数据处理附录

最新更新于 2025 年 10 月 22 日

鉴于

本《数据处理附录》（以下简称 "协议"）补充并基于客户（以下简称 "数据控制方"）与适用的 BIPO 实体（以下简称 "数据处理者"）之间签订的合同（以下简称 "主合同"），用于在主合同项下提供产品和/或服务时处理个人数据。

根据主合同，数据处理者向数据控制者提供以下一项或多项服务和/或软件即服务平台： 全球薪资外包 (GPO) 服务、名义雇主 (EoR) 服务、全球签证服务、承包商服务、BIPO HRMS 平台、Butter 平台和其他相关 BIPO 平台。

数据主体是指通过与个人相关的信息（以下简称 "个人数据 "或 "数据"），如姓名或身份证号码，可以直接或间接识别的任何个人。在本协议中，数据主体可能包括 BIPO 客户的潜在、现任和前任员工，以及员工家属等相关人员。

本协议将于主合同生效日（"生效日"）生效。本协议中未定义的所有以大写字母标明的术语具有主合同中规定的含义。数据控制方和数据处理者合称 "双方"。

双方同意如下：

1. 适用范围和生效

1.1 数据处理者应代表数据控制者并在主合同相关条款，本协议及其指示下处理个人数据，以履行其在主合同下的履约义务。个人数据在附件 1 中描述。

1.2 数据处理的性质、范围和目的，数据处理本身和数据主体群体见附件 1。

1.3 如果数据处理者认为数据控制者的指示违反了数据保护法，它应通知数据控制者。在这种情况下，数据处理者应有权暂停执行该指示，并且在数据控制者发布有关处理个人资料的新的合法指示之前，不对数据控制者承担未能履行主合同规定的适用服务的责任。

2. 数据控制者的义务及权利

2.1 数据控制者应负责遵守适用于其使用平台和服务、处理个人数据的所有数据保护法律，并负责向数据处理器发出指示，将个人数据转移给数据处理器，保护数据主体的权利，包括提供任何必要的通知并获得任何必要的同意和授权。如果第三方基于对其数据的处理而向数据处理者提出索赔，数据控制者应在第一次提出要求时就所有这些索赔向数据处理者作出赔偿。

2.2 数据控制者应对以下情况负全部责任 (i) 个人数据的准确性、质量和合法性，以及数据控制者获得披露或以其他方式提供给数据处理者的个人数据的方式；(ii) 确保数据控制者有权向数据处理者披露或以其他方式提供个人数据进行处理

2.3 如果数据控制者发现数据处理者根据本协议或其指示处理数据时有任何错误或违规行为，应立即全面通知数据处理者。

3. 数据处理者的责任

3.1 数据处理者应按照主合同、本协议的规定，并按照数据控制者的书面指示处理数据。未经授权无权向第三方披露数据，但不适用于以下情况：(i)根据本协议和主合同的规定，(ii)由数据控制人书面要求，或(iii)由法定或法律要求的。在(iii)项的情况下，数据处理者应在适用法律允许的范围内，提前通知数据控制者，并与数据控制者协调。

3.2 在监督机构在合理和必要的范围内进行检查时，只要这些检查涉及到数据处理者的数据处理，数据处理者应支持数据控制员。它应向数据控制者提供后者所需的信息，以证明其在处理方面遵守了适用的数据保护法的要求。

3.3 考虑到数据处理的性质和可获得的信息，数据处理者还应根据要求支持数据控制者遵守数据控制者的以下义务：

3.3.1 确保个人数据处理的安全性、

3.3.2 向监管机构和数据主体通报个人数据违规情况、

3.3.3 如果有必要，进行数据保护影响评估，只要数据处理者的数据处理受到影响、

3.3.4 如有必要，在数据处理者的数据处理受到影响的情况下，与数据保护机构进行必要的事先磋商。

3.4 如果数据处理者意识到在其为数据控制者处理的数据范围内有违反数据保护法的情况，应在没有不当延迟的情况下通知数据控制者。

3.5 数据处理者应责成受雇于处理数据的人员以保密方式处理数据。

3.6 数据处理者可根据第 3.2 和 3.3 节的合作服务，按照数据处理者当时的通行价格要求合理的报酬。但是，如果是由于数据处理者的过错造成的违规，则不适用第 3.3.2 条规定。

4. 跨境数据传输

4.1 在个人数据跨境传输的情况下，数据控制者和数据处理者应采取必要的技术和组织措施，以确保此类传输以适当的保障措施进行，并符合适用的数据保护法规。

4.2 如果个人数据受 GDPR 约束，且数据被转移到欧洲经济区以外的非适当国家，根据 GDPR 第 V 章，为确保对数据主体的适当保护水平，将使用欧盟标准合同条款。这些条款作为附件 4 纳入本协议，具体如下：：

4.2.1 如果数据控制方是出口方，数据处理者是进口方，双方同意使用模块二；

4.2.2 如果数据处理器是出口方，而数据控制方是进口方，双方同意使用模块四。

5. 技术组织措施

5.1 数据处理者应在数据处理开始前采取附件 2 中规定的技术和组织措施。

5.2 这些技术和组织措施受制于技术进步和进一步发展。在这方面，数据处理者可以实施替代的、适当的措施。改变应被记录下来，并且应根据要求向数据控制者提供文件。任何重大变化都应以书面形式通知数据控制者。在发生重大变化的情况下，附件 2 应作相应更新。

6. 控制

6.1 数据控制者应在数据处理者开始处理数据之前，并在此后定期审查根据附件 2 实施的技术和组织措施，并应记录各自的结果，且自行承担费用。数据控制者也应有权在需要的范围内与数据处理者协商进行审计。调查通知应提前沟通，并应在数据处理者的工作时间内进行。数据控制者应考虑到数据处理者的操作流程。

6.2 数据处理者承诺根据要求向数据控制者提供进行全面审查所需的信息并提供相关证据。实施了适当措施的证据也可以通过提交当前的测试证书以及独立审计员（审计员、审计、数据保护官员、IT 安全部门等）的重新报告来提供。在这种情况下，数据控制者应不进行现场检查。

6.3 数据处理者应在必要时为数据控制员提供支持，以达到审计的目的。数据处理者可以要求为其进行审计的努力提供合理的报酬。

7. 分包关系

7.1 数据处理者可以在数据处理者面建立分包关系。承包商及其各自的活动领域应列于主合同。在签署主合同时，数据控制者应被视为已经确认上述关系数据处理者接受。

7.2 数据处理者应将分包商的任何预期变化或新增加的分包商通知数据控制者。

7.3 数据处理者应将本协议中规定的义务，包括技术和组织措施的保证，转交给其分包商。这些技术和组织措施应符合适用的数据保护法的要求。

7.4 如果分包商没有法定的保密或不披露义务，数据处理者应与他们签订保密或不披露协议。

8. 数据主体的权利

8.1 数据主体的权利应向数据控制者主张。

8.2 只要数据主体向数据处理者主张其权利，数据处理者应及时将该请求转交给数据控制者。

8.3 只要数据主体向数据控制者主张其权利，如果数据控制者在没有数据处理者的支持下无法实现其要求，则数据处理者应以适当的技术和组织措施支持数据控制者在必要范围内实现这些要求。

8.4 数据处理者可以根据本协议第 8.3 条的规定，要求为支持活动提供合理报酬。

8.5 如果一方将相关数据对象的个人资料披露给第三方，该方应确保其约束该第三方按照适用的《数据保护法》规定的可比标准来处理、统筹和保护个人资料。

9. 数据保护官（DPO）

如果任何一方对数据保护有任何疑问/澄清，或需要就数据泄露问题进行沟通，请提供以下数据保护专员联系方式：

数据处理者： dpo@biposervice.com

数据控制方：（由客户填写）

10. 责任

10.1 数据处理者应对违反数据保护法规和本协议规定的行为根据主合同中相关条款向数据控制者负责。

10.2 如果由于数据控制者违反了数据保护法而导致第三方对数据处理者提出索赔，数据控制者应在第一时间要求对数据处理者的损失进行赔偿。此外，数据控制者应在必要的范围内协助数据处理者进行法律辩护，并应向数据处理者偿还由该事件引起的所有损失，包括法律辩护的合理费用。

11. 合同期限及数据归还或者删除

11.1 本协议应在双方签署后生效，并应无限期地运行。本协议应在数据处理者进行数据处理时所依据的主要合同终止时结束，而不需要单独终止本协议。

11.2 如有必要，双方应商定适当的过渡性安排，以确保基础处理业务的正常进行，如有必要，也可在主合同结束后进行。

11.3 在数据控制者的请求下，或者在本协议终止或到期时，数据处理者应在客户确认后，销毁并证明已删除，或将其控制或拥有的所有个人数据归还给客户。该要求不适用于数据处理者根据任何适用法律而被要求保留部分或全部个人数据的情况，此时数据处理者应隔离和保护个人数据，不再进行进一步处理，除非法律要求。

11.4 作为根据订单进行适当数据处理的证据的文件，应由数据处理者根据相关的保留期在协议期满后保留。这也适用于其他有法律保留义务的文件（例如，根据税法）。

12. 其他

12.1 如果数据处理者的数据因扣押或查封、破产或组成程序或第三方的其他事件或措施而受到威胁，数据处理者应毫不拖延地通知数据控制者。数据处理者应立即通知所有在这种情况下负责的人，数据的主权和所有权完全由数据控制者作为"责任方 "来承担。

12.2 如果双方之间的服务关系的实际形式发生变化，双方应相应修改附件，并通过相互协商进行交换。在双方签署修正后的附件后，该附件应生效并取代以前适用的附件。

12.3 主合同中数据控制者和数据处理者之间的服务协议中关于管辖法律、仲裁和/或法律地点的规定适用于本协议。

12.4 对协议的修改或补充必须以书面形式进行。这应比照适用于上述书面形式要求的任何修改或取消。

12.5 如果本协议的个别条款无效或变得无效，协议的其余部分的有效性不受影响。无效的条款应被尽可能接近无效条款内容的有效条款重新取代。这一点也应适用于存在漏洞的情况。

附件 1：数据、数据主体、数据处理和数据处理的目的

附件 2：技术和组织措施

附件 3：批准的分包商和分包商的授权领域

附件 4：标准合同条款（如适用）

附件 1.A：合同方列表

1. 自控制者传输至处理者:

数据出口方	**数据进口方**
名称: 客户	名称: BIPO
地址/邮箱：如在主合同中提供	地址/邮箱：如在主合同中提供
联系人名称，职位及联系方式：如在主合同中提供	联系人名称，职位及联系方式：如在主合同中提供
转移相关行为：见附件 1.B	转移相关行为：见附件 1.B
角色: 控制者	角色：处理者

2. 从处理者传输至控制者（欧洲 BIPO 公司作为第三国控制者/客户的处理者）:

数据出口方	**数据进口方**
名称: BIPO	名称: 客户
地址/邮箱：如在主合同中提供	地址/邮箱：如在主合同中提供
联系人名称，职位及联系方式：如在主合同中提供	联系人名称，职位及联系方式：如在主合同中提供
转移相关行为：见附件 1.B	转移相关行为：见附件 1.B
角色: 处理者	角色：控制者

附件 1.B：处理的描述

数据处理者应处理以下数据主体的个人数据:

数据对象可能包含	（由客户修改） 潜在的、现任的和前雇员，以及雇员的家庭成员等相关人员。 名义雇主员工 承包商，与 BIPO 签订服务协议，执行 BIPO 客户指定服务的独立承包商。
个人资料的类别	潜在的、现任的和前雇员数据 （此列表并非详尽无遗——可根据需要由定制客户端进行编辑。） 人力资源及福利处理所必需的员工数据，包括姓名、联系信息（家庭及工作地址、家庭及工作电话号码、手机号码、家庭及工作电子邮件地址）、婚姻状况、出生日期、性别、民族、公民身份、宗教信仰、国籍、签证详细信息、医疗证明、员工职位名称、业务职称、履历、职级或代码、工作地点、所属公司、上级主管、成本中心、工作时间安排、雇佣状态（全职或兼职、长期或临时）、薪酬及相关信息、薪资信息、银行账户信息、津贴、奖金、考勤记录、绩效评估与考核、休假申请、报销申请与支付、紧急联系人信息、工作经历信息、培训与发展信息。 相关人员/家属的信息 相关人员的数据，如家属或受益人的姓名和联系信息（包括家庭住址、家庭和工作电话、手机号码、出生日期、性别、紧急联系人、受益人信息、被抚养人信息）。
处理的频率	持续
BIPO系统位置	（BIPO将更新） （举例：HRMS-新加坡， Butter-法兰克福）
集成系统	（由客户填写） （目的、 输入与输出传输详情 及客户系统位置）
数据处理涉及的国家/地区范围	如服务协议中所述
处理的性质&目的（传输相关行为）	如服务协议中所述
处理的目的	（客户更新）
处理的时间	-服务协议的时长

保留	-个人数据将根据需要予以保留，以满足收集数据的目的，如提供服务和产品，以及 BIPO 为满足其业务要求、履行法律义务、解决争议、保护其资产和执行其权利和协议所需的目的。

附件 1.C：主管的监督机构

根据第 12 条确定主管监管机构：主管监管机构为（国家/地区名称）的（监管机构名称），或任何后续接任的、负责监督（国家/地区名称）数据保护法律实施与执行的主管机构。

依据第 12 条所确定的主管监管机构，负责确保数据输出方的合规性。

附件 2：技术和组织措施

数据处理者已采取技术和组织措施，以确保根据本数据处理附录开展的处理活动符合适用的数据保护规定。

数据处理者特别采取了安全措施，以保证保护标准足以应对系统的保密性、完整性、可用性和复原力方面的风险，同时考虑到数据泄露的可能性以及由此可能对自然人的权利和自由造成的风险的严重性。

技术和组织措施应始终根据技术进步和发展进行监测和更新，以保持或提高数据保护标准。

以下是 BIPO SaaS 应用采用的安全措施：

1. 确保处理系统和服务的持续保密性、完整性、可用性和可复原的措施

- 保密协议；
- 信息安全政策和程序；
- 输入验证和数据库完整性约束
- 备份和恢复测试程序；
- 高度可用和容错的备份存储；
- 防病毒/防火墙保护，安全补丁管理；
- 系统可用性和例外情况的监控和检测；
- 定期的用户访问审查；

2. 加密和保护个人数据的措施：

- 静止状态下的加密和运输中的加密；
- 使用数据掩码来掩盖个人信息，以达到排除故障的目的；

3. 用户识别和授权的措施：

- 关于用户账户和用户访问请求的内部政策和程序；
- 用户访问控制，用户认证；
- 基于 "需要知道 "而授予访问权；
- 对用户活动和数据变化的记录；

4. 储存期间保护数据的措施：

- 休息时的加密；
- 访问控制；
- 对来自不同客户的数据进行逻辑分割；
- 分离环境（生产/测试/开发）；

5. 确保在发生灾难时能够及时恢复服务的措施：

- 业务连续性计划；
- 灾难恢复程序；
- 事故应对计划；

6. 确保事件日志记录的措施

- 启用系统审计日志功能
- 采用安全的日志存储与保留机制
- 实施访问控制，限制日志仅限授权人员访问

7. 确保系统配置（包括默认配置）的措施

- 实施安全默认配置
- 默认启用加密功能

8. 流程与产品的认证/保证措施

- ISO27001 认证及 SOC1、SOC2 Type II 鉴证报告
- 第三方供应商保证机制
- 年度渗透测试

9. 确保数据有限保留的措施

- 约定保留期限的合同条款与内部政策
- 实施安全的数据删除方法

10. 确保问责制的措施

- 定期审查数据保护政策与流程
- 将法律要求纳入政策与实践
- 实施隐私保护默认设计
- 执行定期审计

11. 实现数据可携性与确保删除的措施

- 支持数据导出的系统功能
- 数据彻底清除功能

12. 确保技术及组织措施有效性的措施

- 物理环境安全策略
- 门禁控制系统
- 监控设施（闭路电视、报警系统）
- 机柜上锁、关键设备的安全存放定位

附件 3：批准的分包处理者和分包处理者的授权领域

BIPO 作为处理者时使用分包处理者。特定客户的分包处理者列表将在与客户签订的主服务协议的附录部分提及。

双方为支持项目的执行而与第三方共同使用的辅助服务，如电信服务、云托管服务、票务平台等，不视为本条款所指的分包处理者服务。

附件 4：标准合同条款

第一部分

第 1 条

目的和范围

(a) 该标准合同条款的目的是为了确保个人数据向第三国转移中，遵守欧洲议会和欧盟理事会 2016 年 4 月 27 日 2016/679 号条例（通用数据保护条例）规定的与处理个人数据和该等数据的自由流动有关的保护自然人的要求 1。

(b) 双方：

(i) 附件 I.A.列举的转移个人数据的自然人或法人、公共机构、代理机构或其他实体（以下简称"实体"）（统称为"数据出口方"），和

(ii) 附件 I.A.列举的从数据出口方接收个人数据的位于第三国的实体，通过另一方实体直接或间接地接收数据方也为合同一方（统称为"数据进口方"）。

就标准合同条款（以下简称"条款"）协商一致。

(c) 该等条款适用于附件 I.B.中规定的个人数据的转移。

(d) 包含附件的该等条款的附录为该等条款不可分割的一部分。

第 2 条

效力和条款恒定

(a) 该等条款规定了包括可执行的数据主体权利和有效的法律救济措施在内的适当的保障措施，其依据为根据欧盟 2016/679 号条例第 46 条第（1）项和第 46 条第（2）（c）项规定，就数据从控制者向处理者和/或处理者向处理者传输而言，依据为欧盟 2016/679 号条例第 28 条第（7）项规定的标准合同条款，前提为除根据附录选择适当的模块或者添加或更新信息外不做其他修改。在不直接或间接地与该等条款相矛盾或损害数据主体的基本权利或自由前提下，双方可以将标准合同条款中规定的该等条款纳入其他合同中和/或增加其他条款或额外的保障措施。

(b) 该等条款不得对数据出口方根据欧盟 2016/679 号条例所承担的义务造成不利影响。

第 3 条

第三方受益人

(a) 数据主体可以作为第三方受益人对数据出口方和/或数据进口方援引并执行该等条款，除非：

(i) 第 1 条、第 2 条、第 3 条、第 6 条、第 7 条；

(ii) 第 8 条 -模块 2：第 8.1 条第（b）项，第 8.9 条第（a）、（c）、（d）和（e）项；模块 4：第 8.1 条（b）和第 8.3 条（b）；

(iii) 第 9 条 - 模块 2：第 9 条第（a）、（c）、（d）和（e）项；

(iv) 第 12 条 - 模块 1：第 12 条第（a）和（d）项；模块 2：第 12 条第（a）、（d）和（f）项；

(v) 第 13 条；

(vi) 第 15.1 条第（c）、（d）和（e）项；

(vii) 第 16 条第（e）项；

(viii) 第 18 条 - 模块 2：第 18 条第（a）和（b）项；模块 4：第 18 条。.

(b) （a）项不影响数据主体在欧盟 2016/679 号条例下的权利。

第 4 条

解释

(a) 如果该等条款使用了在欧盟 2016/679 号条例中定义的术语，该等术语应具有与该条例相同的含义。

(b) 该等条款应根据欧盟 2016/679 号条例的规定进行理解和解释。

(c) 该等条款的解释不得与欧盟 2016/679 号条例规定的权利和义务相冲突。

第 5 条

效力层级

如果该等条款与双方在就该等条款达成一致时存在的或随后签订的相关协议的约定相冲突，以该等条款为准。

第 6 条

转移说明

转移的具体事宜，尤其是转移的个人数据种类和转移目的，在附件 I.B.列明。

第 7 条-可选

对接条款

(a) 经该等条款双方同意，非该等条款一方的实体可在任何时候，通过填写附录和签署附件 I.A.，作为数据出口方或数据进口方加入该等条款。

(b) 完成附录且签署附件 I.A 后，加入实体应成为该等条款的一方，并根据其在附件 I.A.中确定的内容享有数据出口方或数据进口方的权利和义务。

(c) 加入的实体在成为一方之前，不享有该等条款规定的任何权利或义务。

第二部分-双方的义务

第 8 条

数据保护保障措施

数据出口方保证，其已尽到合理努力，确定数据进口方能够通过采取适当的技术和组织措施，履行其在该等条款项下的义务。

模块二：从控制者转移到处理者

8.1 说明

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

(b) 如果数据进口方无法遵守这些指示，应立即通知数据出口方。

8.2 目的限制

数据进口方应仅为附件 I.B.中规定的特定转让目的处理个人数据，除非根据数据出口方的进一步指示。

8.3 透明度

经请求，数据出口方应免费向数据主体提供一份该等条款的副本，包括双方所填写的附录。在保护商业秘密或其他保密信息（包括附件 II 中的措施和个人数据）的必要范围内，数据出口方可在分享副本之前编辑附录的部分文本，但如数据主体无法理解其内容或行使其权利时，还应提供有效的摘要。经请求，双方应在不泄露经编辑的信息的情况下，尽可能向数据主体提供编辑的理由。该等条款不影响数据出口方根据欧盟第 2016/679 号条例第 13 和 14 条所承担的义务。

8.4 准确性

如果数据进口方意识到它所接收的个人数据不准确或已经过时，不得无故迟延通知数据出口方。在该情形下，数据进口方应当配合数据出口方对数据进行更正或者删除。

8.5 处理期限和数据的删除或归还

数据进口方的处理应仅在附件 I.B.中规定的期限内进行。在提供处理服务结束后，数据进口方应根据数据出口方的选择，删除代表数据出口方处理的所有个人数据，并向数据出口方证明它已这样做，或向数据出口方归还代表其处理的所有个人数据并删除现有副本。在数据被删除或归还之前，数据进口方应继续确保遵守该等条款。如果适用于数据进口方的当地法律禁止归还或删除个人数据，数据进口方保证它将继续确保遵守该等条款，并且只在当地法律规定的范围内和时间内处理这些数据。这并不影响第 14 条，特别是第 14 条第（e）项对数据进口方的要求，即如果它有理由相信它受到或已经受到不符合第 14 条第（a）项要求的法律或惯例的约束，则在整个合同期内通知数据出口方。

8.6 处理的安全性

(a) 数据进口方，以及在转移过程中的数据出口方，应采取适当的技术和组织措施，以确保个人数据的安全，包括防止安全漏洞导致意外或非法的破坏、丢失、篡改、未经授权的披露或访问（以下简称"个人数据泄露"）。在评估适当的安全水平时，双方应适当考虑技术水平、实施成本、处理的性质、范围、场景和目的以及处理过程中相对于数据主体的风险。如果处理的目的可以通过这种方式实现，双方应特别考虑采用（包括在传输过程中的）加密或假名化。双方应特别考虑采用加密或假名化，包括在转移过程中，如果处理的目的可以通过这种方式实现。在假名化的情况下，在可能的情况下，用于将个人数据归属于特定数据主体的额外信息应保持在数据出口方的排他控制之下。在遵守本段规定的义务时，数据进口方应至少实施附件 II 中规定的技术和组织措施。数据进口方应进行定期检查，以确保这些措施持续提供适当的安全水平。

(b) 数据进口方应仅在执行、管理和监督合同所严格必要的范围内允许其工作人员访问这些数据。应确保被授权处理个人数据的人已承诺保密或负有适当的法定保密义务。

(c) 如果发生涉及数据进口方根据该等条款处理的个人数据泄露事件，数据进口方应采取适当措施处理泄露事件，包括采取措施减轻其可能的不利影响。数据进口方还应在意识到泄露后，不得无故迟延通知数据出口方。该通知应当包含可获得更多信息的联络点的详细信息，对泄露性质的描述（在可能的情况下，包括有关数据主体和个人数据记录的类别和大致数量），可能的后果和为解决数据泄露而采取或建议采取的措施，包括采取措施减轻其可能的不利影响。如果当时无法提供所有信息，初步通知应当包含当时可得的信息，随后在获得进一步信息时，不得无故迟延提供。

(d) 数据进口方应与数据出口方合作并提供协助，使数据出口方能够遵守欧盟 2016/679 号条例规定的义务，特别是通知主管监管部门和受影响的数据主体，需同时考虑到处理的性质和数据进口方所掌握的信息。

8.7 敏感数据

如果转移涉及显示种族或民族血统、政治观点、宗教或哲学信仰或工会会员资格的个人数据、遗传数据或用于唯一识别自然人的生物识别数据、有关健康或个人性生活或性取向的数据、或

与刑事定罪或犯罪有关的数据（以下简称“敏感数据”），数据进口方应根据附件 I.B.中的规定采取特定限制和/或额外保障措施。

8.8 再转移

数据进口方应仅根据数据出口方的书面指示将个人数据披露给第三方。此外，只有在第三方根据适当的模块同意受该等条款约束的情况下，数据才能披露给位于欧盟以外 4 的第三方（与数据进口方在同一国家或在另一个第三国，以下简称“再转移”），或者如果：

(i) 再转移的目标国是根据欧盟 2016/679 号条例第 45 条享受充分性保护决定的国家；；

(ii) 第三方根据欧盟 2016/679 号条例第 46 条或 47 条，以其他方式确保对有关处理的适当保障措施;

(iii) 在特定的行政、监管或司法程序中，为建立、行使或支持权利主张所必需；或者

(iv) 数据进口方的任何再转移都必须遵守该等条款规定的所有其他保障措施，特别是关于目的限制的规定。

数据进口方的任何再转移都必须遵守该等条款规定的所有其他保障措施，特别是关于目的限制的规定。

8.9 文件和合规性

(a) 数据进口方应及时和充分地处理数据出口方提出的与该等条款下的处理有关的询问。

(b) 双方应能证明遵守该等条款。尤其是数据进口方应保留代表数据出口方进行的处理活动的适当文件。

(c) 数据进口方应向数据出口方提供所有必要的信息，以证明遵守该等条款中规定的义务，在合理的时间间隔或有不合规迹象时，应数据出口方的请求，允许并协助对该等条款所涵盖的处理活动进行审计。在决定审查或审计时，数据出口方可以考虑到数据进口方持有的相关认证。

(d) 数据出口方可以自愿选择自行审计，也可以委托独立审计方进行审计。审计可包括对数据进口方的场所或物理设施的检查，在适当的情况下需进行合理通知。

(e) 各方应根据请求向主管监管部门提供（b）和（c）项所述的信息，包括任何审计的结果。

模块四：从处理者转移到控制者

8.1 说明

(a) 数据出口方应仅根据作为控制者的数据进口方的书面指示处理个人数据。

(b) 如果数据出口方无法遵守这些指示，包括如果这些指示违反欧盟 2016/679 号条例或者其他欧盟或成员国数据保护法，应立即通知数据进口方。

(c) 无论是分包处理情形或者就和主管监管部门合作而言，数据进口方应避免采取任何行动，妨碍数据出口方履行欧盟 2016/679 号条例规定的义务。

(d) 在提供处理服务结束后，数据出口方应根据数据进口方的选择，删除代表控制者处理的所有个人数据，并向数据出口方证明它已这样做，或将代表其处理的所有个人数据归还数据进口方并删除现有副本。

8.2 处理的安全性

(a) 双方应采取适当的技术和组织措施确保包括传输过程中的数据安全，防止安全漏洞导致意外或非法的破坏、丢失、篡改、未经授权的披露或访问（以下简称"个人数据泄露"）。在评估适当的安全水平时，双方应适当考虑技术水平、实施成本、处理的性质 7、范围、场景和目的以及处理过程中相对于数据主体的风险。如果处理的目的可以通过这种方式实现，双方应特别考虑采用（包括在传输过程中的）加密或假名化。

(b) 数据出口方应协助数据进口方按照（a）项的规定确保适当水平的数据安全。如果发生与数据出口方根据该等条款处理的个人数据有关的个人数据泄露事件，数据出口方应在意识到这一事件后不得无故迟延通知数据进口方，并协助数据进口方处理该泄露事件。

(c) 数据出口方应确保被授权处理个人数据的人承诺保密或承担适当的法定保密义务。

8.3 文件合规性

(a) 双方应能证明对该等条款的遵守。

(b) 数据出口方应向数据进口方提供所有必要的信息，以证明其遵守该等条款规定的义务，并允许和协助进行审计。

第 9 条

分包处理者的作用

模块二：从控制者转移到处理者

(a) 方案 1：具体的事先授权未经数据出口方事先具体书面授权，数据进口方不得将其根据该等条款代表数据出口方进行的任何处理活动分包给其他处理方。数据进口方应在聘用其他处理方之前至少三十（30）天提交具体授权请求，同时提供必要的信息，以便数据出口方对授权作出决定。已获数据出口方授权的分包处理者名单见附件 III。双方应及时更新附件 III。

方案 2：一般书面授权数据进口方拥有数据出口方的一般授权，可从经同意的清单中聘用分包处理者。数据进口方应至少提前三十（30）天以书面形式明确通知数据出口方通过增加或更换分包处理者对该清单进行的任何预期更改，从而使数据出口方有足够的时间在聘用分包处理者之前反对此类更改。数据进口方应向数据出口方提供必要的信息，使数据出口方能够行使其反对权。

(b) 如果数据进口方聘请分包处理者（代表数据出口方）进行具体的处理活动，它应通过书面合同的方式进行，该合同实质上规定了与数据进口方在该等条款下所受约束相同的数据保护义务，包括数据主体的第三方受益人权利方面。8 双方同意，通过遵守该等条款，数据进口方履行了其在第 8.8 条下的义务。数据进口方应确保分包处理者遵守数据进口方根据该等条款所承担的义务。

(c) 应数据出口方的请求，数据进口方向数据出口方提供与该分包处理者签署的协议及任何后续修订的副本。在保护商业秘密或其他机密信息（包括个人数据）的必要范围内，数据进口方可以在分享副本之前对协议文本进行编辑。

(d) 数据进口方应继续就分包处理者履行其与数据进口方合同项下的义务向数据出口方承担全部责任。数据进口方应将分包处理者未能履行其在该合同下的义务的情况通知数据出口方。

(e) 数据进口方应与分包处理者就第三方受益人条款达成一致，据此，在数据进口方事实上已经消失、在法律上不复存在或已经破产的情况下，数据出口方应有权终止分包处理者合同并指示分包处理者删除或归还个人数据。

第 10 条

数据主体权利

模块二：从控制者转移到处理者

(a) 数据进口方应及时通知数据出口方它从数据主体收到的任何请求。除非得到数据出口方的授权，否则它本身不得对该请求作出回应。

(b) 数据进口方应协助数据出口方履行义务，回应数据主体根据欧盟 2016/679 号条例行使其权利的请求。双方应据此考虑到处理的性质后在附件 II 中规定协助所需的适当的技术和组织措施，以及所需协助的范围和程度。

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

模块四：从处理者转移到控制者

双方应相互协助，回应数据主体基于适用于数据进口方的当地法律提出的询问和请求；就数据出口方在欧盟境内的数据处理，回应数据主体基于欧盟 2016/679 号条例提出的询问和请求。

第 11 条

救济措施

(a) 数据进口方应通过个别通知或在其网站上公告，以透明和易于获知的形式，告知数据主体授权处理投诉的联络点。它应立即处理它从数据主体收到的任何投诉。

[方案：数据进口方同意数据主体在无需承担费用的情况下可向独立的争议解决机构

11 提出申诉。它应以第（a）项规定的方式告知数据主体这种救济措施，而且告知数据主体不要求他们必须使用这种机制，也不要求他们按照特定的顺序寻求救济。]

模块二：从控制者转移到处理者

(b) 如果数据主体与其中一方在遵守该等条款方面出现争议，该方应尽最大努力及时友好地解决问题。双方应相互通知此类争议，并在适当时合作解决这些争议。

(c) 如果数据主体根据第 3 条援引第三方受益权，数据进口方应接受数据主体的决定:

(i) 向其经常居住地或工作地点的成员国的监管机构或根据第 13 条规定的主管监管机构提出投诉;

(ii) 将争端提交给第 18 条意义上的主管法院。.

(d) 双方同意，根据欧盟2016/679号条例第80条第（1）项规定的条件，非营利性机构、组织或协会可代表数据主体行事。

(e) 数据进口方应遵守根据适用的欧盟或成员国法律具有约束力的决定。

(f) 数据进口方同意，数据主体的选择不会损害他/她根据适用法律寻求补救的实质性和程序性权利。

第 12 条

责任

模块四：从处理者转移到控制者

(a) 各方应对其违反任何该等条款而给另一方造成的任何损失承担责任。

(b) 各方应对数据主体承担责任，该方因违反该等条款规定的第三方受益人权利而给数据主体造成任何物质或精神损失，数据主体有权获得补偿。这不影响数据出口方根据欧盟 2016/679 号条例承担的责任。

(c) 如果不只一方应对违反该等条款而给数据主体造成的任何损害承担责任，所有责任方应承担连带责任，数据主体有权在法院对任何一方提起诉讼。

(d) 双方同意，如果一方根据（c）项规定应当承担责任，它应有权向另一方/各方追偿与该另一方/各方对损害的责任相应的那部分赔偿。

(e) 数据进口方的处理者或分包处理者地位不影响其应当承担的责任。

模块二：从控制者转移到处理者

(a) 各方应对其违反任何该等条款而给另一方造成的任何损失承担责任。

(b) 数据进口方应对数据主体承担责任，数据进口方或者其分包处理者因违反该等条款规定的第三方受益人权利而给数据主体造成任何物质或精神损失，数据主体有权获得补偿。

(c) 尽管有（b）项的规定，因数据出口方或数据进口方（或其分包处理者）违反该等条款规定的第三方受益人权利而给数据主体造成任何物质或精神损失，数据出口方应向数据主体承担责任，并且数据主体有权获得赔偿。在数据出口方作为处理者代表控制者时，这不影响根据所适用的欧盟 2016/679 号条例或欧盟 2018/1725 号条例，数据出口方应当承担的责任，也不影响数据控制者应当承担的责任。

(d) 双方同意，如果数据出口方根据（c）项对数据进口方（或其分包处理者）造成的损失应当承担责任，数据出口方有权就数据进口方应当承担的责任损失部分进行追偿。

(e) 如果有一个以上的合同方对违反任何该等条款给数据主体造成的任何损害均应承担责任，所有责任方应承担连带责任，数据主体有权选择任何一方提起司法诉讼。

(f) 双方同意，如果一方根据（e）项被认定为应当承担责任，其有权就其他方应当承担的责任损失部分进行追偿。

(g) 数据进口方不得援引分包处理者的行为来规避责任。

第 13 条

监管

模块二：从控制者转移到处理者

(a) [如果数据出口方设立在欧盟成员国：]如附件 I.C 所示，负责确保数据出口方在数据转移方面遵守欧盟 2016/679 号条例的监管机构应作为主管监管机构。

[如果数据出口方未在欧盟成员国设立，但根据欧盟 2016/679 号条例第 3 条第（2）项属于的适用领域范围，并已根据欧盟 2016/679 号条例第 27 条第（1）项任命了一名代表：] 如附件 I.C 所示，欧盟 2016/679 号条例第 27 条第（1）项所指的代表所在的成员国的监管机构应作为主管监管机构。

[如果数据出口方未在欧盟成员国设立，但根据欧盟 2016/679 号条例第 3 条（2）项属于的适领域范围，但无需根据欧盟 2016/679 号条例第 27 条第（2）项指定代表：] 如附件 I.C 所示，根据该等条款向其提供商品或服务，其个人数据被转移或其行为被监控的数据主体所在的一个成员国的监管部门应作为主管监管部门。

(b) 数据进口方同意在任何旨在确保遵守该等条款的程序中服从主管监管部门的管辖并与之合作。特别是，数据进口方同意回应询问、接收审计和遵守监管部门采取的措施，包括损害赔偿和补偿措施。数据出口方应当就已经采取的必要行动以书面方式向监管部门进行确认。

第三部分 - 当地法律和公共机构访问时的义务

第 14 条

影响遵守该条款的当地法律和惯例

模块二：从控制者转移到处理者

模块四：从处理者转移到控制者 *(欧盟处理者将从第三国控制者那里收集的个人数据与处理者在欧盟收集的个人数据混合起来)*

(a) 双方保证，他们没有理由相信，目的地第三国适用于数据进口方处理个人数据的法律和惯例，包括披露个人数据的任何要求或授权公共当局查阅的措施，会妨碍数据进口方履行该等条款规定的义务。该理解基于该等法律和惯例与该等条款不相抵触，该等法律和惯例本质上应是尊重基本权利和自由的且该等法律和惯例没有超越民主社会为保障欧盟 2016/679 号条例第 23 条第（1）项所列目标之一的必要性和相称性。

(b) 双方声明，在提供（a）项中的保证时，他们特别考虑到了以下因素：

(i) 转移的具体情况，包括处理环节的长度、涉及的行为者的数量和使用的传输渠道；预计再转移情况；接收者的类型；处理的目的；转移的个人数据的种类和格式；发生转移涉及的产业部门；转移数据的存储地点；

(ii) 与特定转让情形相关的目的地第三国的法律和惯例、适用的限制、保障措施，包括那些要求向公共当局披露数据或授权这些当局访问的法律和惯例 12；

(iii) 为补充该等条款规定的保障措施而采取的任何相关的合同、技术或组织保障措施，包括在传输过程中以及在目的地国处理个人数据时采用的措施。.

(c) 数据进口方保证，在进行（b）项规定的评估时，它已尽最大努力向数据出口方提供相关信息，并同意它将继续与数据出口方合作，确保遵守该等条款。

(d) 双方同意将（b）项规定的评估记录在案，并根据请求向主管监管部门提供。

(e) 如果在同意该等条款之后以及在合同期内，数据进口方有理由相信它受到或已经受到不符合（a）项要求的法律或惯例的约束，包括在第三国的法律发生变化或有措施（如披露要求）表明这些法律在实践中的应用不符合（a）项的要求之后，数据进口方同意立即通知数据出口方。

(f) 收到根据（e）发出的通知后，或如果数据出口方有理由相信数据进口方不能再履行其在该等条款下的义务，数据出口方应立即确定数据出口方和/或数据进口方将采取的适当措施（例如，确保安全和保密的技术或组织措施），以应对该等情况。如果数据出口方认为无法确保此类转移的适当保障措施，或者如果主管监管部门指示这样做，数据出口方应暂停数据转移。在这种情况下，数据出口方应有权就涉及该等条款规定的个人数据处理事宜终止合同。如果合同涉及两个以上的合同方，数据出口方只能对相关合同方行使这一终止权，除非双方另有约定。如果合同根据该等条款被终止，则应适用第 16 条第（d）项和第（e）项。

第 15 条

数据进口方在被公共当局访问时的义务

模块二：从控制者转移到处理者

模块四：从处理者转移到控制者 *(欧盟处理者将从第三国控制者那里收到的个人数据与处理者在欧盟收集的个人数据混合起来)*

15.1 通知

(a) 数据进口方同意在以下情况下立即通知数据出口方，并在可能的情况下立即通知数据主体（必要时在数据出口方的帮助下）：

(i) 收到公共当局（包括司法当局）根据目的地国法律提出的具有法律约束力的要求，要求披露根据该等条款转让的个人数据；这种通知应包括关于所要求的个人数据、提出要求的当局、提出要求的法律依据和所提供的答复的信息；或

(ii) 意识到公共当局根据目的地国的法律对根据该等条款转让的个人数据进行任何直接访问；该等通知应包括进口方可获得的所有信息。.

(b) 如果数据进口方根据目的地国的法律被禁止通知数据出口方和/或数据主体，数据进口方同意尽其最大努力获得禁令的豁免，以期尽快传达尽可能多的信息。数据进口方同意记录其最大的努力，以便能够在数据出口方的要求下证明这些努力。

(c) 在目的地国法律允许的情况下，数据进口方同意在合同期内定期向数据出口方提供尽可能多的关于收到的请求的相关信息（特别是请求的数量、请求的数据类型、请求的主管部门、是否对请求提出质疑以及这些质疑的结果等）。[对于模块三：数据出口方应将这些信息转发给控制者]。

(d) 数据进口方同意在合同期内保存（a）至（c）项规定的信息，并根据请求向主管监管部门提供这些信息。

(e) （a）至（c）项不影响数据进口方根据第 14 条（e）条和第 16 条在无法遵守该等条款时立即通知数据出口方的义务。

15.2 对合法性和数据最小化的审查

(a) 数据进口方同意审查披露请求的合法性，特别是它是否持续属于授予提出请求的公共当局的权力范围内，并在经过仔细评估后认为有合理理由认为根据目的地国的法律、所适用的国际法义务和国际礼让原则，该请求是非法的，则对该请求提出质疑。数据进口方应在相同条件下寻求上诉的可能性。在对请求提出质疑时，数据进口方应寻求临时措施，以期在主管司法当局对其案情作出实质性决定之前暂停请求的效力。在根据适用的程序规则要求披露之前，它不应披露所要求的个人数据。这些要求不影响第 14 条第（e）项规定的数据进口方的义务。

(b) 数据进口方同意记录其法律评估和对披露请求的任何质疑，并在目的地国法律允许的范围内，向数据出口方提供这些文件。它还应根据请求向主管监管部门提供该文件。[对于模块三：数据出口方应向控制者提供评估报告。]

(c) 数据进口方同意在回应披露请求时，根据对请求的合理解释，提供允许的最低数量的信息。

第五部分 - 最终条款

第 16 条

无法符合条款及终止

(a) 如果数据进口方因任何原因无法遵守该等条款，应立即通知数据出口方。

(b) 如果数据进口方违反该等条款或无法遵守该等条款，数据出口方应暂停向数据进口方转让个人数据，直到再次确保遵守或终止合同。第 14 条第（f）项不受影响。

(c) 在以下情况下，数据出口方有权就该等条款项下处理个人数据事宜终止合同，如果：

(i) 数据出口方已根据（b）项暂停向数据进口方转移个人数据，而在合理时间（无论如何不超过暂停后 1 个月）内，仍未恢复遵守该等条款；

(ii) 数据进口方严重或持续地违反该等条款；或

(iii) 数据进口方未能遵守主管法院或监管部门关于其在该等条款下的义务的具有约束力的决定。

在该等情况下，它应将这种不遵守规定的情况通知主管监管部门[针对模块三：和控制者]。如果合同涉及两个以上的合同方，除非双方另有约定，否则数据出口方只能对相关合同方行使这一终止权。

(d) [对于模块一、二和三：根据（c）项，在合同终止前已经转移的个人数据，应根据数据出口方的选择立即返还给数据出口方或全部删除。这也应适用于数据的任何副本]。[针对模块四：数据出口方在欧盟收集的、在合同终止前根据（c）项转移的个人数据应立即全部删除，包括其任何副本。] 数据进口方应向数据出口方证明数据的删除。在数据被删除或归还之前，数据进口方应继续确保遵守该等条款。如果适用于数据进口方的当地法律禁止归还或删除转让的个人数据，则数据进口方保证将继续确保遵守该等条款，并仅在当地法律规定的范围内和时间内处理数据。

(e) 在以下情况下，任何一方均可撤销其受该等条款约束的协议：(i) 欧盟委员会根据欧盟 2016/679 号条例第 45 条第（3）项通过一项决定，该决定涉及该等条款适用的个人数据的转移；或(ii) 欧盟 2016/679 号条例成为个人数据被转移至的国家的法律框架的一部分。这不影响根据欧盟 2016/679 号条例适用于有关处理的其他义务。

第 17 条

管辖法律

模块二：从控制者转移到处理者

该等条款应受欧盟成员国之一的法律管辖，前提是该法律允许第三方受益人权利。双方同意这应是（指明成员国）的法律] 双方同意，如果符合第一句话的条件，则以主合同中提到的国家的法律为准，否则以德国法律为准。

模块四：从处理者转移至控制者

该等条款应受允许第三方受益权的国家的法律管辖。双方同意，如果符合第一条的条件，应以主合同中提到的国家的法律为准，否则以德国法律为准。

第 18 条

法院和管辖权的选择

模块二：从控制者转移到处理者

(a) 由该等条款引起的任何争议应由欧盟成员国的法院解决。

(b) 双方同意，这些法院应是德国的法院。

(c) 数据主体也可在其惯常居住地的成员国法院对数据出口方和/或数据进口方提起法律诉讼。

(d) 双方同意接受这些法院的管辖。

模块四：从处理者转移到控制者

由这些条款引起的任何争议应由主合同中提到的国家的法院解决，如果法律不适用，则由德国法院解决。

附件

附件 1

见数据处理附录中附件 1

附件 2 技术和组织性措施，包括确保数据安全的技术和组织性措施

见数据处理附录中附件 2

附件 3 分包处理者列表

见数据处理附录中附件 3