A. Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China) (Contract Language: Chinese)

Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China)

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，经双方协商一致，订立本合同。

双方确认并同意，本合同的中文版本为双方签订的正式版本。 非正式的英文翻译版本仅供无法阅读中文的人士理解参考。 如果双方同意签订本合同的英文版本，该等同意应被理解为双方已经签订了本合同的中文版本。

个人信息处理者：见附件 7-相关方名单

地址：见附件 7-相关方名单

联系方式：见附件 7-相关方名单

联系人：见附件 7-相关方名单　　职务：见附件 7-相关方名单

境外接收方：见附件 7-相关方名单

地址：见附件 7-相关方名单

联系方式：见附件 7-相关方名单

联系人：见附件 7-相关方名单 职务：见附件 7-相关方名单

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，双方【已】/【约定】于【主协议签订日期】订立一份商业合同，即主协议。

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，双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"双方"。

（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：详见附件 E – 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：

（1）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。

（2）已采取的补救措施。

（3）个人信息主体可以采取的减轻危害的措施。

（4）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）双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）双方声明，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：

（1）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。

（2）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。

（3）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）双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

双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双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：境外接收方授权答复有关个人信息处理的询问或者投诉的联系人为境外接收方的数据保护人员。个人信息主体可通过境外接收方网站公布的电话及电子邮件联系该等人员。更多详情，请参见附件"中国互联网信息办公室"，该文件将向或已向当地的中国互联网信息办公室备案。

（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，双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）双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）双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）双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）经双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）双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）双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双方承担责任。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）如本合同与双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、因本合同引起的双方间的任何争议，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（具体地址以主协议中载明的地址为准）

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 7 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 3 个工作日应当视为收讫。

（四）双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，双方应当协商解决；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 德国慕尼黑 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）本合同正本一式贰份，双方各执 壹份，其法律效力相同。本合同于线上签订或签署（且可作为原始、有效的条款和条件执行，无需签名）

个人信息处理者：[签署主协议的授权签字人]_____

_____年_____月_____日[主协议签署日期]

境外接收方：[签署主协议的授权签字人]_____

_____年_____月_____日[主协议签署日期]

附录一

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：见附件 D -处理或传输说明

（二）处理方式：见附录 D -处理或传输说明中的“（次级）处理性质”

（三）出境个人信息的规模：小规模处理及传输个人信息。更多详情，请参见附件“中国互联网信息办公室”，该文件将向或已向当地的中国互联网信息办公室备案。

（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）：

个人信息（参考 GB/T 35273-2020 第 3.1 条）

个人信息主体（参考 GB/T 35273-2020 第 3.3 条）

个人信息控制者（参考 GB/T 35273-2020 第 3.4 条）

明示同意（参考 GB/T 35273-2020 第 3.6 条）

授权同意（参考 GB/T 35273-2020 第 3.7 条）

个性化展示（参考 GB/T 35273-2020 第 3.16 条）

业务功能（参考 GB/T 35273-2020 第 3.17 条）

更多详情，请参见附件"中国互联网信息办公室"，该文件将向或已向当地的中国互联网信息办公室备案。

（五）出境敏感个人信息种类（如适用，参考 GB/T 35273《信息安全技术 个人信息安全规范》和相关标准）：无

（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）：不适用

（七）传输方式：网络在线传输

（八）出境后保存期限：

自主协议生效之日至主协议终止之日（待确定）

（九）出境后保存地点：境外接收方的办公地址或注册地址，或其次级信息处理者的保存地点。

（十）其他事项（视情况填写）：无

附录二

双方约定的其他条款（如需要）

无。

B. Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China) (Contract Language: English)

Standard Contract for Outbound Cross-border Transfer of Personal Information (People's Republic of China)

The Personal Information Handler and the Overseas Recipient will carry out the activities concerning the outbound cross-border transfer of Personal Information in accordance with this Contract. The Parties have entered into or agreed to enter into a commercial contract to further the commercial acts related to such activities, namely the Main-Agreement on the date of conclusion of the Main-Agreement.

The major body of this Contract is drafted in accordance with the requirements of the *Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information*. Other agreements between the Parties, if any, may be specified in Appendix II. The Appendix forms an integrated part of this Contract.

Article 1 Definitions

In this Contract, unless the context otherwise requires:

1. "Personal Information Handler" refers to any organization or individual that independently decides the purpose and method of the Personal Information handling activities and transfers Personal Information outside the territory of the People's Republic of China.

2. "Overseas Recipient" refers to an organization or individual outside the territory of the People's Republic of China that receives Personal Information from the Personal Information Handler.

3. Personal Information Handler or Overseas Recipient are referred to individually as a "Party", and collectively as the "Parties".

4. "Personal Information Subject" refers to a natural person identified by or associated with the Personal Information.

5. "Personal Information" refers to all kinds of information related to identified or identifiable natural persons that are electronically or otherwise recorded, excluding information that has been anonymized.

6. "Sensitive Personal Information" refers to the Personal Information that, once leaked or illegally used, is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety, including biometric recognition, religious belief, specific identity, medical health, financial account, personal whereabouts, and the Personal Information of minors under the age of 14.

7. "Regulatory Authority" refers to the Cyberspace Administration of the People's Republic of China at the provincial level or above.

8. "Relevant Laws and Regulations" refer to the laws and regulations of the People's Republic of China, such as the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, the *Civil Code of the People's Republic of China*, *Civil Procedure Law of*

the People's Republic of China, and *Measures for the Standard Contract for Outbound Cross-border Transfer of Personal Information*.

9. The meanings of other terms not defined in the Contract are in line with those stipulated in the Relevant Laws and Regulations.

Article 2 Obligations of the Personal Information Handler

The Personal Information Handler shall perform the following obligations:

1. Handle Personal Information in accordance with the Relevant Laws and Regulations. The Personal Information to be transferred overseas shall be limited to the minimum scope required for the purpose of handling.

2. Inform the Personal Information Subject of matters such as the name and contact information of the Overseas Recipient, the purpose of handling, method of handling, type of Personal Information, retention periods, and the methods and procedures for the Personal Information Subject to exercise his/her rights specified in Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*". Where Sensitive Personal Information is transferred overseas, the Personal Information Subject shall be informed of the necessity of the outbound cross-border transfer of Sensitive Personal Information and the impact on the rights and interests of the Personal Information Subject, unless otherwise provided in the laws and administrative regulations that such notification is not required.

3. If Personal Information is transferred overseas based on the consent of the individual, the separate consent of the Personal Information Subject shall be obtained. Where the Personal Information involves that of a minor under the age of 14, the separate consent of the minor's parent or any other guardian, shall be obtained. Where written consent is required by laws and administrative regulations, the written consent shall be obtained.

4. Inform the Personal Information Subject that the Personal Information Handler and the Overseas Recipient have agreed that the Personal Information Subject is a third-party beneficiary under this Contract, and if the Personal Information Subject fails to raise an express rejection within thirty days, the Personal Information Subject shall be entitled to act as a third-party beneficiary in accordance with the Contract.

5. Make reasonable efforts to ensure that the Overseas Recipient has taken the following technical and organizational measures to perform its obligations under this Contract (taking into account potential Personal Information security risks that may be caused by the purpose of Personal Information handling, the type, scale, scope and sensitivity of the Personal Information, the scale and frequency of the transfer, the period of the outbound cross-border transfer of Personal Information, the period of retention by the Overseas Recipient, and other matters that may lead to a Personal Information security risk): APPENDIX E. – TECHNICAL AND ORGANISATIONAL MEASURES.

6. Provide copies of Relevant Laws and Regulations and technical standards to the Overseas Recipient upon request.

7. Reply to inquiries from the Regulatory Authority about the Overseas Recipient's handling activities.

8. Carry out a Personal Information Protection Impact Assessment in accordance with the Relevant Laws and Regulations regarding the proposed transfer of Personal Information to the Overseas Recipient. The assessment shall focus on the following matters:

(1) the legality, legitimacy and necessity of the purpose, scope and method of handling Personal Information by the Personal Information Handler and Overseas Recipient;

(2) the scale, scope, type, and sensitivity of Personal Information to be transferred overseas, and the risks that the outbound cross-border transfer may pose to Personal Information rights and interests;

(3) the obligations that the Overseas Recipient undertakes to assume, and whether the organizational and technical measures and capabilities to perform such obligations are sufficient to ensure the security of the Personal Information to be transferred overseas;

(4) risk of Personal Information being tampered with, destroyed, leaked, lost, illegally used, etc. after the outbound cross-border transfer, and whether there are channels for individuals to smoothly exercise Personal Information rights and interests etc.;

(5) in accordance with Article 4 hereof, to evaluate whether the performance of this Contract will be affected by the local policies and regulations with respect to protection of Personal Information; and

(6) other matters that may affect the security of outbound cross-border transfer of Personal Information.

The Personal Information Protection Impact Assessment Report shall be kept for at least three years.

9. Provide a copy of this Contract to the Personal Information Subject upon the Personal Information Subject 's request. If trade secrets or confidential business information are involved, the relevant contents of the copy of this Contract may be appropriately redacted, provided that such redaction will not affect the understanding of the Personal Information Subject.

10. Assume a burden of proof for the performance of obligations under this Contract.

11. In accordance with Relevant Laws and Regulations, provide the Regulatory Authority with all information as described in Article 3.11, including all compliance audit results.

Article 3 Obligations of the Overseas Recipient

The Overseas Recipient shall perform the following obligations:

1. Handle the Personal Information in accordance with Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*". Where the Overseas Recipient handles the Personal Information in a way beyond the purpose and method of the Personal Information handling, and types of the Personal Information as agreed, it shall obtain the separate consent of the Personal Information Subject in advance if the handling of Personal Information is based on the consent of the Personal Information Subject; where the Personal Information of a minor under the age of 14 is involved, the separate consent of the minor's parent, or any other guardian, shall be obtained.

2. Where the Overseas Recipient is contracted by the Personal Information Handler to handle Personal Information, the Overseas Recipient shall handle the Personal Information in accordance with the agreement with the Personal Information Handler and shall not handle the

Personal Information in a way beyond the purpose or method of the Personal Information handling.

3. Provide a copy of this Contract to the Personal Information Subject upon the Personal Information Subject's request. If trade secrets or other confidential business information are involved, relevant parts of this Contract may be appropriately redacted, provided that such redaction will not affect the understanding of the Personal Information Subject.

4. Handle the Personal Information in a manner that has the least impact on the rights and interests of the Personal Information Subject.

5. The retention period of Personal Information shall be the minimum period necessary for achieving the purpose of handling. Upon expiry of the retention period, the Personal Information (including all back-up copies) shall be deleted. Where the handling of Personal Information is contracted by the Personal Information Handler, and the personal information handling agreement fails to become effective, becomes null and void, or is cancelled or terminated, the Personal Information being handled shall be returned to the Personal Information Handler or deleted, and a written statement shall be provided to the Personal Information Handler. If it is technically difficult to delete the Personal Information, the handling of the Personal Information, other than the storage and any necessary measures taken for security protection, shall be ceased.

6. Ensure the security of Personal Information handling in the following ways:

   (1) take technical and organizational measures including but not limited to those listed in Article 2.5 of this Contract and carry out regular inspections to ensure the security of Personal Information; and

   (2) ensure that the personnel authorized to handle Personal Information perform their confidentiality obligations and establish access control permissions of minimum authorization.

7. In the event that Personal information is or may be tampered with, destroyed, leaked, lost, illegally used, provided or accessed without authorization, the Overseas Recipient shall:

   (1) promptly take appropriate measures to mitigate the adverse impact on the Personal Information Subject;

   (2) immediately notify the Personal Information Handler and report to the Regulatory Authority in accordance with the Relevant Laws and Regulations. The notice shall contain the following contents:

      i. the type of Personal Information to which the tampering with, destruction, leakage, loss, illegal use, unauthorized provision or access occurs or may occur, the cause of such event or potential event, and the potential harm;

      ii. remedial measures that have been taken;

      iii. measures that can be taken by the Personal Information Subject to mitigate harm; and

      iv. contact information of the person, or team, in charge of handling the situation.

   (3) where the Relevant Laws and Regulations require the notification of the Personal Information Subject, the content of the notice shall include the foregoing contents in Article 3.7. (2) above; where the handling of Personal Information is contracted by the

Personal Information Handler, the Personal Information Handler shall notify the Personal Information Subject;

(4) record and retain all the situations thereof relating to the occurrence or potential occurrence of tampering, destruction, leakage, loss, illegal use, unauthorized provision or access, including all remedial measures taken.

8. The Overseas Recipient may provide Personal Information to the third party located outside the territory of the People's Republic of China only, if all of the following requirements are met:

(1) there is a necessity from the business perspective;

(2) the Personal Information Subject has been informed of such third party's name, contact information, the purpose of handling, method of handling, type of Personal Information, retention periods, and the methods and procedures for the Personal Information Subject to exercise his/her rights. Where Sensitive Personal Information is provided to such third party, the Personal Information Subject should also be informed of the necessity of the outbound cross-border transfer of Sensitive Personal Information and the impact on the rights and interests of the Personal Information Subject. However, unless otherwise provided by laws and administrative regulations that such notification is not required;

(3) where the handling of Personal Information is based on the consent of the Personal Information Subject, the separate consent of the Personal Information Subject shall be obtained; where the Personal Information of a minor under the age of 14 is involved, the separate consent of the minor's parent, or any other guardian, shall be obtained. Where written consent is required by laws and administrative regulations, such written consent shall be obtained;

(4) enter into a written agreement with the third party to ensure that the handling of Personal Information by the third party meets the standards for protection of Personal Information required by the Relevant Laws and Regulations of the People's Republic of China, and the Overseas Recipient will assume the liability for the infringement of Personal Information Subject's rights due to the provision of Personal Information to the third party located outside the territory of the People's Republic of China;

(5) provide a copy of the above agreement to the Personal Information Subject upon the Personal Information Subject's request. If trade secrets or other confidential business information are involved, relevant parts of the agreement may be appropriately redacted provided that such redaction will not affect the understanding of the Personal Information Subject.

9. Where the Overseas Recipient is contracted by the Personal Information Handler to handle Personal Information, and the Overseas Recipient intends to sub-contract the handling to a third party, the Overseas Recipient shall obtain the consent of the Personal Information Handler in advance and shall ensure that the sub-contractor will not handle Personal Information in a way beyond the purpose and method of the handling as specified in Appendix I "*Description of the Outbound Cross-border Transfer of Personal Information*", and shall monitor the Personal Information handling activities of the third party.

10. When making use of Personal Information for automated decision-making, the Overseas Recipient shall ensure the transparency of decision-making and fair and impartial results, and shall not carry out unreasonable or differential treatment of the Personal Information Subject in terms of transaction conditions, such as transaction price. Where automated decision-making is

used for pushing information and commercial marketing to the Personal Information Subject, the Overseas Recipient shall also provide the Personal Information Subject with options that are not specific to the individuals' characteristics, or a convenient way for the Personal Information Subject to reject the automated decision-making.

11. Undertake to provide the Personal Information Handler with all necessary information required to comply with the obligations under this Contract, provide the Personal Information Handler access to review the necessary data documents, and files, or conduct a compliance audit of the handling activities under this Contract, and the Overseas Recipient shall facilitate the compliance audit conducted by the Personal Information Handler.

12. Maintain an accurate record of the Personal Information handling activities carried out for at least 3 years and provide the relevant records and documents to the Regulatory Authority directly or through the Personal Information Handler, as required by the Relevant Laws and Regulations.

13. Agree to be subject to supervision by the Regulatory Authority during an enforcement procedure related to supervising the implementation of this Contract, including but not limited to responding to inquiries and inspections by the Regulatory Authority, following the actions taken or decisions made by the Regulatory Authority, and providing written confirmation that necessary measures have been taken etc.

Article 4 The Impact of Personal Information Protection Policies and Regulations in the Overseas Recipient's Country or Region on the Performance of this Contract

1. The Parties warrant that they have exercised reasonable care when entering into this Contract and are not aware of Personal Information protection policies and regulations in the Overseas Recipient's country or region (including any requirements on providing Personal Information or authorizing public authorities to access Personal Information) that would have an impact on the Overseas Recipient's performance of its obligations under this Contract.

2. The Parties declare that, when making the warranties in Article 4.1, they have conducted the assessment in conjunction with the following circumstances:

   (1) the specific circumstances of outbound cross-border transfer, including the purpose of handling the Personal Information, the types, scale, scope and sensitivity of the Personal Information transferred, the scale and frequency of transfer, the period of the outbound cross-border transfer of Personal Information and the retention period of the Overseas Recipient, the previous experience of the Overseas Recipient with respect to outbound cross-border transfer and handling of similar Personal Information, whether any Personal Information security incident had occurred to the Overseas Recipient and whether such incident was timely and effectively handled, whether the Overseas Recipient has received any request to provide Personal Information to the public authority of the country or region where it is located and how the Overseas Recipient has responded to such request;

   (2) the Personal Information protection policies and regulations of the country or region where the Overseas Recipient is located, including the following elements:

      i. the existing Personal Information protection laws, regulations and generally applicable standards of the country or region;

ii. the regional or global organizations of Personal Information protection that the country or region accedes to, and binding international commitments made by the country or region; and

iii. the mechanisms for Personal Information protection implemented in the country or region, such as whether there are supervision and enforcement authorities and relevant judicial authorities responsible for protecting Personal Information.

(3) the Overseas Recipient's security management system and technical capabilities.

3. The Overseas Recipient warrants that it has used its best efforts to provide the Personal Information Handler with the necessary relevant information for the assessment under Article 4.2.

4. The Parties shall keep a record of any such assessment carried out under Article 4.2 as well as the assessment results.

5. Where the Overseas Recipient is unable to perform this Contract due to any change in the policies and regulations on Personal Information protection of the country or region where the Overseas Recipient is located (including any change of laws or mandatory measures in the country or region where the Overseas Recipient is located), the Overseas Recipient shall notify the Personal Information Handler immediately after being aware of the aforesaid change.

6. If the Overseas Recipient receives a request for provision of Personal Information under this Contract from a governmental authority or judicial authority in the country or region where the Overseas Recipient is located, it shall promptly notify the Personal Information Handler.

Article 5 Rights of the Personal Information Subject

The Parties agree that the Personal Information Subject shall be entitled to the following rights as a third-party beneficiary under this Contract.

1. The Personal Information Subject, in accordance with Relevant Laws and Regulations, has the right to know and to make decisions on the handling of the Personal Information, the right to restrict or refuse handling of the Personal Information Subject's Personal Information by others, the right to request access to, copy, correct, supplement or delete the Personal Information, and the right to request others to explain the rules for the handling of the Personal Information Subject's Personal Information.

2. When the Personal Information Subject requests to exercise the above-mentioned rights regarding their Personal Information that has been transferred overseas, the Personal Information Subject may request the Personal Information Handler to take appropriate measures for the realization of those rights, or directly make the request to the Overseas Recipient. If the Personal Information Handler is unable to realize those rights, it shall notify the Overseas Recipient and request the Overseas Recipient to assist in the realization.

3. The Overseas Recipient shall, as notified by the Personal Information Handler or requested by the Personal Information Subject, realize the rights that the Personal Information Subject is entitled to within a reasonable period and in accordance with the Relevant Laws and Regulations.

   The Overseas Recipient shall inform the Personal Information Subject about the relevant information which shall be true, accurate and complete, in an obvious way and using clear and understandable language.

4. If the Overseas Recipient intends to refuse the request of the Personal Information Subject, it shall inform the Personal Information Subject the reasons of the refusal, as well as the channels for the Personal Information Subject to raise complaints with the relevant Regulatory Authority and seek judicial remedies.

5. The Personal Information Subject, as a third-party beneficiary to this Contract, has the right to claim against one or both, the Personal Information Handler and the Overseas Recipient, in accordance with this Contract and require them to perform the following clauses under this Contract relating to the rights of the Personal Information Subject:

   (1) Article 2, except for Articles 2.5, 2.6 and 2.7;
   (2) Article 3, except for Articles 3.7(2) and 3.7(4), 3.9, 3.11, 3.12 and 3.13;
   (3) Article 4, except for Articles 4.5 and 4.6;
   (4) Article 5;
   (5) Article 6;
   (6) Article 8.2 and 8.3; and
   (7) Article 9.5.

   The above agreement shall not affect the rights and interests of the Personal Information Subject in accordance with the Personal Information Protection Law of the People's Republic of China.

Article 6 Remedies

1. The Overseas Recipient shall identify a contact person who is authorized to respond to enquiries or complaints concerning the handling of Personal Information, and it shall promptly deal with any enquiries or complaints from the Personal Information Subject. The Overseas Recipient shall notify the Personal Information Handler of the contact information and shall inform the Personal Information Subject of the contact information in a manner which is easy to understand, by separate notice or announcement on its website. To be specific: The contact person who is authorized to respond to enquiries or complaints concerning the handling of Personal Information is the Data Protection Officer of the Overseas Recipient, that can be contacted over the phone number and email address published on the website of the Overseas Recipient. For more details, see Appendix "CAC", that will be or is filed with the local CAC.

2. If a dispute arises between either Party and the Personal Information Subject with respect to the performance of this Contract, such Party shall notify the other Party and the Parties shall cooperate to resolve the dispute.

3. If the dispute cannot be resolved amicably and the Personal Information Subject exercises the rights as a third-party beneficiary in accordance with Article 5, the Overseas Recipient shall accept that the Personal Information Subject may safeguard his/her rights through either of the following means:

   (1) lodging a complaint with the Regulatory Authority; and
   (2) bringing a lawsuit to the court specified in Article 6.5.

4. The Parties agree that when the Personal Information Subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, if the Personal Information

Subject chooses to apply the Relevant Laws and Regulations of the People's Republic of China, such choice shall prevail.

5. The parties agree that if the Personal Information Subject exercises the rights as a third-party beneficiary with respect to a dispute under this Contract, the Personal Information Subject may file a lawsuit with a competent court in accordance with the Civil Procedure Law of the People's Republic of China.

6. The Parties agree that the choices made by the Personal Information Subject to safeguard his/her rights will not impair the rights of the Personal Information Subject to seek remedies in accordance with other laws and regulations.

Article 7 Termination of the Contract

1. If the Overseas Recipient breaches the obligations specified in this Contract or the Overseas Recipient is unable to perform this Contract due to a change in the policies and regulations on Personal Information protection in the Overseas Recipient's country or region (including amendment to the laws or adoption of compulsory measures in the Overseas Recipient's country or region), the Personal Information Handler may suspend the provision of Personal Information to the Overseas Recipient until the breach is corrected or the Contract is terminated.

2. In case of any of the following circumstances, the Personal Information Handler shall be entitled to terminate this Contract and notify the Regulatory Authority where necessary:

   (1) where the Personal Information Handler has suspended the provision of Personal Information to the Overseas Recipient for more than one month in accordance with Article 7.1;

   (2) the Overseas Recipient's compliance with this Contract will violate the laws and regulations of its own country or region;

   (3) the Overseas Recipient seriously or persistently breaches the obligations under this Contract;

   (4) the Overseas Recipient or the Personal Information Handler have breached this Contract pursuant to a final decision of a competent court or the regulatory body supervising the Overseas Recipient; and

   The Overseas Recipient may also terminate this Contract in case of sub-paragraph (1), (2) or (4) of above.

3. The Contract may be terminated upon mutual agreement by the Parties, provided that such termination shall not exempt the Parties from the obligations of protecting Personal Information during the handling of the Personal Information.

4. If the Contract is terminated, the Overseas Recipient shall promptly return or delete the Personal Information (including all back-up copies) received hereunder and provide the Personal Information Handler with a written statement. If it is technically difficult to delete the Personal Information, any handling of the Personal Information, other than the storage and taking necessary security protection measures, shall be ceased.

Article 8 Liability for Breach of the Contract

1. Each Party shall be liable to the other Party for any damage as a result of its breach of this Contract.

2. Each Party shall bear civil liabilities to the Personal Information Subject if its breach of this Contract infringes the rights of the Personal Information Subject, without prejudice to the administrative, criminal or other legal liabilities that shall be assumed by the Personal Information Handler under the Relevant Laws and Regulations.

3. The Parties shall assume joint and several liability in accordance with the law. The Personal Information Subject shall have the right to request each Party or the Parties to assume liability. When the liability assumed by one Party exceeds the liability such Party shall be assumed, it shall have the right to claim against the other Party accordingly.

Article 9 Miscellaneous

1. If this Contract conflicts with any other legal documents existing between the Parties, the provisions of this Contract shall prevail.

2. The formation, validity, performance and interpretation of this Contract and any dispute between the Parties arising from this Contract shall be governed by the Relevant Laws and Regulations of the People's Republic of China.

3. All notices shall be promptly transmitted or posted by electronic mail, cable, telex, facsimile (confirmation copy sent by airmail), or registered airmail to (specified address in the Main Agreement or such other address as may be substituted for such address by written notice). Receipt of any notice under this Contract shall be deemed to have been received seven days after its postmark-date in the case of registered airmail and three working days after dispatch in the case of e-mail, cable, telex or facsimile transmission.

4. Any dispute arising from this Contract between the Parties, the Personal Information Handler and the Overseas Recipient, as well as a claim by either Party against the other for recovery of compensation already paid to the Personal Information Subject, shall be resolved by the Parties through negotiation; if such negotiation fails, either Party may adopt any of the following methods to resolve the dispute (check the box for the chosen arbitration institution, if arbitration is required):

   (1) Arbitration. The dispute shall be submitted to:

   ☐ China International Economic and Trade Arbitration Commission
   ☐ China Maritime Arbitration Commission
   ☐ Beijing Arbitration Commission (Beijing International Arbitration Center)
   ☐ Shanghai International Arbitration Center
   X Other arbitration institutions that are members of the Convention on the Recognition and Enforcement of Overseas Arbitral Awards

   The arbitration shall be conducted in Munich, Germany (the place of arbitration) in accordance with its arbitration rules then in force.

   (2) Litigation. Submit the dispute to a Chinese court with jurisdiction in accordance with the applicable laws.

5. This Contract shall be interpreted in accordance with Relevant Laws and Regulations and shall not be interpreted in a manner inconsistent with the rights and obligations set forth in Relevant Laws and Regulations.

6. This Contract shall be executed in two originals, and the Parties, the Personal Information Handler and the Overseas Recipient, shall each hold one original(s), with equal legal effect.

   This contract is signed or concluded online (implemented as terms and conditions and is and original and valid without signature).

Personal Information Handler: Authorized Person, that signed the Main Agreement

Date: Date of Main Agreement

Overseas Recipient: Authorized Person, that signed the Main Agreement

Date: Date of Main Agreement

Appendix I

Description of the Outbound Cross-border Transfer of Personal Information

The details of the outbound cross-border transfer of Personal Information under this Contract are as follows:

1. Purpose of handling: see APPENDIX D – DESCRIPTION OF THE PROCESSING OR THE TRANSFER

2. Method of handling: published as “Nature of (sub-) processing” in APPENDIX D – DESCRIPTION OF THE PROCESSING OR THE TRANSFER

3. The scale of Personal Information to be transferred overseas: Processing and transfer on a small scale. For more details, see Appendix "CAC", that will be or is filed with the local CAC.

4. Type of Personal Information to be transferred overseas (please refer to the *Information Security Technologies - Personal Information Security Specifications (GB/T 35273)* and relevant standards):

   Personal Information (3.1 in GB/T 35273-2020)
   PI Subject (3.3 in GB/T 35273-2020)
   PI Controller (3.4 in GB/T 35273-2020)
   Explicit consent (3.6 in GB/T 35273-2020)
   Consent (3.7 in GB/T 35273-2020)
   Personalized display (3.16 in GB/T 35273-2020)
   Business function (3.17 in GB/T 35273-2020)

For more details, see Appendix "CAC", that will be or is filed with the local CAC.

5. Type of Sensitive Personal Information to be transferred abroad (please refer to the *Information Security Technologies - Personal Information Security Specifications (GB/T 35273)* and relevant standards, if applicable): None.

6. The Overseas Recipient transfers Personal Information only to the following third parties outside the People's Republic of China (if applicable): N/A.

7. Method of transfer: Online Transfer.

8. Retention period after the cross-border transfer:

   From date of Main Agreement to Date of Termination of Main Agreement (which cannot be determined yet).

9. Storage location after the outbound cross-border transfer: Office und legal entity address of Overseas Recipient, or its sub-processors storage locations.

10. Other matters (to be filled in as appropriate): None.

Appendix II

Other Terms as Agreed by the Parties (If Necessary): None.

C. Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China) (Contract Language: Englisch)

Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China)

This Data Processing Agreement and National Joint Controllership Agreement to comply with PIPL (People's Republic of China) (**Agreement**) is concluded on the same date as the Services Agreement (as defined below) and is concluded by and between

(1) the **Personal Information Handler**, named with its Company details as a Party in the Services Agreement (as defined below), and

(2) the **Entrusted Person**, named with its Company details as a Party in the Services Agreement (as defined below).

(together the **Parties**)

1. Preamble

1.1 The Entrusted Person is a provider of professional services (**Services**) and/or provides its Services as a Joint-Controller and is based in the People's Republic of China. The Personal Information Handler is also based in the People's Republic of China. The Parties entered into an agreement which describes the Services provided by the Entrusted Person acting on behalf of the Personal Information Handler, or acting jointly with the Personal Information Handler, in more detail (**Services Agreement**).

1.2 The Parties have agreed to enter into this Agreement in relation to the Processing of Personal Information by the Entrusted Person, or jointly by the Entrusted Person and the Personal Information Handler, in the course of providing the Services. The terms of this Agreement are intended to apply in addition to and not in substitution of the terms of the Services Agreement.

1.3 This Agreement applies to all activities involving the Handling of Personal Information of natural persons within the borders of the People's Republic of China.

2. Definitions and interpretation

2.1 **PIPL** means the Personal Information Protection Law of the People's Republic of China, passed at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021, that entered into force on November 1, 2021, as amended or superseded from time to time. The legal definitions from Article 73 PIPL shall apply.

2.2 **Personal Information** means all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons, not including information after anonymization Handling.

2.3 **Personal Information Handling** includes Personal Information collection, storage, use, processing, transmission, provision, disclosure, deletion, etc.

2.4 **Sensitive Personal Information** means Personal Information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security, including information on biometric characteristics, religious beliefs, specially-designated status, medical health, financial accounts, individual location tracking, etc., as well as the Personal Information of minors under the age of 14.

2.5 **Data Protection Officer** means the Personal Information Protection Officer.

2.6 **Joint-Controller** means an Entrusted Person that qualifies as a Second PI Handler that jointly decides with the Personal Information Handler on the Personal Information Handling purposes and Handling methods.

2.7 **Data Protection Legislation** means the Personal Information Protection Law of the People's Republic of China as well as any regulation adopted, published, administered, implemented, or enforced by the Government of the People's Republic of China, as amended or superseded from time to time, and any related case-law.

3. General Obligations

3.1 Each Party shall comply with all applicable requirements of Data Protection Legislation. This Clause is in addition to, and does not relieve any Party from complying with, a Party's obligations under Data Protection Legislation.

3.2 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, without prejudice to the generality of this Clause, the Personal Information Handler will ensure that it has all necessary Consents and notices in place to enable the lawful transfer of the Personal Information to the Entrusted Person in connection with the performance of its obligations under the Services Agreement.

3.3 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, to the extent within the Personal Information Handler's control having regard to the Entrusted Person's obligations under the Services Agreement, the Personal Information Handler shall be responsible for the accuracy and quality of the Personal Information transferred to the Entrusted Person.

3.4 If the Entrusted Person is Handling Personal Information on behalf of the Personal Information Handler, the Entrusted Person shall have an ongoing obligation throughout the duration of the Services Agreement to identify and report to the Personal Information Handler best practice techniques relating to the Handling of Personal Information and the emergence of new and evolving technologies which could improve the availability, confidentiality and/or integrity of the Handling of Personal Information.

4. Sub-Handlers

4.1 If the Handling involves more than one Entrusted Person (**Sub-Handler**), the Handling must be made in accordance with a contract or written agreement whereby their obligations, responsibilities and roles related to the Handling are clearly defined.

4.2 The Personal Information Handler hereby authorizes the Entrusted Person to appoint Sub-Handlers (General Written Authorization). The Entrusted Person shall name all its Sub-Handlers to the Personal Information Handler prior to initiation of Handling.

4.3 With respect to each Sub-Handler appointed by the Entrusted Person under General Written Authorization, the Entrusted Person shall (a) undertake appropriate due diligence prior to the Handling of Personal Information by such Sub-Handler to ensure that it is capable of providing the level of protection for Personal Information required by the terms of the Services Agreement and this Agreement, and (b) enter into a written Agreement with the Sub-Handler incorporating terms which are substantially similar (and no less onerous) than those set out in this Agreement and which meet the requirements stipulated by PIPL.

4.4 In regard to the Agreement between the Personal Information Handler and the Entrusted Person, the Entrusted Person remain fully liable to the Personal Information Handler for all acts or omissions of its Sub-Handlers as though they were its own.

4.5 To the extent that the Entrusted Person has already appointed any Sub-Handlers prior to the Handling of any Personal Information under this Agreement, the Entrusted Person shall ensure that its obligations under this Section are met.

4.6 Where the Entrusted Person proposes any changes concerning the addition or replacement of any Sub-Handler, it shall notify the Personal Information Handler in writing as soon as reasonably practicable prior to implementing such change specifying (a) the name of any Sub-Handler which it proposes to add or replace, and (b) the Handling activity or activities affected by the proposed change, and (c) the reasons for the proposed change, and (d) the proposed date for implementation of the change.

4.7 If within thirty (30) days of receipt of a notice the Personal Information Handler (acting reasonably and in good faith) notifies the Entrusted Person in writing of any objections to the proposed change, the Parties shall use their respective reasonable endeavors to resolve the Personal Information Handler's objections. Where such resolution cannot be agreed within thirty (30) days of the Entrusted Person's receipt of the Personal Information Handler's objections (or such longer period as the Parties may agree in writing) the Personal Information Handler may, notwithstanding the terms of the Services Agreement, serve written notice on the Entrusted Person to terminate the Services Agreement (to the extent that the provision of the Services are or would be affected by the proposed change).

4.8 The Entrusted Person shall, upon the Personal Information Handler's request, provide the Personal Information Handler with copies of any Agreements between the Entrusted Person and its Sub-Handlers (which may be redacted to remove information which is confidential to the Entrusted Person and/or its Sub-Handlers and which is not relevant to the terms of this Agreement).

5. Obligations of the Entrusted Person (Art. 5, 6, 7, 8, 9, and 10 PIPL)

5.1 The Entrusted Person shall observe the principles of legality, propriety, necessity, and sincerity for Personal Information Handling. The Entrusted Person shall not Handle Personal Information in misleading, swindling, coercive, or other such ways.

5.2 The Entrusted Person shall Handle Personal Information only for clear and reasonable purposes, that shall be directly related to the Handling purpose, using methods with the smallest influence on individual rights and interests.

5.3 The Entrusted Person shall limit the collection of Personal Information to the smallest scope for realizing the Handling purpose, and not collect Personal Information excessive.

5.4 The Entrusted Person shall observe the principles of openness and transparency in the Handling of Personal Information, disclose the rules for Handling Personal Information and clearly indicate the purpose, method, and scope of Handling.

5.5 The Entrusted Person shall ensure the quality of Personal Information and avoid adverse effects on individual rights and interests from inaccurate or incomplete Personal Information.

5.6 The Entrusted Person shall bear full responsibility for its own Personal Information Handling activities and adopt all necessary measures to safeguard the security of the Personal Information it Handles. The Parties agreed on the required technical and organizational measures and procedures in APPENDIX E – TECHNICAL AND ORGANISATIONAL MEASURES.

5.7 The Entrusted Person shall not illegally collect, use, process, or transmit other persons' Personal Information, or illegally sell, buy, provide, or disclose other persons' Personal Information, or engage in Personal Information Handling activities harming national security or the public interest.

6. Consent and Legal Grounds (Art. 13, 14, 15, and 16 PIPL)

6.1 In principle, the Entrusted Person shall Handle Personal Information with the individual's consent.

6.2 However, the Entrusted Person may Handle Personal Information without the individual's consent in cases (1) where necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts, or (2) where necessary to fulfill statutory duties and responsibilities or statutory obligations, or (3) where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions, or (4) Handling Personal Information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest, or (5) when Handling Personal Information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of PIPL, or (6) in other circumstances provided in laws and administrative regulations.

6.3 Where Personal Information is Handled by the Entrusted Person based on the individual's consent, said consent shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Where laws or administrative regulations provide that separate consent or written consent shall be obtained to Handle Personal Information, those provisions are to be followed by the Entrusted Person.

6.4 Where the Entrusted Person changes the purpose of Personal Information Handling, the Handling method, or the categories of Handled Personal Information, the Entrusted Person shall obtain the individual's consent again.

6.5 Where Personal Information is Handled by the Entrusted Person based on the individual's consent, the Entrusted Person shall inform individuals about their right to rescind their consent. The Entrusted Person shall provide a convenient way to withdraw consent.

6.6 The Entrusted Person shall not refuse to provide products or services on the basis that an individual does not consent to the Handling of its Personal Information or rescinds its consent, except where Handling Personal Information is necessary for the provision of products or services.

7. Transparency towards and Notifications of Individuals (Art. 17 and 18 PIPL)

7.1 The Entrusted Person shall, before Handling Personal Information, explicitly notify individuals truthfully, accurately, and fully, using clear and easily understood language, namely about (1) the name or personal name and contact method of the Entrusted Person, and (2) the purpose of Personal Information Handling and the Handling methods, the categories of Handled Personal Information, and the retention period, and (3) methods and procedures for individuals to exercise the rights provided by PIPL, and (4) other items that laws or administrative regulations provide shall be notified. Where the Entrusted Person Handles Personal Information exclusively for the Personal Information Handler, the Entrusted Person shall, before Handling Personal Information, explicitly notify and inform individuals by means of the Transparency Document that was published on the website of the Personal Information Handler.

7.2 Where a change occurs in the matters provided in the previous paragraph, individuals shall be notified by the Entrusted Person about the change.

7.3 Where the Entrusted Person notify the matters as provided under Section 7.1 through the method of formulating Personal Information Handling rules, the Handling rules shall be made public disclosed and convenient to read and store.

7.4 The Entrusted Person may not notify individuals about the items provided in Section 7.1 under circumstances where laws or administrative regulations provide that confidentiality shall be preserved or notification is not necessary.

7.5 Under emergency circumstances, where it is impossible to notify individuals in a timely manner in order to protect natural persons' lives, health, and the security of their property, the Entrusted Person shall notify them after the conclusion of the emergency circumstances.

8. Retention (Art. 19 PIPL)

8.1 The Entrusted Person shall, except where laws or administrative regulations provide otherwise, use the shortest period necessary to realize the purpose of the Personal Information Handling as retention period.

9. Rights and Obligations of each Party if the Parties act as Joint-Controllers (Art. 20 PIPL)

9.1 This Section 9 shall apply only if the Personal Information Handler and the Entrusted Person act jointly as Joint-Controllers. The Clauses of Section 9 of this Agreement shall supersede any conflicting Clauses in other Sections of this Agreement regarding to both Joint-Controllers.

9.2 This Agreement does not influence an individual's rights to demand any of the Joint-Controllers to perform under PIPL provisions.

9.3 Where the Joint-Controllers harm Personal Information rights and interests, resulting in damages, they bear joint liability according to the law.

9.4 The Joint-Controllers determined the scope, subject, purpose and nature of the Handling, the type of Personal Information and categories of individuals in the Services Agreement and/or in APPENDIX D – DESCRIPTION OF THE PROCESSING OR THE TRANSFER.

9.5 The Joint-Controllers shall jointly ensure compliance with Data Protection Legislation when Handling Personal Information. Both controllers are equally responsible for the legality and lawfulness of joint Handling.

9.6 The Personal Information Handler undertakes to provide the individuals with all information regarding their rights under PIPL. The Personal Information Handler acts as the contact point for individuals.

9.7 The Joint-Controllers shall bear joint responsibility for Personal Information Handling activities and adopt all necessary measures to safeguard the security of the Personal Information they Handle jointly. The Parties agreed on the technical and organizational measures and procedures in APPENDIX E – TECHNICAL AND ORGANISATIONAL MEASURES.

9.8 The Joint-Controllers shall jointly appoint only Sub-Handlers which adopted necessary measures to safeguard the security of the Personal Information they Handle and comply with PIPL.

9.9 Each Joint-Controller shall appoint a Data Protection Officer. Both Data Protection Officers shall act jointly in good faith.

9.10 Where one of the Joint-Controllers provides a third party with Personal Information, that Joint-Controller shall notify individuals about the name or personal name of the recipient, their contact method, the Handling purpose, Handling method, and Personal Information categories, and obtain separate consent from the individuals.

9.11 Where one of the Joint-Controllers provides a third party with Personal Information, that third party shall Handle Personal Information within the scope of Handling purposes, Handling methods, Personal Information categories, etc. and when the third party is changing the original Handling purpose or Handling methods, that third party shall inform and obtain the individual's consent again.

10. General Obligations of the Entrusted Person (Art. 21 PIPL)

10.1 Where the Personal Information Handler entrust the Handling of Personal Information, it shall conclude an agreement with the Entrusted Person on the purpose for entrusted Handling, the time limit, the Handling method, categories of Personal Information, protection measures, as

well as the rights and duties of both sides, etc., and conduct supervision of the Personal Information Handling activities of the Entrusted Person.

10.2 The time limit of Handling of Personal Information by the Entrusted Person is the duration of the Services Agreement. The protection measures are agreed on with APPENDIX E – TECHNICAL AND ORGANISATIONAL MEASURES.

10.3 The Personal Information Handler published a “List of (sub) processors, recipients in third countries and international organizations” on its website. In this document, the “Purpose for entrusted Handling” is published as “Subject matter of (sub-) processing”, the “Handling method” is published as “Nature of (sub-) processing”, and the “Categories of Personal Information” are published as “Categories of Personal Data”.

10.4 The Personal Information Handler is granted the right to conduct supervision of the Personal Information Handling activities of the Entrusted Person.

10.5 The Entrusted Person shall Handle Personal Information exclusively according to this Agreement. The Entrusted Person shall not Handle Personal Information for Handling purposes or in Handling methods, etc., in excess of this Agreement.

10.6 If this Agreement does not take effect, is void, has been cancelled, or has been terminated, the Entrusted Person shall return the Personal Information to the Personal Information Handler or delete it, and may not retain it.

11. Mergers, separations, dissolution, declaration of bankruptcy, and other such reasons (Art. 22 PIPL)

11.1 The Entrusted Person shall not transfer any Personal Information Handled on behalf or for the Personal Information Handler due to mergers, separations, dissolution, declaration of bankruptcy, and other such reasons. Wherever such reason may occur, the Personal Information Handler is to be informed and shall decide on the transfer of Personal Information, the return of the Personal Information to the Personal Information Handler or the deletion of the Personal Information.

12. Notifications where Personal Information Handlers provide other Personal Information Handlers with the Personal Information they Handle (Art. 23 PIPL)

12.1 Where the Entrusted Person provide other Personal Information Handlers with the Personal Information it Handles, the Entrusted person shall notify individuals about the name or personal name of the recipient, their contact method, the Handling purpose, Handling method, and Personal Information categories, and obtain separate consent from the individual.

12.2 Where the Entrusted Person provide other Personal Information Handlers with the Personal Information it Handles, the Entrusted person shall make sure by means of a contract that all recipients that Handle Personal Information within the above-mentioned scope of Handling purposes, Handling methods, Personal Information categories, etc. and where recipients change the original Handling purpose or Handling methods, the Entrusted Person shall make sure by means of a contract, that the recipients obtain the individual’s consent again.

13. Automated Decision-Making (Art. 24 PIPL)

13.1 The Entrusted Person shall not use any methods for or engage with any automated decision-making regarding the Personal Information that is Handled for or on behalf of the Personal Information Handler.

14. Non Disclosure of Personal Information (Art. 25 PIPL)

14.1 The Entrusted Person shall not disclose any Personal Information Handled on behalf of the Personal Information Handler to third parties. Sub-Handlers are not considered to be third parties.

15. Major influence on individual rights and interests (Art. 27 PIPL)

15.1 Where the Entrusted Person Handles Personal Information that has been disclosed by the persons themselves or was otherwise lawfully disclosed, except where the person clearly refuses, and that may have a major influence on individual rights and interests, the Entrusted Person shall obtain personal consent in accordance with the provisions of PIPL.

16. Sensitive Personal Information (Art. 28, 29, 30, 31, and 32 PIPL)

16.1 In general, the Entrusted Person shall not Handle Sensitive Personal Information on behalf of the Personal Information Handler. However, if the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, it may do so only where there is a specific purpose and a need to fulfill, and under circumstances of strict protection measures.

16.2 If the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall obtain the individual's separate consent. Where laws or administrative regulations provide that written consent shall be obtained for Handling Sensitive Personal Information, those provisions are to be followed by the Entrusted Person.

16.3 If the Entrusted Person would Handle Sensitive Personal Information in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall, in addition to the items set out in Article 17, Paragraph 1, of PIPL, also notify individuals of the necessity and influence on the individual's rights and interests of Handling the Sensitive Personal Information, except where PIPL provides that it is permitted not to notify the individuals.

16.4 In general, the Entrusted Person shall not Handle Personal Information of minors under the age of 14 on behalf of the Personal Information Handler. However, if the Entrusted Person would Handle Personal Information of minors under the age of 14 in exceptional circumstances on behalf of the Personal Information Handler, the Entrusted Person shall obtain the consent of the parent or other guardian of the minor. Where the Entrusted Person Handle the Personal Information of minors under the age of 14, the Entrusted Person shall formulate specialized Personal Information Handling rules.

16.5 Where laws or administrative regulations provide that relevant administrative licenses shall be obtained or other restrictions apply to the Handling of Sensitive Personal Information, those provisions are to be followed by the Entrusted Person.

17. Cross-Border Provision of Personal Information (Art. 38, 39, 40, 41, 42 and 43 PIPL)

17.1 Where the Entrusted Person, on behalf of the Personal Information Handler, truly need to provide Personal Information outside the borders of the People's Republic of China for business or other such requirements, the Entrusted Person shall meet all requirements of PIPL.

17.2 In particular, in such case, the Entrusted Person shall meet one of the following conditions: (1) passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of PIPL, or (2) undergoing Personal Information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department, or (3) concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides, or (4) meet other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.

17.3 Where treaties or international agreements that the People's Republic of China has concluded or acceded to contain relevant provisions such as conditions on providing personal data outside the borders of the People's Republic of China, those provisions may be carried out by the Entrusted Person.

17.4 The Entrusted Person shall adopt necessary measures to ensure that foreign receiving parties' Personal Information Handling activities reach the standard of Personal Information protection provided in PIPL.

17.5 Where the Entrusted Person provide Personal Information outside of the borders of the People's Republic of China, the Entrusted Person shall notify the individual about the foreign receiving side's name or personal name, contact method, Handling purpose, Handling methods, and Personal Information categories, as well as ways or procedures for individuals to exercise the rights provided in PIPL with the foreign receiving side, and other such matters, and obtain individuals' separate consent.

17.6 If the Entrusted Person is a Critical information infrastructure operator that is Handling Personal Information and reaches the quantities provided by the State cybersecurity and informatization department the Entrusted Person shall store Personal Information collected and produced within the borders of the People's Republic of China domestically. Where the Entrusted Person need to provide it abroad, the Entrusted Person shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cybersecurity and informatization department provisions permit that security assessment not be conducted, those provisions are to be followed by the Entrusted Person.

17.7 Competent authorities of the People's Republic of China, according to relevant laws and treaties or international agreements that the People's Republic of China has concluded or acceded to, or according to the principle of equality and mutual benefit, are to Handle foreign judicial or law enforcement authorities' requests regarding the provision of Personal Information stored domestically. Without the approval of the competent authorities of the People's Republic of China, the Entrusted Person may not provide Personal Information stored within the mainland territory of the People's Republic of China to foreign judicial or law enforcement agencies.

17.8 The Entrusted Person shall observe the lists of the State cybersecurity and informatization department that contain foreign organizations or individuals with limitations or prohibitions regarding the provision of personal information to them and shall under no circumstances transfer or provide Personal Information to any foreign organization or individual that is named or included on such lists.

17.9 Where the People's Republic of China has adopted reciprocal measures against any country or region on the basis of actual circumstances, based on Art. 43 PIPL, the Entrusted Person shall comply with any such decision, and where required, without undue delay cease and desist any transfer to the respective country or region.

18. Individuals' Rights in Personal Information Handling Activities (Art. 44, 45, 46, 47, 48, 49, and 50 PIPL)

18.1 The Entrusted Person shall comply with its own obligations under Art. 44, 45, 46, 47, 48, 49, and 50 PIPL and inform the Personal Information Handler, with undue delay, fully about any individual that has contacted the Entrusted Person regarding any Rights in Personal Information Handling Activities relating to any Personal Information Handled on behalf of the Personal Information Handler.

18.2 Where the Entrusted Person Handles Personal Information on behalf of the Personal Information Handler, the Entrusted Person shall, before Handling Personal Information, inform individuals about their Rights in Personal Information Handling Activities regarding the Personal Information Handler by means of the Transparency Document published on the website of the Personal Information Handler.

19. Other Duties of the Entrusted Person (Art. 51, 52, 53, 54, 55, 56, 57, 58 and 59 PIPL)

19.1 The Entrusted Person shall, on the basis of the Personal Information Handling purpose, Handling methods, Personal Information categories, as well as the influence on individuals' rights and interests, possibly existing security risks, etc., adopt at least the following measures to ensure Personal Information Handling conforms to the provisions of laws and administrative regulations, and prevent unauthorized access as well as Personal Information leaks, distortion, or loss: (1) formulate internal management structures and operating rules, and (2) implement categorized management of Personal Information, and (3) adopt corresponding technical security measures such as encryption, de-identification, etc., and (4) reasonably determine operational limits for Personal Information Handling, and regularly conducting security education and training for employees, and (5) formulate and organize the implementation of Personal Information security incident response plans, and (6) take other measures provided in laws or administrative regulations.

19.2 If the Entrusted Person has reached the quantities provided by the State cybersecurity and informatization department, it shall appoint a Personal Information Protection Officer, to be responsible for supervising Personal Information Handling activities as well as adopted protection measures, etc., and shall disclose the methods of contacting the Personal Information Protection Officer, and report the personal names of the Officer and contact methods to the departments fulfilling Personal Information protection duties and responsibilities.

19.3 If the Entrusted Person engages a Personal Information Handler outside the borders of the People's Republic of China, the Entrusted Person shall make sure that the foreign Personal Information Handler has dedicated an entity or appointed a representative within the borders of

the People's Republic of China that is responsible for matters related to the Personal Information which it Handles, and that the name of the relevant entity or the personal name of the representative and contact method, etc., was reported to the departments fulfilling personal information protection duties and responsibilities.

19.4 The Entrusted Person shall regularly engage in audits of their Personal Information Handling and compliance with laws and administrative regulations.

19.5 When one of the following circumstances is present, the Entrusted Person shall conduct a Personal Information Protection Impact Assessment in advance, and record the Handling situation: (1) Handling Sensitive Personal Information, or (2) Using Personal Information to conduct automated decision-making, or (3) Entrusting Personal Information Handling, providing Personal Information to other Personal Information Handlers, or disclosing Personal Information, or (4) Providing Personal Information abroad, or (5) other Personal Information Handling activities with a major influence on individuals.

19.6 The Entrusted Person shall include the following content in the Personal Information Protection Impact Assessment: (1) whether or not the Personal Information Handling purpose, Handling method, etc., are lawful, legitimate, and necessary, and (2) the influence on individuals' rights and interests, and the security risks, and (3) whether protective measures undertaken are legal, effective, and suitable to the degree of risk. The Entrusted Person shall preserve the Personal Information Protection Impact Assessment Reports and Handling status records for at least three years.

19.7 Where a Personal Information leak, distortion, or loss occurs or might have occurred, the Entrusted Person shall immediately adopt remedial measures, and notify the Personal Information Handler to allow him to notify the departments fulfilling Personal Information protection duties and responsibilities and the individuals. The notification shall include the following items (1) the information categories, causes, and possible harm caused by the leak, distortion, or loss that occurred or might have occurred, and (2) the remedial measures taken by the Personal Information Handler and measures individuals can adopt to mitigate harm, and (3) the contact method of the Entrusted Person.

19.8 If the Entrusted Person is providing important Internet platform services, that have a large number of users, and its business models are complex, the Entrusted Person shall fulfill the obligations in Art. 58 PIPL.

19.9 The Entrusted Persons shall, according to the provisions of PIPL and relevant laws and administrative regulations, take necessary measures to safeguard the security of the Personal Information it Handles, and assist the Personal Information Handler in fulfilling its obligations provided in PIPL.

20. Legal Liability (Art. 66 PIPL)

20.1 Where the Entrusted Person has Handled Personal Information in violation of PIPL or Personal Information is Handled by the Entrusted Person without fulfilling Personal Information protection duties in accordance with the provisions of PIPL, and the Entrusted Person acted on behalf of the Personal Information Handler, the Personal Information Handler is entitled to order correction, and order the provisional suspension or termination of service provision of the application programs unlawfully Handling Personal Information.

21. Compensation for infringements (Art. 69 PIPL)

21.1 Where the Entrusted Person Handled Personal Information, and such operation is infringing Personal Information rights and interests and results in harm, and the Entrusted Person cannot prove they are not at fault, the Entrusted Person shall bear compensation and take responsibility for the infringement. Responsibility to compensate for infringement shall be determined according to the resulting loss to the individual or the Personal Information Handler's resulting benefits. Where the loss to the individual and the Personal Information Handler's benefits are difficult to determine, a court may determine compensation according to practical conditions.

D. DESCRIPTION OF THE PROCESSING OR THE TRANSFER

Categories of data subjects / personal information subjects whose personal information is processed or transferred:

Customers, potential customers, employees, business partners, suppliers.

Categories of personal data / personal information processed or transferred:

Customer data, data of potential customers, employee data, data of business partners, supplier data.

Sensitive data processed or transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Sensitive data / sensitive personal information processed or transferred:

None.

Applied restrictions or safeguards:

None, because no sensitive data is processed or transferred.

Frequency of transfer:

The data is transferred on a continuous basis as long as the Main-Agreement is in force.

Nature of the processing:

See Main-Agreement, the following processing could occur: collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, otherwise making available, alignment, combination, restriction, erasure, destruction.

Purpose(s) for which the personal data / personal information is processed on behalf of the controller or Purpose(s) of the data transfer and further processing:

See Main-Agreement.

Duration of the processing:

Duration of the Main-Agreement.

The period for which the personal information will be retained, or, if that is not possible, the criteria used to determine that period

The criteria for determining the retention period is resulting from the main contract and statutory retention periods.

For processing by or transfer to (sub-) processors, also specify subject matter, nature and duration of the processing

Subject matter of (sub-) processing: SEE APPENDIX D

Nature of (sub-) processing: SEE APPENDIX D

Duration of (sub-) processing: SEE APPENDIX D

E. TECHNICAL AND ORGANISATIONAL MEASURES

The technical and organizational security measures mentioned as follows are the minimum required from you, and are also fulfilled by us. If you have not implemented these technical and organizational security measures, please inform us immediately. Furthermore, you shall send us a list of all additional technical and organizational security measures taken by you, if any.

1. Measures of pseudonymization and encryption of personal information

Pseudonymisation of personal information that are no longer needed in plain text
Encryption of websites (SSL)
Encryption of e-mail (TLS 1.2 or 1.3)

2. Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

Confidentiality agreements with employees
NDAs with third parties
Data Protection agreements with employees
Firewall
Anti-Virus
Regular backups

3. Measures for ensuring the ability to restore the availability and access to personal information in a timely manner in the event of a physical or technical incident

Regular backups of the whole system
Regular test of backup and recovery
Regular training of IT staff

4. Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

In-house checks
Regular review of processes by IT
Regular audits (e.g. by the DPO)

5. Measures for user identification and authorisation

Authentication with username / password
Regular checks of authorisations

Password guideline
Limitation of the number of administrators
Management of rights by system administrator

6. Measures for the protection of data during transmission

Use of encryption technologies
Logging of activities and events
Encryption of email (TIS 1.2 or 1.3)
Use of company internal / restricted drives

7. Measures for the protection of data during storage

Logging of actions and events
Limitation of the number of administrator's
Firewall

8. Measures for ensuring physical security of locations at which personal information are processed

Manual locking system
Security locks
Key control

9. Measures for ensuring events logging

Logging activated on application level
Regular manual checks of logs

10. Measures for ensuring system configuration, including default configuration

Configuration change control process
Data protection by default is observed
Configuration only by system administrator
Regular training of IT staff

11. Measures for internal IT and IT security governance and management

IT security policy
Training of employees on data security

IT team with clear roles and responsibilities

12. Measures for certification/assurance of processes and products

Clear overview of the provisions applicable to the provided products/services/processes
Regular internal and/or external audits
Assignment of audit responsibilities to certified experts

13. Measures for ensuring data minimization

Identification of the purpose of processing
Assessment of a link between processing and purpose
Identification of the applicable retention periods for each data category
Secure erasure of the data after expiration of the retention period

14. Measures for ensuring data quality

Logging of entry and modification of data
Assignment of rights for data entry
Traceability of entry, modification of data by individual user names (not user groups)

15. Measures for ensuring limited data retention

Regular training on retention periods
Regular audit and assessment of retained data

16. Measures for ensuring accountability

Provision of training / awareness rising
Regular controls and checks
Appropriate policies on data protection
Conclusion of SCCs

17. Measures for allowing data portability and ensuring erasure

Personal information is stored in a structured format
Monitoring of legal deadline ensured
Observation of retention periods
Establishment of data portability process
Proper handling of data subject requests

Secure data erasure and data carrier destruction ensured by contracting with Notebook12 GmbH & Co. KG, Fraunhoferring 3, 85238 Petershausen, Germany, email: info@notebook12.com

18. **For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter**

Standard Contractual Clauses (SCCs) are signed or agreed on
Contractually agreed on effective control rights
Contractually agreed on provision of assistance to the controller