在《数据处理协议》中纳入标准合同条款

最后更新日期：2023年2月22日

本文件由客户与 海菲秀 LLC（“海菲秀”）签订，以纳入标准合同条款（“HF 标准合同条款”）。

鉴于本文件中的共同承诺和约定，双方特此达成如下协议：

**定义**

除非《数据处理协议》中另有定义，本 HF 标准合同条款中使用的下列术语应具有以下规定的含义：

* “《采购协议》”是指构成客户与海菲秀和/或其关联方之间商业交易基础的先前签订的协议。
* “关联公司” 就一方而言，是指由该方控制或与该方处于共同控制下的任何实体，其中控制是指直接或间接拥有该实体 50%（百分之五十）以上的表决权。
* “客户”是指在 海菲秀l 账户信息中指明的提供者（诊所/中心）或在《采购协议》的签名中指明的用户。
* “欧盟数据保护法”是指（a）《欧盟通用数据保护条例》（第2016/679号条例）（GDPR）；（b）《欧盟电子隐私指令》（第002/58/EC号指令）；以及（c）依据或根据以上任何法规制定的任何欧盟成员国法律，包括以上各项法律的修订或替代版本。
* “欧盟 SCC”是指 2021 年 6 月 4 日第 (EU) 2021/914 号决议中规定的标准合同条款。欧洲议会和理事会作出此决议的目的是根据 (EU) 2016/679 号条例规定向第三国传输个人数据所适用的标准合同条款。
* “IDTA”是指信息专员办公室根据 2022 年 3 月 21 日生效的 2018 年 《S119A(1) 数据保护法》B1.0 版发布的欧盟标准合同条款的《国际数据传输附录》。
* “瑞士数据保护法”是指 1992 年颁布至 2022 年 12 月 31 日废止的《瑞士联邦数据保护法》（FADP）；从 2023 年 1 月 1 日起，应适用 2020 年 9 月颁布的《经修订的瑞士联邦数据保护法》（修订版 FADP），包括该法律的修订或替代版本。
* “英国数据保护法”是指《数据保护、隐私和电子通信（修订等）（退出欧盟）条例》（第2019/419号条例），并且由根据欧盟相关法规（2018年《退出欧盟法》第3条）颁布的2018年《数据保护法》和《英国DPA（保留（欧盟）第2016/679号条例》（英国GDPR）进行补充，包括以上法律将来的修订或替代版本。

本 HF 标准合同条款中以粗体字表示但未定义的所有其他术语应当适用《数据处理协议》或《采购协议》中规定的含义。

1. **欧盟标准合同条款**

通过引述将欧盟标准合同条款的板块二（将数据从控制者传输至处理者，其中客户是所传输数据的控制者）和板块三（将数据从处理者传输至处理者，其中客户是所传输数据的处理者）纳入《数据处理协议》，纳入的具体条款详述如下：

1.1. 对接条款。不适用第7条中规定的此选项。

1.2.指示。就第 8.1(b) 条而言，双方同意接受《数据处理协议》中所载的客户的书面指示（包括代表控制者提出的指示），包括与国际数据传输有关的指示。

1.3.关于删除数据的确认声明。根据第8.5条规定，双方同意，客户将向海菲秀 确认声明其已按照海菲秀 的书面要求删除个人数据。

1.4.合规性检查。双方理解，第 8.9 条规定的审核权应按照《数据处理协议》中关于审核的规定执行。

1.5.分包处理者。在第 9(a) 条中，应适用选项 2，客户将根据协议或《数据处理附录》中的条款规定，在分包处理者变更前三十 (30) 天通知客户。

1.6.补救措施。在第11条中，不适用可选的措辞。

1.7.责任。双方同意，客户根据第 12 条对海菲秀 承担的责任应适用《数据处理协议》中包含的责任限制和排除条款。

1.8.法律适用。就第 17 条（选项 1）而言，双方同意欧盟标准合同条款应适用西班牙法律管辖。

1.9.管辖法院和管辖权。就第 18 条第（a）项和第（b）项而言，双方同意因欧盟 SCC引起的任何争议应当由西班牙法院解决。

1.10.附件。欧盟标准合同条款的附件一、附件二和附件三应视为已使用本 HF 标准合同条款附件1中所列的信息填写完成。

1.11.冲突。如果本 HF 标准合同条款的正文或其纳入的《数据处理协议》与标准合同条款之间存在任何冲突或差异，应当以标准合同条款为准。

1. **英国标准合同条款。**

如果根据《数据处理协议》传输至海菲秀的任何个人数据受英国数据保护法管辖并且源自英国，则应视为已签署 IDTA，并且 IDTA 将整合和补充欧盟标准合同如下：

2.1.协议双方。第 1 部分表 1 已使用此 HF 标准合同条款附件 1 中所列的详细信息填写完成。

2.2.标准合同条款、板块和条款。第 1 部分表 2 已使用上述第1条中所列的信息填写完成。

2.3.附件。第 1 部分表 3 中提到的“附件信息”已使用此 HF 标准合同条款附件 1 中所列的信息填写完成。

2.4.终止。客户（作为输入方）可以根据IDTA第19条终止该IDTA。

1. **瑞士标准合同条款。**

如果根据《数据处理协议》传输至海菲秀的任何个人数据受瑞士数据保护法管辖并且源自英国，则应适用欧盟标准合同条款并采用以下修改调整：

3.1.管辖地。“成员国”一词不应被解释为排除瑞士的数据主体根据欧盟标准合同条款第 18(c) 条在瑞士起诉执行其权利的可能性。

3.2.监管机构。根据欧盟标准合同条款第 13 条规定，瑞士联邦数据保护和信息专员有权管辖受瑞士数据保护法约束的个人数据传输。

1. 本 HF 标准合同条款应终止并替换任何先前版本的标准合同条款，而这些先前的条款是本 HF 标准合同条款生效前《数据保护协议》的组成部分。
2. 除本 HF 标准合同条款中另有规定外，《数据保护协议》不受影响，将根据其条款继续完全有效，并且本 HF 标准合同条款应受《采购协议》的条款和条件约束。如果本 HF 标准合同条款与《数据处理协议》或任何先前的修订协议之间存在冲突，应当以本 HF 标准合同条款的规定为准。
3. 本 HF 标准合同条款仅在客户与 海菲秀 LLC 或其关联方或子公司之间先前已签订协议的情况下有效。
4. 本 HF 标准合同条款将在以下时间起生效：（i）将完整签署的文本发送至 dpo@海菲秀.com 并且海菲秀确认收到该签署的文本；（ii）在 HF 标准合同条款被自动视为纳入协议的情况下，从首次将数据传输到 除 EEA、英国、瑞士或充分保护的国家（视情况适用）以外的国家之日起。

双方已于下述最后签名日期正式签署本协议，以昭信守。本 HF 标准合同条款上的这些签名构成对标准合同条款（如适用，包括IDTA 和《瑞士修订协议》）的接受和签署。

附件1

1. 处理详情
2. 相关方名单

|  |  |  |
| --- | --- | --- |
|  | **信息输出方** | **信息输入方** |
| 名称和商号（如果不同） | 客户：是指在 海菲秀 账户信息中指明的提供者（诊所/中心）或在《采购协议》的签名中指明的用户 | 海菲秀 LLC |
| 官方注册号（如果有） （公司编号或类似标识信息） | 用户账户信息或《购买协议》签名中指明的信息 | 201233810062 |
| 地址 | 用户账户信息或《购买协议》签名中指明的信息 | 2165 E. Spring Street,  Long Beach, CA 90806 |
| 联系人的姓名、职务和联系方式： | 用户账户信息或《购买协议》签名中指明的信息 | Ignacio de la Corte，数据保护官（DPO）  dpo@海菲秀.com |
| 与根据欧盟标准合同条款 传输的数据相关的活动 | 详见《数据处理协议》 | 详见《数据处理协议》 |
| 签名和日期 | 签署本 HF 标准合同条款 即视为已签署欧盟标准合同条款 | 签署本 HF 标准合同条款 即视为已签署欧盟标准合同条款 |
| 角色 | 处理者／分包处理者 | 控制者／处理者 |

1. 传输描述

|  |
| --- |
| *传输的个人数据的***数据主体类别** 其个人数据由 海菲秀 处理的客户、消费者和授权用户，目的是提供 海菲秀 账户和设备服务，包括与设备交互。 |
| *传输的***个人数据的类别** 传输的个人数据由客户或代表客户提供，并由 海菲秀 在提供设备服务时处理。  个人数据通常包括：（i）数据主体的联系方式和账户信息，例如全名、电话号码、电子邮件地址、职位和 IP 地址；（ii）护理历史和表现。 |
| **传输的敏感数据（如果适用）**以及适用的限制或保护措施，*该等措施应充分考虑数据的性质和所涉及的风险，例如严格的目的限制、访问限制（包括仅供接受过专门培训的员工访问）、保留访问数据的记录、对后续传输的限制或额外的安全措施* 处理的个人数据将不会包括敏感的个人数据，包括关于种族或族裔出身、政治观点、宗教或哲学信仰、工会会员身份、性生活、政府颁发的身份证号码、信用卡详细信息、PCI 相关敏感数据（包括但不限于磁条和芯片数据、CAV2/CVC2/CVV2/CID4 号码和个人识别号（PIN））、健康或医疗记录和犯罪记录等信息。 |
| **传输频率**（*例如，数据是一次性传输或持续传输*） 在提供或使用设备或服务期间持续传输 |
| **处理的性质** 处理的个人数据可能会涉及以下处理活动：收集、通过传输和查询而披露 |
| **数据传输***和进一步处理*的**目的** 出于《数据处理协议》中所述的目的（“允许的目的”）处理个人数据。 |
| **保留个人数据的期限**，*或者如果无法确定具体期限，则用于确定该期限的标准* 个人数据可能会在 海菲秀 设备服务的合同期限内以及法律要求保留的任何额外期限内处理。 |
| **对于向处理者／分包处理者进行的传输**，*还需指明处理的主题、性质和持续时间* 数据不会传输给分包处理者。 |

1. 主管监管机构

是指根据第 13 条确定的欧盟成员国的主管监管机构。

1. 技术和组织措施，包括确保数据安全的技术和组织措施

在不影响根据《数据处理协议》适用于服务的安全控制措施之前提下，海菲秀 根据 EDPB 的非约束性指南实施以下补充措施：

技术措施

* 海菲秀 使用端到端加密。
* 海菲秀 对传输中的数据和静态数据进行加密。

其他合同措施

* 透明。
* 如有要求，海菲秀 将采取合理的商业努力（尽其所知）提供关于公共主管部门（包括情报领域）具有数据访问权限的信息，以评估目的地国家的法律是否符合《EDPB 欧洲基本保证》。
* 海菲秀 确认声明：（1）其没有构建，且不会故意构建公共主管部门可以用于访问其个人数据或信息系统的后门程序或类似程序；（2）其没有改变，且不会故意改变其流程，以方便公共主管部门访问数据；（3）国家法律或政府政策不要求 海菲秀 创建或维护后门、或为访问个人数据或系统提供便利、或由其持有或交出加密密钥（可能会根据法律发展而变化）。如果 海菲秀 无法遵守与国际传输相关的法律义务和／或合同承诺，因此无法达到“基本同等数据保护水平”的要求标准，海菲秀 将通知客户。
* 具体行动。
* 海菲秀 应当：（i）审查法律请求的合法性，并在合法且适当的情况下对法律请求提出质疑；（ii）如果法律请求不符合 GDPR 第 46 条规定或关于个人数据合法传输的任何其他规定，其将通知公共主管部门（在上述每种情况下，在关于法律请求的适用数据保护法律要求的范围内）。

组织措施

* 透明和问责制。
* 海菲秀 已书面制定相应的政策和程序，用于处理和回应政府或执法部门提出的要求提供客户数据的请求。
* 海菲秀 书面记载并记录从公共主管部门收到的访问请求以及提供的回应，并且可以应要求向客户提供此类信息。
* 海菲秀 提供并定期维护《政府数据请求政策》和《透明度报告》网页，该网页描述了关于政府／执法部门数据请求的政策，并记录了公共主管部门提出请求的数量以及我们的回应，可在 [\*链接\*] 获得。
* 通过和审查内部政策。
* 海菲秀 监控与欧盟/欧洲经济区以外的个人数据跨境传输相关的法律和法规变化，以确保数据继续获得基本同等水平的保护。
* 海菲秀 定期审查内部政策，以评估补充措施的适当性／有效性，并在必要时确定和实施额外或替代解决方案。在适用和适当的情况下，海菲秀 将努力实施任何额外的必要技术、组织和／或合同措施。
* 组织方法和数据最小化措施。
* 海菲秀 已采用组织控制措施遵守问责制原则，包括访问管理控制。
* 海菲秀 实行数据最小化原则，以限制可能遭受未经授权访问的数据量。
* 海菲秀 已采用最佳实践，适当和及时地让数据保护官（DPO）和法务部参与，并向其提供国际个人数据传输相关事宜的信息访问权限。