商是否已履行其义务；或事业部有权要求供应商提供相关证据。

5.4 供应商监控和评估

5.4.1 持续监控和监督

在与供应商合作期间，安全团队有权利用其专业知识，代表事业部指导和监控供应商履行情况。如发现任

何违反协议或适用法律的情况，安全团队必须立即通知事业部，且事业部必须敦促供应商进行整改。

事业部必须向供应商传达全部客户个人信息保护要求，并监督补救措施实施情况。事业部对供应商遵守协议负有最终责任。

法务部必须从合规角度提供法律意见。

如果发生任何合同纠纷，参照 LVMH W&J 关于合同管理的法律事务相关规定予以解决。

5.4.2 集中风险管理

在管理具有制度集中化特征的供应商时，应当加强监控供应商的频率和力度，防止因供应商突然终止服务或服务质量急剧下降对 LVMH W&J 业务造成的负面影响。

事业部应要求具有制度集中化特征的供应商向 LVMH W&J 提供相对专用的资源，如服务团队、场所、系统和设备等，并定期检查资源情况，以确保资源的即时可用性。

事业部应与该等供应商保持密切联系，并要求供应商提供确凿证据，证明其遵守协议的情况。

5.4.3 年度审计

事业部必须牵头开展年度供应商评估/审计，监控供应商的资质情况；在此期间，安全团队应当规划供应商的年度客户个人信息保护安全审计工作。年度审计的复杂程度取决于供应商将提供的服务（即是属于客户个人信息委托管理、委托开发还是供应商作为数据共同控制者），并以协议项下的适用要求为依据：

- 如属客户个人信息委托管理和数据共同控制者，则年度审计的范围包括但不限于：政策和标准、网络安全、物理安全、身份和访问管理、信息系统的使用、信息传输安全；
- 如属委托开发，则年度审计的范围包括但不限于：政策和标准、加密情况、物理安全、代码安全、系统安全架构。

可由安全团队、安全团队指定的第三方开展年度审计或通过要求供应商根据【供应商年度自检清单】完成自检来开展年度审计。同时，法务部可从隐私和合规角度支持年度审计，并就法律问题提供建议。年度审计结果必须能够反映供应商遵守协议的情况。事业部必须记录并向安全团队和 CTO/CIO 报告年度审计结果。

对于年度审计中发现的客户个人信息保护风险，安全团队应识别安全控制差距，并就补救提供建议。相应地，事业部必须敦促供应商立即采取整改措施，确保适当处理所有已发现的安全控制差距并交由安全团队审查。

5.5 供应商关系终止

协议终止或期满（未续约）后，事业部必须确保供应商已停止收集客户个人信息，并已交还和/或销毁供应

商所持有的全部客户个人信息。为此，如有必要，安全团队有权从安全团队指定一名负责人，在其认为有用的任何检查中确认供应商是否已履行其义务；或事业部有权要求供应商提供相关证据。

第 6 章：适用法律

本章概述了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）》

《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

第 7 章：政策管理

7.1 政策所有者

作为政策所有者，安全团队必须每年或在其认为必要时审核本政策。如果适用法律或监管指南发生重大变化，或产品/服务、供应商关系管理发生变化，安全团队应聘请经验丰富且具有专业知识的人员更新本政策。

7.2 审批

CTO/CIO 须负责审批本政策，并每两年或在其认为必要时审核并重新批准本政策。

本政策可不时予以修改或补充。可采用强化政策要求、补充限制和宽免或补充风险相关措施等形式补充本政策。只要该等补充文件是为了促进本政策中规定的原则和限制，且不具有减轻该等原则和限制的效果，则无需事先获得 CTO/CIO 的批准。

7.3 冲突解决

本政策的所有例外情况均须取得安全团队和 CTO/CIO 的批准。

2019

Customer Personal Information Protection Policy

FOR VENDOR MANAGEMENT

LVMH
WATCHES & JEWELRY

Contents

Chapter 1: Objective

The Customer Personal Information Protection Policy – For Vendor Management (this "Policy") provides guidelines for managing Vendor with respect to customer personal information protection. This Policy encompasses personal information protection standards to ensure all vendors of LVMH, Watch & Jewelry("LVMH W&J") meet the objectives of customer personal information protections and fulfill contractual obligations prescribed in *[Customer Personal Information Protection Agreement – For Vendor Use]*(the "Agreement") under the supervision of LVMH W&J.

Chapter 2: Scope

This Policy applies to LVMH China W&J departments, including Purchase Department, Business Unit, Security Team and Legal.

Chapter 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.

“Vendor Performance” means Vendor’s performance on CPI protection.

“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.

Chapter 4: Governance and Responsibility

4.1 Purchase Department

Purchase Department shall be responsible for 1) participating in Vendor Admission and ensuring the qualification of Vendor meets the requirements by LVMH W&J, 2) reviewing Vendor annual audit results and quality control.

4.2 Business Unit

Business Unit with interaction with contracted Vendor is responsible for 1) taking charge of Vendor management, 2) serving as the internal contact in LVMH W&J with Vendor, 3) delivering CPI protection requirements proposed by Security Team to Vendor in time, 4) supervising and be accountable for Vendor Performance, 6) reporting Vendor's violation of internal information security policies and this Policy.

4.3 Security Team

Security Team is be responsible for 1) developing and maintaining information security program including CPI protection strategy, policy and associated procedures (including this Policy), 2) developing CPI protection security objectives and requirements for specific projects, 3)contributing to Vendor Admission from the CPI protection perspective,4) cooperating with Vendor during the execution of the Agreement, 5) guiding and monitoring Vendor CPI protection Performance,6)liaising with relevant external regulators when required.

4.4 Legal

Legal shall be responsible for 1) reviewing contracts/agreements with Vendor, 2) supporting execution of the Agreement from legal compliance perspective, 3) providing legal consultation for any contractual dispute.

Chapter 5: Vendor management

5.1 Vendor Admission

In light of the overarching CPI protection strategy developed by Security Team, Security Team shall be responsible for developing overall CPI protection objectives (e.g. intensity of control over access management of CPI, technical measures for transfer/storage, *etc.*) for specific projects involving contracted Vendor, taking business scenarios and nature of CPI to be collected, which shall be aligned with Business Unit, into account. Security Team is also responsible for developing Vendor assessment system in line with internal Vendor security policies and formulating

[Vendor Information Security Assessment] and checklists.

Before engaging any Vendor, Business Unit should lead CPI security impact assessment to assess and deal with security risks in CPI processing activities. Detailed information refers to *[Customer Personal Information Protection Policy – For Employee Management]*.

5.1.1 Admission Assessment

During the Vendor admission stage, Purchase department and Business Unit must lead Vendor qualification verification before placing an order or entering into a contract with any Vendor. Business Unit must fill in the checklists from [Vendor Information Security Assessment]. The engagement risk is determined based on criteria in relation to the confidentiality, integrity, availability and traceability requirements over Vendor.

Admission assessment results must clarify whether Vendor is capable to fulfill the CPI protection objectives developed by Security Team and whether LVMH W&J can accept the data security risks brought by the introduction of the Vendor. Admission assessment results must be communicated with Security Team. Security Team should advise on Vendor admission from the CPI protection perspective, and Vendor with the following characteristics is preferred:

- Vendor is capable to ensure the security of CPI.
- Storage and processing of CPI within the territory of China is preferred.
- Vendor is willing to provide dedicated resources in protecting CPI and dealing with Security Incident.

With regards to risks identified during the admission assessment, Security Team shall consider any feasible and economical compensatory controls in order to alleviate any potential consequences brought by such risks. Such compensatory controls will be implemented by Security Team during the execution of the Agreement with Vendor.

5.1.2 Vendor due diligence

Business Unit must work with the Purchase Department to lead due diligence of Vendor. Security Team is responsible for planning Vendor information security due diligence as part of due diligence. Security due diligence can be performed at the premise of Vendor by Security Team/third-party designated by Legal or Security Team. Security due diligence can also be performed by Business Unit requesting Vendor to provide evidence according to a list of evidence to be collected drafted by Security Team.

The content of due diligence may include but is not limited to:

- Reputation
- Professional experience and quality of responsible personnel
- Valid information security related certification (e.g. ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 29151,security product certification)
- Physical security for offices and facilities
- Information security incident history
- Violation history

Security Team may customize the content of the security due diligence according to business needs and the actual situation of Vendor. Results of the security due diligence should be reported to Business Unit and Purchase department. Business Unit and Purchase Department must examine the authenticity of Vendor's qualification based on security due diligence results along with other due diligence programs.

Additionally, if Vendor is using subcontractors to support the LVMH W&J relationship, LVMH W&J expects that Vendor manages its own due diligence program to review the qualification of the subcontractor.

5.2 Agreement Award

Legal, Purchase Department, Business Unit and Security Team must review contracts and agreements with Vendor. Participation of Legal is restricted to the discussion of the issues pertaining to legal aspects of the contract.

Security Team has drafted LVMH W&J standard Vendor CPI protection agreement template (the Agreement) for the certain types of Vendor and recommends it for conclusion.

In the event of using LVMH W&J's agreement template,

- Security Team must customize the Agreement according to 1) the CPI protection objectives and requirements for specific projects, 2) types of Vendor, 3) the actual situation of Vendor and 4) compensatory controls to be implemented. Security Team must ensure clauses in the Agreement contain all necessary security measures to protect the Confidentiality, Availability and Integrity of CPI.
- Business Unit may input any business concerns related to specific clauses in the Agreement. Such business concerns must encompass the importance of business, the importance of Vendor and nature of CPI (amount of CPI, amount of Customers, sensitivity of CPI).
- Any changes to the legal terms of the Agreement are subject to final approval from Legal. In addition,

Legal must keep tracking the evolutionary personal information protection related legislation and cooperate with Security Team in updating the Agreement as an on-going effort. Legal must ensure that the Agreement contains all applicable protection requirements prescribed in Applicable Legislation.

If template of the Agreement is drafted by Vendor, Vendor's template must be reviewed by Legal, Business Unit, Security Team and Purchase Department to ensure it sets out the same rights and obligations as those set out in the Agreement to the extent relevant, including in particular the obligation to ensure the protection of CPI, compliance to Applicable Legislation and the right to audit. If Vendor's template fails to do so, Legal must negotiate the foregoing requirements with Vendor and make necessary amendments to relevant provisions.

The signing of agreements with Vendor on behalf of LVMH W&J is allowable only after its approval from Legal. Business Unit organizes the signing of the Agreement on behalf of LVMH W&J. The Agreement along with the*[Confidentiality Agreement],*must be signed by Business Unit with Vendor and/or by sub-contractors of Vendor. The terms and conditions laid down by the Agreement shall prevail over Vendor's security documents.

Vendor lists, services provided, and contractual information must be recorded and maintained by the responsible personnel from Security Team.

5.3 Execution of the Agreement

In order to implement the Agreement and fulfill LVMH W&J's contractual rights, associated departments are obligated to participate in the Lifecycle Management of CPI.

5.3.1 Collection of CPI

In the event of Commissioned Management of CPI, prior to commission collection of CPI to Vendor,

- Business Unit must draft written approval, in consultant with Security Team, and sent it to Vendor (as part of the Purchase Agreement, or by email or other recordable forms of transmission) to specify the authorized scope of CPI collection (i.e. types of CPI, methods of collection, frequency of collection, purpose of collection, *etc.*) which shall follow the minimum collection principle prescribed by Applicable Legislation.
- Business Unit must also determine the core/additional business functions that require collecting CPI and specify such information in the written approval.
- Business Unit must send privacy policy to Vendor followed by instructions on how to release and maintain

privacy policy on each Digital Channel. If privacy policy is updated, Business Unit must send the latest version of privacy policy to Vendor in time.

In the event of Commissioned Management of CPI and Data Co-controller,

- Business Unit is responsible for supervise the legitimacy of Vendor's collection activities of CPI (e.g. whether Vendor collects CPI out of the scope authorized by LVMH, whether Vendor purchases CPI from illegal channels) and report any breach of the Agreement to Security Team and Legal immediately.

5.3.2 Storage of CPI

In the event of Commissioned Management of CPI,

- By default, Vendor is only allowed to store CPI within the territory of China. If storage and processing of CPI outside the territory of China is indeed necessary, Business Unit shall issue written approval to Vendor (more information refers to *"5.3.4 Transfer of CPI"* in this Policy).
- Prior to choose LVMH W&J Ali yun cloud platform (refer to LVMH group principle)
    - If vendor provides SAAS service of CPI and all the data hosting on vendor site, business unit must request vendor to provide CPI protection policy and mechanism and certificates (e.g. MLPS, ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 29151, security product certification)

In the event of Commissioned Management of CPI and Data Co-controller,

- Business Unit must request Vendor to provide 1) relevant documents pertaining to data security policy and standard, 2) Identity and access management related policy, 3) lists of employees who have access to CPI, 4) backup policy and standard, 5) records regarding every security measure implemented by Vendor to protect stored CPI, 6) documents recording any major change to such security measures, 7) annual test and audit reports, and 8) other materials mentioned in Clause 7 in Article 4 of the Customer Personal Information Protection Agreement- For Vendor Use, if applicable. 9) provide CSL related to authentications. 10) access log management mechanism
- Security Team must review the above documents and identify any possible risks that may leads to violation of the Agreement. Security Team should 1) propose enhanced data protection measures, which should be communicated with Vendor by Business Unit,2) consider deploying compensatory control measures especially for risks regarded as critical and important risks.

5.3.3 Processing of CPI

In the event of Commissioned Management of CPI,

- Business Unit must request Vendor to provide 1) CPI protection plans or policies, 2) lists of CPI protection related roles and responsibilities, 3) contact information of Vendor's security contact personnel, 4) CPI security impact assessment reports, 5) records of personnel management and training, 6) incident response plans for Security Incident,7) register of the Processing activities, 8) other materials mentioned in Clause 10-18 in Article 4 of the Agreement, if applicable.
- Security Team must review the above documents and identify any possible risks that may leads to violation of the Agreement. Security Team should consider deploying compensatory control measures especially for risks regarded as critical and important risks.
- If Vendor propose including any sub-contractors in processing CPI, Business Unit must consult Security Team regarding any potential risks that sub-contractors may bring to processing of CPI before making decisions. If sub-contractors have been authorized by Business Unit, contracts/agreements that set out the same rights and obligations as those set out in the Agreement to the extent relevant must be signed by sub-contractors to govern the processing activities by the latter. Under this circumstance, advice from Security Team and approval from Legal must be sought. Written approval for engaging sub-contractors must be drafted by Business Unit and send to Vendor.
- When Vendor merges with a third party, is merged by a third party or is directly or indirectly controlled by a third party, Business Unit must decide whether Commissioned Management of CPI may continue. Business Unit must consult Security Team regarding any potential risks before making decisions. If Commissioned Management of CPI needs to stop, Business Unit must inform Vendor immediately that the latter must not disclose any CPI of LVMH W&J to the third party and return the CPI to LVMH W&J within the time period defined by Business Unit or destroy permanently all CPI that Vendor may hold; If Commissioned Management of CPI may continue, Business Unit must send written approval to Vendor and request the latter to remain compliant to the Agreement.
- In case of any actual or reasonably suspected Security Incident or Data Breach, Business Unit must 1) keep close communication with Vendor's security contact and report the incident to LVMH W&J management and Security Team immediately following the internal incident response process, 2)request Vendor to follow the

relevant clauses in the Agreement stipulating Vendor shall not inform any third party, including concerned Customer, of any Data Breach without first obtaining prior written consent, 3) cooperate with PR team of LVMH W&J in public disclosure related affairs, if necessary, 4) request Vendor to provide the register of Security Incidents as per the Agreement after the incident; Security Team must 1) assign responsible personnel from Security Team or commission third party investigation agency to conduct investigation if necessary, 2) monitor Vendor's remediation actions to mitigate the effects of Security Incident, 3) CISO must cooperate with investigation and interviews of associated regulatory bodies when required; In the case where the determination of the damage/cost caused by Security Incident is disputed, Legal and Business Unit should beinvolved in investigations and negotiations to reduce LVMH W&J's losses following relevant provisions of LVMH W&J's legal affairs on contract management.

5.3.4 Transfer of CPI

In the event of Commissioned Management of CPI,

- By default, Vendor is only allowed to keep the Lifecycle Management of CPI exclusively in the territory of China. Should Vendor propose cross-border transfer of CPI due to Vendor's own technology and service concerns during the execution of Agreement, Business Unit must involve Security Team in decision-making process to figure out whether cross-border transfer is necessary, which CPI to be transferred, any potential risks in cross-border transfer, *etc.* and if not, how business would be affected if Vendor's proposal has been denied ,*etc.* Legal is responsible for commenting on compliance issues.
- Should cross-border transfer be indeed necessary, it should conform to conditions for cross-border transfer refers to 2.7 "International transfers of Personal Data" in Attachment V of *General Service Purchase Agreement.* Prior to the cross-border transfer, Business Unit is entitled to review CPI security assessment report drafted by Vendor and consult with Security Team before issuing written approval to Vendor.

In the event of Commissioned Management of CPI and Data Co-controller, when Vendor transfers collected or/and stored CPI to LVMH W&J,

- Business Unit must assign responsible personnel to collect CPI. Business Unit must ensure the secure transfer of CPI by examining whether files sent via Email or portable storage devices have been encrypted by Vendor, whether Vendor has adopted reliable delivery channels, whether received CPI is complete and valid.

5.3.5 Destruction of CPI

When the storage period of CPI expires, Business Unit must ensure Vendor has stopped collecting of CPI and has returned and/or destroyed all the CPI Vendor holds. Security Team is entitled to carry out checks to confirm whether Vendor has fulfilled its obligation by assigning responsible personnel from Security Team in on-site audit, if necessary; or Business Unit is entitled to request Vendor to provide evidence.

5.4 Vendor Monitoring and Evaluation

5.4.1 On-going Monitoring and Supervision

During the engagement with Vendor, Security Team is entitled to leverage their expertise in guiding and monitoring Vendor Performance on behalf of Business Unit. Should any violation of the Agreement and Applicable Legislation have been discovered, Security Team must immediately inform Business Unit and the latter must urge Vendor to make corrections.

Business Unit must communicate all the CPI protection requirements to Vendor and supervising remediation actions.

Business Unit is ultimately accountable for Vendor's compliance to the Agreement.

Legal may provide legal consultation from the compliance perspective.

In case of a contractual dispute, it shall be handled with reference to the relevant provisions of LVMH W&J's legal affairs on contract management.

5.4.2 Centralized Risk Management

When managing Vendor with the characteristics of institutional concentration, the frequency and intensity of monitoring against Vendor should be enhanced to prevent negative effects on LVMH W&J's business caused by unexpected termination of Vendor's services or sharp decline in service quality.

Business Unit should require Vendor with the characteristics of institutional concentration to provide LVMH W&J with relatively dedicated resources, such as service teams, sites, systems and equipment and regularly check the resources to ensure the timely availability of the resources.

Business Unit should keep close communication with such Vendor and request the latter to provide solid evidence to demonstrate its compliance situation to the Agreement.

5.4.3 Annual Audit

Business Unit must lead the annual Vendor evaluation/audit to monitor Vendor's qualification, during which Security Team should plan the annual CPI protection security audit for Vendor. The complexity of annual audit will depend on the service to be fulfilled by Vendor (i.e. whether Commissioned Management of CPI, Commissioned Development or vendor serving as Data Co-controller) and can be derived from applicable requirements under the Agreement:

- In the event of Commissioned Management of CPI and Data Co-controller, scope of the annual audit includes but is not limited to: policy and standard, network security, physical security, Identity and access management, usage of information system, information transmission security;
- In the event of Commissioned Development, scope of the annual audit includes but is not limited to: policy and standard, cryptography, physical security, code security, security architecture of system.

Annual audit can either be conducted by Security Team, third-party designated by Security Team or by requesting Vendor to complete self-check in accordance with the [Vendor Annual Self-Checklist]. Meanwhile, Legal may support the annual audit from the privacy and compliance perspective and advising on legal concerns. Annual audit result must be able to reflect Vendor's compliance situation with the Agreement. Annual audit results must be recorded by Business Unit and reported to Security Team and CTO/CIO.

With respect to CPI protection risks identified in annual audit, Security Team should identify security control gaps and provide recommendations for remediation. Accordingly, Business Unit must urge Vendor to immediate correction actions and make sure all identified security control gaps are appropriately treated and reviewed by Security Team.

5.5 Vendor Relations Termination

Upon termination or expiry of the Agreement (with no contract renewal), Business Unit must ensure Vendor has stopped collecting of CPI and has returned and/or destroyed all the CPI Vendor holds. As such, Security Team is entitled to designate responsible personnel from Security Team in any checks it deems useful to confirm whether Vendor has fulfilled its obligation, if necessary; or Business Unit is entitled to request Vendor to provide evidence.

Chapter 6: Applicable Legislation

This chapter outlines relevant laws, regulations, rules, national standards and guidelines applicable to the protection of CPI, 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)

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

Chapter 7:Policy Administration

7.1 Policy Owner

As the policy owner, Security Team must review this Policy annually or as deemed necessary. Security Team should engage experienced and knowledgeable resources to update this Policy if there are significant changes in Applicable Legislation, or regulatory guidance, or changes in the products/services, Vendor relations management.

7.2 Approval

CTO/CIO must approve this Policy and must review and re-approve this Policy every two years or as deemed necessary.

This Policy may be modified or supplemented from time to time. The supplements may take the form of enhanced policy requirements, additional limits and tolerances, or additional risk-related steps. So long as such supplements are in furtherance of the principles and limits set forth in this Policy, and do not have the effect of reducing them, they are permitted without prior CTO/CIO approval.

7.3 Resolution of Conflicts

All exceptions to this Policy must be approved by Security Team and CTO/CIO.