PayPal

>> 查看所有协议

PayPal卡处理产品数据保护附录

最后更新日期：2021年12月1日

本PayPal卡处理产品数据保护附录（以下简称本“附录”）适用于PayPal集团成员（以下简称“PayPal”）向您，即商家（以下简称“商家”或“您”）提供卡处理、网关和（或）防欺诈保护服务（以下简称“付款服务”）的任何产品、服务或其他产品或服务。本附录不适用于PayPal钱包服务，例如使用PayPal付款或PayPal的延期付款服务。本附录构成商家与PayPal就PayPal向您提供付款服务达成的相关协议（以下简称“《协议》”）的一部分，并通过参考纳入其中。如果本附录的条款与《协议》之间存在任何冲突，则以本附录的条款为准。本附录中使用但未定义的大写术语应具有《协议》中所述的含义。

本附录自以下两者中的较晚日期起生效：（i）《协议》中规定的生效日期，或（ii）就本附录发布的通知或向您发出的通知中所述的生效日期。我们可能会不时修订本附录。除非另有说明，否则修订版从发布至PayPal网站起即刻生效。如果我们所做的变更减少了您应享受的权利或增加了您应承担的责任，我们将在《协议》要求的时间范围内，在PayPal网站的“规则更新”页面上发布相应声明。如果您不同意对本附录的任何变更，您可以停止使用付款服务。

定义

以下术语在本附录中使用时具有以下含义：

“**控制者**”是指*确定处理个人数据的目的和方式的实体，或者，如果该术语（或涉及类似功能的术语）在数据保护法律中有所定义，则“控制者”应具有适用的数据保护法律中规定的含义。*

“**客户**”是指使用付款服务的客户，在本附录中，客户是数据主体。

“**客户数据**”是指（i）客户提供给商家，商家通过使用付款服务转交给PayPal的个人数据；（ii）PayPal在商家使用付款服务的过程中从客户的设备和浏览器中收集的个人数据。

“**数据保护法律**”是指适用于提供付款服务的任何适用的数据保护法律、法规、指令、监管要求和行为守则，包括对其作出的任何修订以及任何相关的法规或文书（例如，《2018年加州消费者隐私法》（加州民法典第1798.100节等）、《通用数据保护条例》（欧盟）2016/679（GDPR）、澳大利亚《1988年隐私法》（联邦法）、《个人信息保护和电子文件法》（加拿大）、《个人数据（隐私）条例》（第486章）（香港）、巴西《通用数据保护法》第13,709/2018号联邦法律和《2012年个人数据保护法》（新加坡））。

“PayPal集团”是指PayPal以及PayPal或其继任者不时直接或间接拥有或控制的所有公司。

“**个人数据**”是指与已识别或可识别的自然人（以下简称“数据主体”）有关的任何信息；可识别的自然人尤其是指通过参照姓名、身份证号码、位置数据、网络识别码等标识符或通过与该自然人的身体、生理、遗传、心理、经济、文化或社会身份有关的一个或多个特定因素可直接或间接识别的自然人。

本附录中所使用的“**流程**”或涉及类似功能的术语应具有适用的数据保护法律中规定的含义。

PayPal作为控制者

PayPal应遵守本附录中有关处理客户数据的适用于控制者的数据保护法律要求（包括但不限于始终实施并维护所有与处理客户数据有关的适当安全措施），不得故意对个人数据做任何或允许做任何可能导致商家违反数据保护法律的事情。PayPal仅应将客户数据传输给签订书面协议的第三方、分处理商或PayPal集团的成员，该协议应包含保护客户数据的条款，而此类条款的保护程度不低于本附录中规定的条款。

处理与付款服务有关的客户数据

双方确认并同意，商家和PayPal是与付款服务有关的所有已处理客户数据的各自独立控制者。因此，PayPal会独立确定处理此类客户数据的目的和方法，而并非与商家共同处理此类客户数据的联合控制者。

双方确认并同意，PayPal可以出于以下有限目的使用、复制并处理客户数据和付款交易数据：

- 在合理必要的情况下向商家及其客户提供和改进付款服务，包括防欺诈保护工具；
- 监控、防止和检测欺诈付款交易，并防止对商家、PayPal和第三方造成伤害；

- 遵守适用于PayPal处理和保留付款数据时需要遵守的法律或监管义务，包括适用的反洗钱和身份验证义务；
- 分析、开发和改进PayPal的产品和服务；
- 内部使用，包括但不限于数据分析和指标；
- 当在汇总中无法识别您的个人或用户客户数据时，汇编和披露客户数据和付款交易数据，包括按地区或行业计算您的平均值；
- 遵守适用的法律要求，并协助执法机构，依法回应其披露信息的请求；以及
- 其告知商家的任何其他目的，只要此类目的符合数据保护法律的规定。

商家对客户的通知

商家应作出商业上合理的努力，（i）在其隐私权保护规则中通知客户，如本附录所述，就处理客户数据而言，PayPal是独立控制者；以及（ii）在商家的隐私权保护规则中加入PayPal隐私政策的链接www.paypal.com。

互助

双方同意在合理必要的范围内相互合作，使另一方可以根据数据保护法律充分履行作为独立控制者的责任。双方同意，在商家收到主体访问请求或客户根据数据保护法律行使其权利的情况下，商家应直接对此类客户的访问请求作出回应。商家还应告知客户，他们可以根据**www.paypal.com**的《隐私政策》中所述的指示，行使其与PayPal的付款服务相关的数据主体权利。此外，如果因任何安全事件，PayPal自行决定必须通知受影响的客户，并且PayPal没有与受影响的客户进行此类通信的必要联系信息，则商家应作出商业上合理的努力，向PayPal提供商家可能拥有的客户信息，以便PayPal遵守数据保护法律下适用的通知受影响客户的义务。

跨境数据传输

双方同意，PayPal可在提供付款处理服务所需的情况下，将根据此《协议》处理的客户数据传输到数据收集地以外的国家或地区。如果PayPal将受本附录保护的客户数据传输到数据收集地的适用监管机构尚未对其做出适当性裁定的司法管辖区，PayPal将确保根据适用的数据保护法律为客户数据传输实施相应的保障措施。例如，出于遵守GDPR的目的，我们依靠主管监管机构批准的有法律约束力的公司规则和其他数据传输机制，将客户个人数据传输给PayPal集团的其他成员。

关于您向PayPal传输位于欧盟、瑞士、欧洲经济区和（或）其成员国或英国境内的客户的数据，我们分别同意：（i）在适用范围内，您对《协议》的签署将被视为签署并接受2021年6月4日通过的欧盟委员会（EU）第2021/914号实施决定，该决定涉及商家作为数据输入方并以控制者的身份根据GDPR向第三国传输个人数据的标准合同条款（以下简称“欧盟传输条款”），并将被视为作为数据输出方签署并接受国务大臣根据2018年《数据保护法》第17C（b）条制定的、在英国目前有效的

法规中规定的标准数据保护条款（以下简称“英国传输条款”）；（ii）在适用范围内，PayPal对《协议》的签署将被视为PayPal作为数据输入方并以控制者的身份签署并接受欧盟传输条款，并将被视为作为数据输入方签署并接受英国传输条款；以及（iii）双方应遵守欧盟传输条款模块1的规定。如果欧盟委员会或英国国务大臣（或其他适用的英国授权机构）分别修订并在此后公布新的欧盟传输条款或英国传输条款（或欧盟委员会或英国国务大臣（或其他适用的英国授权机构）另有其他要求或以其他方式实施）。双方同意，此类新的欧盟传输条款或英国传输条款（如适用）将取代目前的欧盟传输条款或英国传输条款（如适用），并且双方同意采取一切必要措施，使新的欧盟传输条款或英国传输条款（如适用）得以执行。欧盟传输条款（模块1）和英国传输条款将通过引用纳入《协议》，并在此《协议》生效时被视为由双方正式签署，同时须遵守以下详细规定：

A）欧盟传输条款

1. 第17条（适用法律）的选项1适用，卢森堡的法律管辖欧盟条款。
2. 根据第18条（法院和司法管辖权的选择），卢森堡法院将解决因欧盟条款而产生的任何争议；以及
3. 双方同意，欧盟传输条款附录所要求的详细规定载于附件1。

B）英国传输条款

1. 第II（h）（iii）条被纳入《协议》，PayPal对《协议》的签署将被视为PayPal作为数据输入方的必要首肯；
2. 双方同意，英国传输条款附件B所要求的详细规定载于附件1（在适用范围内）。

附件1

欧盟传输条款附录和英国传输条款附件B

A）根据欧盟传输条款和英国传输条款的要求，以下内容适用

附件1.A. 双方列表

数据输出方

- 名称和地址：数据输出方是商家，地址与《协议》中提供的地址一致
- 联系人的姓名、职位和联系方式：与《协议》中提供的一致
- 与根据标准合同条款传输的数据有关的活动：与《协议》中提供的一致
- 签名和日期：请参阅本附录的“跨境传输”部分
- 角色（控制者/处理者）：控制者

数据输入方

- 名称和地址：数据输入方是根据《协议》提供服务的PayPal集团成员，地址与《协议》中提供的地址一致
- 联系人的姓名、职位和联系方式：与《协议》中提供的一致
- 与根据标准合同条款传输的数据有关的活动：与《协议》中提供的一致 签名和日期：请参阅本附录的“跨境传输”部分
- 角色（控制者/处理者）：控制者

附件1.B. 传输说明

数据主体
传输的个人数据涉及以下类别的数据主体:

数据输出方及其客户、员工和其他业务联系人。

传输的个人数据的类别

传输的个人数据可能包括以下类别的数据:

姓名、收费金额、日期/时间、银行账户详情、付款卡详情、CVC代码、邮政编码、国家或地区代码、地址、邮箱地址、传真、电话、网站、过期数据、发货详情、纳税状况、唯一客户标识符、IP地址、位置，以及PayPal根据《协议》收到的任何其他数据。

敏感数据（如适用）和应用的限制或保障措施

传输的个人数据涉及以下类别的敏感数据:

- 不适用，除非商家配置服务以获取此类数据。
- 应用限制和保障措施:
- 不适用，除非商家配置服务以获取此类数据。

处理的性质

- 按照《协议》规定。

传输目的
传输目的如下:

- 根据《协议》履行数据输入方向数据输出方提供的服务。

- 识别正在影响或可能影响数据输入方、数据输出方或数据输入方的其他客户的欺诈活动和风险。
- 遵守适用于数据输入方的法律。
- 遵守本数据保护附录的规定。

个人数据将被保留的期限，或者用于确定该期限的标准（如无法确定该期限）

数据输入方仅在收集数据的相关目的所需的时间范围内保留个人数据（请参阅上述目的）。为确定个人数据的适当保留期限，数据输入方会考虑个人数据的数量、性质和敏感性，未经授权使用或披露个人数据造成伤害的潜在风险，处理个人数据的目的以及此类目的是否可以通过其他方式实现，以及适用的法律、监管、税务、会计或其他要求。

传输至（二级）处理者时，也要说明处理的主题事项、性质和期限

数据输入方可能会与按照数据输入方的指示和代表数据输入方履行服务及职能的第三方服务提供商共享个人数据。例如，这些第三方服务提供商可能会提供《协议》规定的服务内容，例如客户认证、交易处理或客户支持，或者向数据输入方提供某项服务，以支持《协议》规定的服务（例如存储）。在确定由第三方服务提供商进行处理的期限时，数据输入方将应用本附件1.B中规定的上述标准。

附件1.C. 监管机构

根据欧盟传输条款第13（a）条，负责确保数据输出方在数据传输方面遵守欧盟第2016/679号条例的监管机构应作为主管监管机构行事。

附件2. 技术和组织措施，包括确保数据安全的技术和组织措施

1. 假名化、加密和传输过程中的数据保护。

PayPal的规则确保遵守这一原则，并要求使用技术控制措施来防止个人数据泄露风险。PayPal对所有传输中和静止的个人数据都实施加密。我们还采用行业标准的假名化技术，例如在适用的情况下采用标记化来保护个人数据。PayPal拥有全面的规则，规定了当数据在企业内部传输和向外部第三方传输时保护数据的关键义务和流程。

2. 变更管理和业务连续性。

PayPal强大的变更管理流程可确保变更得到适当的计划、批准、执行和审查，从而在整个生命周期内保护数据和系统的持续可用性和可恢复性。公司的业务连续性管

理流程提供了一个框架，旨在建立组织恢复力，构建有效响应的能力，从而保障主要利益相关者的利益。

3. 灾难恢复。

PayPal强大的灾难恢复计划制定了在发生任何重大中断的情况下恢复信息或技术系统的流程，工作重点是支持关键业务流程和客户活动的IT系统。PayPal的技术基础设施被放置在多个安全数据中心，这些数据中心具有主要和次要功能，每个中心都配备了网络和安全基础设施、专用应用程序和数据库服务器以及存储。

4. 定期测试、评估和评价技术和组织措施的有效性。

PayPal定期计划、执行和报告公司的测试计划结果，以评估和评价其技术和组织措施的有效性。该计划由我们的企业风险和合规团队进行管理，他们与相关的利益相关者合作，以获得和评估测试、报告和补救（如有必要）所需的信息。

5. 用户身份验证和授权。

PayPal的访问管理流程要求用户使用唯一的企业网络账号和密码登录企业网络，进行用户身份验证，然后才能访问任何其他范围内的应用程序。自动执行有关密码组合、长度、更改、重设和锁定的规则。基于角色的访问和审批每季度进行一次认证，在所有范围内的系统中实施，以落实最低权限原则。

6. 个人数据处理地点的物理安全。

PayPal的全球安全和安保规则和流程根据适用的法律、法规和合作伙伴要求，规定了促进健全的安全和安保流程（包括物理安全）的必要要求。根据公司的信息安全处理标准，在建设收发室、设备存储室、运输和收货区、计算机/服务器室、通信保险库或机密文件/信息存储区等特殊或敏感区域时，将特别注重安全系统和保障措施。

7. 事件记录和配置。

PayPal已经概述并定义了事件记录和监控类型和属性。公司收集并汇总了多种类型的日志到集中安全监控系统。标准的配置管理控制已经到位，可确保从系统中收集日志，然后转发到我们的集中安全监控系统。PayPal规则和支持流程规定，系统配置和强化基准必须在所有系统中实施。

8. IT治理和管理；流程和产品的认证和保证。

PayPal在全公司范围内推广树立强大的安全理念。我们的首席信息安全官负责监督我们全球企业的信息安全。作为企业风险与合规管理计划的一部分，我们的技术监督和信息安全计划旨在支持公司管理技术和信息安全风险，识别、保护、检测、应对信息安全威胁并从信息安全威胁中恢复。PayPal通过各种企业计划对其流程和产品予以认证和保证，包括（i）对PayPal的技术行业标准义务进行审计和评估，包括但不限于ISO 27001、支付卡行业（PCI）的适用标准（DSS、PIN、P2PE等）和美国注册会计师协会（AICPA）的SOC-1和SOC-2；（ii）风险控制识别流程（RCIP），确保早期参与并采用标准方法来衡量、管理和监控与产品解决方案的制定和发布相关的风险；（iii）整合到产品和软件开发流程初期的隐私影响评估；（iv）全面的第三方管理计划，该计划通过在与第三方合作的整个生命周期内持续管理风险来提供保证。

9. 数据最小化。

我们的规则要求，要通过技术控制确保收集和生成的数据元素具有充分性、相关性，并仅限于与数据处理目的相关的必要范围内。PayPal的隐私影响评估流程确保遵守这些规则。

10. 数据质量和保留。

PayPal的访问和质量规则确保所有个人数据是正确的、完整的、最新的数据，使个人用户能够访问系统来纠正和修改他们的详细信息（例如，地址、联系信息等），并在收到数据主体的纠正要求时，提供使其拥有纠正权的服务。我们的数据治理计划负责监控数据质量、问题和补救措施（如有必要）。我们要求所有数据根据其业务价值进行分类，并指定保留期，这是基于PayPal的法律、监管和业务记录要求所作的规定。保留期满后，数据和信息将被处置、删除或销毁。

11. 责任制。

PayPal制定了一套信息安全、技术、数据治理、第三方管理和隐私权保护规则和原则，这些规则和原则与行业标准保持一致，旨在通过利益相关者的协作和合作，使其认识并遵守整个组织范围内的此类规则和控制措施，确保整个组织自上而下参与其中，承担责任。每个计划都定义了跨职能的数据相关决策、流程和控制措施的责任。作为数据控制者，PayPal负责通过实施隐私计划规则以及底层组织和技术控制结构，证明其遵守了GDPR和其他适用数据保护法律中含责任承担义务的相关条款，从而确保整个企业遵守隐私法律、法规、规则和程序。这包括能够通过以下方式证明对数据保护法律的遵守：1）强大的合规文化，2）企业风险和合规治理结构，包括管理委员会、监督角色、隐私报告，3）业务职能部门对隐私权保护计划的合规性负责，包括建立、记录和维护业务流程和控制措施，4）企业合规组织内的全球隐私部门监督企业对隐私权保护计划的遵守情况，并定义由业务职能部门运

用的规则、标准、程序和工具，5）由全球隐私职能部门与企业沟通，提高对隐私权保护的认识和理解，6）企业风险和合规管理框架，确保使用一致的流程，包括隐私影响评估、隐私监控和测试、隐私问题管理、隐私培训、年度隐私计划，以及7）向监督隐私权保护计划的管理委员会提交报告和分析。

12. 数据主体权利。

PayPal制定了一个计划来确保数据主体的访问、纠正和删除等权利得到满足。除非PayPal有法律、监管义务或其他合法的业务原因需要保留数据，否则将满足数据删除的要求。PayPal的规则确保删除在整个客户的生命周期内都会发生。

13. 处理者。

PayPal制定了一个全面的第三方管理计划，该计划通过在与第三方合作的整个生命周期内持续管理风险来提供保证。我们实施合同控制措施，要求我们的处理者及其二级处理者在整个处理链中实施全面的数据安全和隐私标准。所有二级处理者在被聘用前必须得到我们的事先批准。

B）以下内容仅适用于英国传输条款

接收者
传输的个人数据只可向以下接收者披露：

- 输入方的服务提供商、附属公司以及根据《协议》履行服务的人员。

数据输出方的数据保护注册信息（如适用）

不适用。

其他有用信息（存储限制和其他相关信息）

参照《协议》和本附件1的上述规定。