拉卡拉支付个人信息保护政策

本版发布日期：2023 年 6 月 14 日

生效日期：2023 年 6 月 29 日

概述

我们深知个人信息对您的重要性，也感谢您对拉卡拉支付股份有限公司（以下简称“我们”）的信任。我们将通过本政策向您说明我们会如何收集、使用、保护、保存及对外提供您的信息，并说明您享有的权利，其中要点如下：

1、为了便于您了解您在使用我们的服务时，我们需要收集的信息类型与用途，我们将结合具体服务向您逐一说明。

2、为了向您提供服务所需，我们会按照合法、正当、必要的原则收集您的信息。

3、如果为了向您提供服务而需要将您的信息共享至第三方，我们将评估该第三方收集信息的合法性、正当性、必要性。我们将要求第三方对您的信息采取保护措施并且严格遵守相关法律法规与监管要求。另外，我们会按照法律法规及国家标准的要求以确认协议、具体场景下的文案确认、弹窗提示等形式征得您的同意或确认第三方已经征得您的同意。

4、如果为了向您提供服务而需要从第三方获取您的信息，我们将要求第三方说明信息来源，并要求第三方保障其提供信息的合法性；如果我们开展业务需进行的个人信息处理活动超出您原本向第三方提供个人信息时的授权范围，我们将征得您的明确同意。

5、您可以通过本政策介绍的方式访问和管理您的信息、设置隐私功能、注销拉卡拉服务账号或进行投诉举报。

6、本政策仅适用于拉卡拉支付股份有限公司提供的产品和服务及其延伸的功能（以下简称“拉卡拉支付服务”），包括 APP、网站、客户端、小程序、公众号、POS 机以及随技术发展出现的新形态向您提供的各项产品和服务。如我们提供的某款产品有单独的个人信息保护政策或相应的用户服务协议当中存在特殊约定，则该产品的个人信息保护政策将优先适用，该款产品个人信息保护政策和用户服务协议未涵盖的内容，以本政策内容为准。

本政策中涉及的专用术语和关键词有：

1、个人信息：指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。本个人信息保护政策中涉及的个人信息包括：**个人基本信息（包括个人姓名、个人电话号码、住址、电子邮箱）；个人身份信息（包括身份证）；个人生物识别信息（包括人脸活体检测照片）；网络身份标识信息（包括 APP 登录账号、密码）；个人财产信息（银行账户、流水记录）；个人常用设备信息（包括设备识别号（如 IMEI/IDFA/OPENUDID）；精准定位信息。**

2、个人敏感信息：指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。本个人信息保护政策中涉及的个人敏感信息包括：您的个人身份信息（包括身份证）；个人生物识别信息（包括人脸活体检测照片）；个人财产信息（银行账户、流水记录）；精准定位信息。

3、关联方：指一方现在或将来控制、受控制或与其处于共同控制下的任何公司、机构以及上述公司或机构的法定代表人。“控制”是指直接或间接地拥有影响所提及公司管理的能力，无论是通过所有权、有投票权的股份、合同或其他被人民法院认定的方式。

您可以根据以下索引阅读相应章节，进一步了解本政策的具体约定：

一、我们如何收集和使用您的个人信息

二、我们如何使用 Cookie、Beacon、Proxy 等技术

三、我们如何共享、转让、公开披露、委托处理您的个人信息

四、我们如何保护和保存您的个人信息

五、您如何管理您的个人信息

六、未成年人的个人信息保护

七、通知和修订

八、如何联系我们

拉卡拉支付股份有限公司（注册地址：北京市海淀区北清路中关村壹号 D1 座 6 层 606；常用办公地址：北京市海淀区北清路中关村壹号 D1 座）（以下简称“我们”）在您使用拉卡拉支付服务时，将按照本个人信息保护政策（以下简称“本政策”）收集、使用、保护、保存及对外提供您的信息。同时，我们会通过本政策向您说明，我们如何为您提供访问、更新、管理和保护您的信息的服务。本政策与您使用我们的服务关系紧密，我们建议您仔细阅读并理解本政策全部内容，做出您认为适当的选择。我们努力用通俗易懂、简明扼要的文字表达，并对本政策中与您的权益存在重大关系的条款和个人敏感信息，采用粗体字进行标注以提示您注意。

为了遵守国家法律法规及监管规定（例如：进行实名制管理、履行反洗钱职责、安全管理），也为了向您提供服务及提升服务质量（例如：支持我们设计新服务或完善已有服务功能，为您提供和推荐更为优质或适合的服务），我们需要收集、存储、使用及对外提供您的信息。您同意我们按照本政策约定处理您的信息，以便您享受优质、便捷的服务，同时更好地保护您的账户及资金安全。

一、我们如何收集和使用您的个人信息

（一）我们如何收集您的信息

在您使用拉卡拉支付服务的过程中，在以下情形中我们需要收集您的一些信息，用以向您提供服务、提升我们的服务质量、保障您的账户和资金安全以及符合国家法律法规及监管规定：

1、依据法律法规及监管规定履行反洗钱义务及进行实名制管理

（1）**在您注册拉卡拉服务账号时，您需提供手机号码作为您的有效联系方式。**如您不提供前述信息，可能无法注册拉卡拉服务账号。**根据相关法律法规的规定，您需通过身份基本信息多重交叉验证后方可使用我们的部分服务，例如您使用银行卡收单服务时，需要提供本人身份证信息、本人人脸活体认证、本人银行卡认证以完成身份基本信息多重交叉验证。**如您不提供前述信息，可能无法使用需要通过多重交叉验证后方可使用的部分服务，但不影响您使用我们提供的其他服务。同时，为了验证您提供信息的准确性和完整性，我们会与合法留存您的前述信息的国家机关、金融机构、企事业单位进行核对；

（2）**我们需根据《中华人民共和国反洗钱法》、《支付机构反洗钱和反恐怖融资管理办法》等反洗钱相关法律法规及监管要求，提示您适时提供有效身份证件的彩色影印件或照片及您的手机号码或其它联系方式以供我们核对并留存；**如您不提供前述信息或不同意我们留存，可能无法使用与监管要求相关的部分服务，但不影响您使用我们提供的其他服务。

2、向您提供服务

（1）若您为个人用户，我们可为您提供互联网支付服务、移动支付服务、数字电视支付服务、预付卡受理服务：

① 互联网支付：为了您能使用互联网支付服务，在您开通互联网支付服务，将您的银行卡与互联网支付账户绑定时，您需提供您的银行卡卡号、姓名、身份证号码、银行预留手机号、手机验证码。我们会将该等信息与发卡银行进行验证。为了完成支付和通过银行的验证，同时采集必要风控信息，保障交易的安全可信，您需要提供银行卡卡号、个人姓名、身份证号码、银行预留手机号，我们还需要采集您的交易金额、设备型号、IP 地址、个人位置信息、设备软件版本信息、设备识别码、设备标识符。如您不提供上述信息，将无法使用互联网支付服务。

② 移动支付：为了您能使用移动支付服务，在您开通移动支付服务，将您的银行卡与移动支付账户绑定时，您需提供您的银行卡卡号、姓名、身份证号码、银行预留手机号、手机验证码。我们会将该等信息与发卡银行进行验证。为了完成支付和通过银行的验证，同时采集必要风控信息，保障交易的安全可信，您需要提供银行卡卡号、个人姓名、身份证号码、银行预留手机号，我们还需要采集您的交易金额、设备型号、IP 地址、个人位置信息、设备软件版本信息、设备识别码、设备标识符。如您不提供上述信息，将无法使用移动支付服务。

③ 数字电视支付：为了您能使用数字电视支付服务，在您开通数字电视支付服务，将您的银行卡与数字电视支付账户绑定时，您需提供您的银行卡卡号、姓名、身份证号码、银行预留手机号、手机验证码。您需按照页面提示输入收款人账户、收款人部分姓名、转账金额。如您不提供前述信息，转账可能无法进行，但不影响您使用我们提供的其他服务。我行还会收集您的收付款交易信息，形成收款人名册，以简化您的转账操作。上述信息属于个人敏感信息，如您拒绝提供该信息，仅会使您无法使用上述功能。

④ 预付卡受理：为了您能使用预付卡受理服务，在您开通预付卡受理服务，将您的银行卡与预付卡收单商户账户绑定时，您需提供您的银行卡卡号、姓名、身份证号码、营业执照号码、银行预留手机号、手机验证码。如您不提供前述信息，预付卡支付转账可能无法进行，但不影响您使用我们提供的其他服务。如您拒绝提供该信息，仅会使您无法使用上述功能。

（2）若您为特约商户，我们可为您提供互联网支付服务、移动支付服务、数字电视支付服务、预付卡受理服务以及银行卡收单服务。在您使用这些服务时，我们需要您提供以下信息，如您不提供此类信息，您将无法使用相关功能，但不影响您使用我们提供的其他服务。

① 商户开通服务：为了保证您正常使用拉卡拉提供的支付服务，我们需在为您开通商户的过程中，需要获取您的 1）个人信息，包括手机号码、姓名、身份证号、身份证正反面照片、 邮箱（非必填）；2）收款入账银行账户信息，包括开户行、户名、账号；3）店铺经营信息，包括店铺名称、店铺地址、门头照或经营场所照片。

② 商户升级服务：您可以通过提交更多认证资料提升您的商户等级，认证资料包括 1）信用卡认证信息，包括您本人的信用卡开户行、账户名、卡号、银行预留手机号码；2）营业执照认证信息，包括您开通商户时使用的经营店铺名称、营业执照号、营业执照照片。

③ 商户提款服务：您使用提款服务时，需要先开通服务功能，对您在商户开通过程中提交的个人信息、银行卡信息进行再次验证。

④ 收款交易：在您使用我们的收款服务时，为保证交易的安全性和合规性，我们需要获取您的 GPS 定位信息、手机蓝牙权限、设备识别号 IMEI/IDFA、以及交易卡卡号信息（加密）。

⑤ 交易查询：为了向您提供日常交易、资金管理服务，方便您实时查看交易信息与经营数据，我们记录并向您展示您的交易流水及划款入账信息。

（3）在线客服：为了更好的达成我们向您提供的服务，我们向您提供在线客服服务，您使用时我们需要获取您的相机及相册使用权限、麦克风权限、外部读写存储权限，方便您更好的与我们交流。

（4）增值业务：我们在为您提供的其他增值业务过程中，会在您明确授权的情况下向您提供相应的服务。

（5）其他业务：我们将会不断更新产品和服务，如您申办我们提供的其他业务，我们将会根据业务需要使用您的个人信息。

3、使用 SDK 实现的业务功能

（1）AVOS 数据统计服务：用于统计、分析 APP 数据，记录用户行为，我们可能会获取您的设备标识、设备型号、运营商、APP 版本信息。

（2）百度 OCR 识别：用于身份认证服务，我们可能会通过此服务来采集您的身份证照片及照片内容（如姓名、身份证号、地址）信息。

（3）文通 OCR 识别：用于在公安系统的身份认证，我们可能会获取您的身份证照片及照片内容（如姓名、身份证号、地址）信息。

（4）合合 OCR 识别：用于在公安系统的身份认证，我们可能会获取您的身份证照片及照片内容（如姓名、身份证号、地址）信息。

（5）商汤 OCR：用于身份认证，我们可能会获取您的身份证照片及照片内容（如姓名、身份证号、地址、银行卡号）信息。

（6）商汤人脸识别：用于人脸识别服务，我们可能会获取您的人脸照片信息,我们将在使用您的人脸照片实现认证功能后删除您的人脸照片原始图像。

（7）邦盛设备指纹：用于生成唯一设备指纹标识，我们可能会获取您的手机硬件信息（如 CPU、IMEI 等）、手机系统信息（如内存、网络、蓝牙）信息。

（8）银盾思创密码键盘：用于身份认证，我们可能会获取您通过密码键盘设置的登录、支付加密数据信息。

（9）腾讯 SDK：用于收集 APP 崩溃日志，我们可能会收集您的日志信息（包括：第三方开发者自定义日志、Logcat 日志以及 APP 崩溃堆栈信息）、设备 ID（包括：androidid 以及 idfv）、联网信息、系统名称、系统版本以及国家码。

（10）淘宝 SDK：采用阿里的 WEEX 架构实现客户端跨平台开发，不收集您的任何信息。

（11）微信 openSDK：用于提供微信分享服务，我们可能会收集您准备收藏或分享朋友圈的图片信息。

（12）Zxing 二维码 SDK：用于二维码拍照和获取相册里的二维码，我们需要获取您的相册存储权限和相机权限。

（13）云核网络密码键盘：用于身份认证，我们可能会获取您通过密码键盘设置的登录、支付加密数据信息。

（14）阿里云号码认证 SDK：用于一键登录功能，我们可能会获取您的本机号码。

（15）腾讯 TPNS 推送 SDK：用于推送通知，不收集您的任何信息。

（16）百度语音识别 SDK：用于语音合成，播报推送信息，不收集您的任何信息。

4、您在使用拉卡拉支付服务的某些 APP 产品的情形中，您可选择是否授权我们收集、使用您的个人信息。如您拒绝授权部分功能或服务所需信息，您将无法使用相关功能或服务，但这不影响您正常使用拉卡拉支付服务的其他功能或服务：

（1）设备信息，用于统计、分析 APP 数据，记录用户行为，提供定位服务，推送 APP 消息服务，生成唯一设备指纹标识。

（2）位置信息，用于提供定位服务，在使用开通商户、收款服务时，保证安全性合规性。

（3）摄像头，用于直接拍摄并上传图片用于开通商户、商户升级、在线客服咨询、特定场景下经授权的人脸识别等明确场景。

（4）相册/存储，用于手机中的照片、图片或视频的取用和上传。

（5）蓝牙，用于实现手机与刷卡器设备的连接，便于使用收单服务。

（6）网络通讯，用于与服务端进行通讯。拒绝授权后，APP 所有基于网络服务的功能将无法使用。APP 系统后台保存您使用 APP 时所使用设备的网络信息，包括 IP、端口信息。

上述功能可能需要您在您的设备中向我们开启您的设备、地理位置（位置信息）、相机（摄像头）、相册（存储）、蓝牙的访问权限，以实现这些功能所涉及的信息的收集和使用。请您注意，您开启这些权限，即代表您授权我们可以收集和使用这些信息来实现上述功能。若您取消了这些授权，我们将不再继续收集和使用您的这些信息，但同时也无法为您提供上述与这些授权所对应的功能。

5、当您在拉卡拉支付服务的产品上进行人脸识别以进行身份认证时，我们会采集您的人脸照片，并将在实现认证功能后删除您的人脸照片原始图像。

6、安全管理

为了保障向您提供的服务的安全稳定运行，我们需要记录您使用的服务类别、方式及相关操作信息，例如：所属运营商、设备硬件信息、设备型号、IP 地址、设备软件版本信息、设备识别码、设备标识符、所在地区、网络使用习惯以及其他与拉卡拉支付服务相关的日志信息。如您不同意我们记录前述信息，可能无法完成风控验证。

7、根据相关法律法规及国家标准，在以下情形中，我们可能会依法收集并使用您的个人信息无需征得您的同意：

（1）与个人信息控制者履行法律法规规定的义务相关的；

（2）与国家安全、国防安全直接相关的；

（3）与公共安全、公共卫生、重大公共利益直接相关的；

（4）与犯罪侦查、起诉、审判和判决执行等直接相关的；

（5）出于维护您或他人的生命、财产等重大合法权益但又很难得到您本人同意的；

（6）所收集的个人信息是您自行向社会公众公开的；

（7）根据您的要求签订和履行合同所必需的；

（8）从合法公开披露的信息中收集个人信息，例如：合法的新闻报道、政府信息公开等渠道；

（9）用于维护所提供的服务的安全稳定运行所必需的，例如：发现、处置服务的故障；

（10）法律法规规定的其他情形。

8、其他

如您选择使用我们提供的其他服务，基于该服务我们需要收集您的信息的，我们会另行向您说明信息收集的范围与目的，并征得您的同意。我们会按照本政策以及相应的用户协议约定使用、存储、对外提供及保护您的信息；如您选择不提供前述信息，您可能无法使用某项或某部分服务，但不影响您使用我们提供的其他服务。

（二）我们从第三方获得您个人信息的情形

在取得您同意的前提下，我们可能从合法持有您个人信息的第三方机构获得您的个人信息，如技术、咨询服务供应商、金融机构等，这些合作机构会提供与我们服务相关的产品和服务，帮助检测和防止潜在的违法犯罪行为和违反我们政策的行为。

（三）我们如何使用您的信息

我们收集您信息的目的主要是为了向您提供安全、高效的服务体验。我们会出于以下目的使用您的个人信息：

1、进行身份证件认证、人脸识别、银行卡认证、工商认证

为了遵守个人用户实名制管理规定(反洗钱/反欺诈)和为您提供安全服务的需要，您同意并授权我们收集和使用您的1）**若您为个人用户：姓名、性别、国籍、职业、住所地或者工作单位地址、身份证件或者其他身份证明文件的种类、证件号码、证件有效期限（开始时间-截止时间）、人脸照片、手机号码、银行卡号、银行预留手机号；2）若您为企业用户：企业名称、住所、经营范围、可证明企业依法设立或者可依法开展经营、社会活动的执照、证件或者文件的名称（比如统一社会信用代码）、号码和有效期限、企业银行账户名称、账号、开户行、法定代表人姓名、身份证或者其他身份证明文件的种类、证件号码、证件有效期限（开始时间-截止时间）、人脸照片及手机号码、委托代理人姓名、身份证或者其他身份证明文件的种类、证件号码、证件有效期限（开始时间-截止时间）、人脸照片及手机号码，以及受益所有人的姓名、地址、身份证或者其他身份证明文件的种类、证件号码、证件有效期限，**并以加密传输方式将其共享给提供验证服务的第三方机构进行一致性比对并输出核验结果；您同意并授权第三方机构使用您的个人信息用于验证服务并以加密传输的方式向我们返回核验结果。如果您不提供上述信息则无法使用根据中国相关法律法规必须进行实名制管理的相关服务。

2、为您提供您选择的相关服务

您在使用我们平台上的服务时，我们会使用您的个人身份信息、个人财产信息及其他在业务具体开展过程中基于您的同意而采集的信息对产品或服务进行适用性评估、验证服务真实性、处理产品或服务请求以及完成服务指令并向您发送服务通知等。同时，为了遵守相关法律法规及监管规定，也为了便于您查询服务记录或历史状态，我们会将您使用的身份信息、服务信息及行为信息进行存档，并严格按照法律法规的规定对这些信息进行妥善保管。上述信息为开展我们服务所必需的信息，如果您不提供上述信息，将可能导致我们无法为您提供上述服务。

3、提供客户服务及进行投诉处理

我们的在线客服会使用您的账号信息和服务信息。为保证您的账号安全，我们的在线客服会使用您的账号信息与您核验您的身份。当您需要我们提供与您服务信息相关的客服与售后服务时，我们将会提供账户绑定服务并查询您的服务信息。

为了保证您及他人的合法权益，如您被他人投诉或投诉他人，在必要时，我们会将您的姓名及身份证号码、投诉相关内容提供给消费者权益保护部门及监管机关，以便及时解决投诉纠纷，但法律法规明确禁止提供的除外。

4、改进我们的产品和服务

（1）我们会在采取脱敏、去标识化等方式对您的信息进行处理后再进行综合统计、分析加工，以便为您提供更加准确、个性、流畅及便捷的服务，或帮助我们评估、改善或设计服务及运营活动等；

（2）为了提升您的服务体验，我们可能会向您提供客户服务以及营销活动通知、商业性电子信息或广告，**如您不希望接收此类信息，您可按照我们提示的方法选择退订，例如回复“TD”退订此类短信。**

当我们要将信息用于本政策未载明的其他用途时，会按照法律法规及国家标准的要求以确认协议、具体场景下的文案确认动作等形式再次征得您的同意。

5、保障服务安全所必须的功能

为提高您使用我们的产品与/或服务时系统的安全性，更准确地预防钓鱼网站欺诈和保护账户安全，我们可能会通过了解您的浏览信息、服务信息、您常用的软件信息、设备信息等手段来判断您的账号风险，并可能会记录一些我们认为有风险的链接；我们也会收集您的设备信息对于我们系统问题进行分析、统计流量并排查可能存在的风险、在您选择向我们发送异常信息时予以排查。

（四）您个人信息使用的规则

1、我们会根据本政策的约定并为实现我们的产品与/或服务功能、履行协议、提供服务、解决争议、保障交易安全等目的对您所提供的以及我们收集的个人信息进行使用。

2、请您注意，您在使用我们的产品与/或服务时所提供的所有个人信息，除非您删除或通过系统设置拒绝我们收集，否则将在您使用我们的产品与/或服务期间持续授权我们使用。您注销账号请求处理完成后，我们将停止您使用该账号的权限并按照相关法律法规的要求删除您的个人信息或进行匿名化处理。

3、当我们展示您的个人信息时，我们会根据《个人金融信息保护技术规范》（JR/T 0171-2020）采用模糊化、不可逆等技术处理方式对您的信息进行脱敏，以保护您的信息安全。

4、当我们要将您的个人信息用于本政策未载明的其它用途时，或基于特定目的收集而来的信息用于其他目的时，会事先征求您的同意。

二、我们如何使用 Cookie、Beacon、Proxy 等技术

为使您获得更轻松的访问体验，您使用拉卡拉支付提供的服务时，我们可能会通过小型数据文件识别您的身份，这么做可帮您省去重复输入注册信息的步骤，或者帮助判断您的账户安全状态。这些数据文件可能是 Cookie、Flash Cookie，您的浏览器或关联应用程序提供的其他本地存储（以下简称“Cookie”）。借助于 Cookie，在您使用您的浏览器访问服务器后，服务器会传给浏览器一段特定的数据识别串。每次浏览器访问该服务器，都必须带上这段数据识别串进行校验，Cookie 中不包括任何用户敏感信息。

请您理解，我们的某些服务只能通过使用 Cookie 才可得到实现。**如您的浏览器或浏览器附加服务允许，您可以修改对 Cookie 的接受程度或者拒绝拉卡拉支付的 Cookie。**多数浏览器工具条中的“帮助”部分会告诉您怎样防止您的浏览器接受新的 Cookie，怎样让您的浏览器在您收到一条新 Cookie 时通知您或者怎样彻底关闭 Cookie。此外，您可以通过改变浏览器附加程序的设置，或通过访问提供商的网页，来关闭或删除浏览器附加程序使用的类似数据（例如：Flash Cookie）。但这一举动在某些情况下可能会影响您安全使用拉卡拉支付提供的服务。

我们网站上还可能包含一些电子图像（以下简称“网络 Beacon”），使用网络 Beacon 可以帮助网站计算浏览网页的用户或访问某些 Cookie，我们会通过网络 Beacon 收集**您浏览网页活动的信息，例如：您访问的页面地址、您先前访问的援引页面的位置、您的浏览环境以及显示设定。**

如您通过我们的网站或 APP，使用了由第三方而非拉卡拉支付提供的服务时，为尽力确保您的账号安全，使您获得更安全的访问体验，我们可能会使用专用的网络协议及代理技术（以下简称“Proxy 技术”）。使用 Proxy 技术，可以帮助您识别到我们已知的高风险站点，减少由此引起的钓鱼、账号泄露等风险，同时更有利于保障您和第三方的共同权益，阻止不法分子篡改您和您希望访问的第三方之间正常服务内容，例如：不安全路由器、非法基站等引起的广告注入、非法内容篡改等。在此过程中，我们也可能会获得和保存关于**您计算机的相关信息，例如：IP 地址、硬件 ID**。

三、我们如何共享、转让、公开披露、委托处理您的个人信息

（一）共享

1、业务共享

我们承诺对您的信息进行严格保密。除法律法规及监管部门另有规定外，我们仅在以下情形中与第三方共享您的信息，第三方包括我们的关联方、合作金融机构以及其他合作伙伴。如果为了向您提供服务而需要将您的信息共享至第三方，我们将评估该第三方收集信息的合法性、正当性、必要性。当您通过拉卡拉服务账号使用第三方主体通过拉卡拉支付服务的 APP、网站、客户端、小程序、公众号、POS 机或其他应用提供的产品或服务时，我们将基于您在具体场景下的授权将您的拉卡拉用户 ID 及页面提示的相关信息传递给第三方。向您取得授权的页面提示上会展示具体授权对象以及授权信息类型，您的信息将通过加密通道传递给第三方。我们将会根据本政策的约定与第三方共享您的个人信息，但我们只会共享必要的个人信

息，且受本政策中所声明目的的约束。第三方如要改变个人信息的处理目的，将再次征求您的授权同意。我们将要求第三方对您的信息采取保护措施，并且严格遵守相关法律法规与监管要求。

（1）某些产品或服务可能由第三方提供或由我们与第三方共同提供，因此，只有共享您的信息，才能提供您需要的产品或服务。

（2）如您已授权合法征信机构为您提供征信服务，则您同意并授权我们向该征信机构提供您的**商户基本信息、商户基本信息变更历史及商户交易流水信息**。

（3）如您选择参与我们和第三方联合开展的推广活动，我们可能与其共享活动过程中产生的、为完成活动所必要的信息，以便第三方能及时向您发放奖励、补贴或为您提供服务，我们会依据法律法规或国家标准的要求，在活动规则页面或通过其他途径向您明确告知需要向第三方提供何种信息。

（4）事先获得您明确同意的情况下，我们会在法律法规允许且不违背公序良俗的范围内，依据您的授权范围与第三方共享您的信息。

2、其它合作共享

我们可能会向合作伙伴等第三方共享您的**服务信息、账户信息及设备信息**，以保障为您提供的服务顺利完成。但我们仅会出于合法、正当、必要、特定、明确的目的共享您的个人信息，并且只会共享提供服务所必要的个人信息。我们的合作伙伴无权将共享的个人信息用于任何其他用途。我们的合作伙伴包括以下类型：

（1）提供技术、咨询服务的供应商。我们可能会将您的手机号码等个人信息共享给支持我们提供服务的第三方。这些机构包括为我们提供基础设施技术服务、数据处理服务、电信服务、审计服务和法律服务等的机构。但我们要求这些服务提供商只能出于为我们提供服务的目的使用您的信息，而不得出于其自身利益使用您的信息。

（2）合作金融机构及保险机构，这些机构可以向我们提供金融服务产品。除非您同意将这些信息用于其他用途，否则这些金融机构不得将此类信息用于相关产品之外的其他目的。

（3）第三方 SDK 服务机构。为了向您提供更好的服务，我们接入了第三方 SDK 服务，并将您的部分信息提供给第三方服务机构。

① 百度定位：用于提供定位服务，北京百度网讯科技有限公司可能获取了您的 IMEI 信息、位置信息、运营商信息。

② AVOS 推送：用于为您提供推送 APP 消息服务，美味书签（北京）信息技术有限公司可能会获取您的手机设备标识、设备型号、运营商、网络类型信息。

③ 华为推送：用于为您提供推送 APP 消息服务，华为终端有限公司可能会获取您的手机设备标识、设备型号、运营商、网络类型信息。

④ 小米推送：用于为您提供推送 APP 消息服务，小米科技有限责任公司可能会获取您的手机设备标识、设备型号、运营商、网络类型信息。

⑤ 魅族推送：用于为您提供推送 APP 消息服务，珠海市魅族科技有限公司可能会获取您的手机设备标识、设备型号、运营商、网络类型信息。

⑥ Share：用于提供社会化分享服务（包括：微信、QQ、微博），广州掌淘网络科技有限公司可能会获取您的手机设备标识、网络状态信息。

⑦ OPPO 推送：用于为您提供推送 APP 消息服务，OPPO 广东移动通信有限公司可能会获取您的手机设备标识、设备型号、运营商、网络类型信息。

⑧ VIVO 推送：用于为您提供推送 APP 消息服务，维沃移动通信有限公司可能会获取您的手机设备标识、设备型号、运营商、网络类型信息。

⑨ 百度云推送：用于为您提供推送 APP 消息服务，北京百度网讯科技有限公司可能会获取您的手机设备信息。

⑩ 腾讯 SDK：（1）为优化产品和服务，收集 APP 崩溃日志，深圳市腾讯计算机系统有限公司可能需要向 APP 开发者和/或终端用户收集相关个人信息，主要包括：日志信息（包括：第三方开发者自定义日志、Logcat 日志以及 APP 崩溃堆栈信息）、设备 ID（包括：androidid 以及 idfv）、联网信息、系统名称、系统版本以及国家码。（2）为分析用户统计错误以及进行 APP 版本更新，深圳市腾讯计算机系统有限公司可能会获取您的设备 MAC 地址、文件存储权限、相机权限、系统设置权限、网路权限。

⑪ 微信 openSDK：用于向您提供微信分享服务，深圳市腾讯计算机系统有限公司可能会获取您的 openID 并收集您的图片数据用于分享到朋友圈或微信收藏，但不会用于关联和追踪用户。

⑫ 友盟数据统计服务：用于统计、分析 APP 数据以及记录用户行为，友盟同欣（北京）科技有限公司可能会获取您的设备标识、设备 MAC 地址、设备型号、运营商、APP 版本信息。

⑬ 腾讯 X5 内核：用于兼容显示 h5 页面，深圳市腾讯计算机系统有限公司可能会获取您的设备 MAC 地址、文件存储权限和相机权限，以方便您上传照片和视频等。

⑭ 易道博识 OCR 识别：用于商户身份证识别、银行卡识别，北京易道博识科技有限公司可能会获取您的身份证信息，银行卡信息。

⑮ Firebase crashlytic：用于统计 APP 崩溃情况。谷歌有限责任公司可能会获取了您的 IMEI 信息、位置信息。

上述相关第三方服务商收集前述信息发生信息泄露的，由相关第三方服务商承担相应的法律责任。

若您不同意上述第三方服务商收集前述信息，可能无法获得相应服务，但不影响您正常使用 APP 其他功能或服务。

3、对我们与之共享个人信息的公司、组织和个人，我们会与其签署严格的保密协定，要求他们按照我们的说明、本政策以及其他任何相关的保密和安全措施来处理个人信息。在个人敏感数据使用上，我们要求第三方采用数据脱敏和加密技术，从而更好地保护用户数据。

4、为了遵守法律、执行或适用我们的使用条件和其他协议，或者为了保护我们、您或其他我们客户的权利及其财产或安全，比如为防止欺诈等违法活动和减少信用风险，在取得您的同意后，我们可能会与银联、人民银行等监管机构或组织交换您的个人信息、服务信息及活动信息。不过,这并不代表我们会违反本政策中所作的承诺而为获利目的出售、出租、共享或以其它方式披露的个人信息。

5、若您未能按照与我们及我们其他用户签订的协议等法律文本的约定履行应尽义务，我们有权将上述信息写入黑名单，且与必要第三方进行数据共享，以供我们平台及第三方审核、催收之用。

（二）转让

我们不会将您的个人信息转让给任何公司、组织和个人，但以下情况除外：

1、事先获得您明确的同意或授权；

2、根据法律法规或强制性的行政或司法要求；

3、在涉及资产转让、收购、兼并、重组或破产清算时，如涉及到个人信息转让，我们会向您告知有关情况，并要求新的持有您个人信息的公司、组织继续受本政策的约束，如变更个人信息使用目的时，我们将要求该公司、组织重新取得您的明确同意。

（三）公开披露

我们仅会在以下情况下，且采取符合业界标准的安全防护措施的前提下，才会公开披露您的个人信息。除此之外，原则上我们不会将您的信息进行公开披露。如确需公开披露时，我们会向您告知公开披露的目的、披露信息的类型及可能涉及的敏感信息，并征得您的明确同意。

1、根据您的需求，在您明确同意的披露方式下披露您所指定的个人信息；

2、根据法律、法规的要求、强制性的行政执法、司法要求所必须提供您个人信息的情况下，我们可能会依据所要求的个人信息类型和披露方式公开披露您的个人信息。

（四）委托处理

为了提升信息处理效率，降低信息处理成本，或提高信息处理准确性，我们可能会委托有能力的我们的关联方或其他专业机构代表我们来处理信息。我们会通过书面协议、现场审计等方式要求受托公司遵守严格的保密义务及采取有效的保密措施，禁止其将这些信息用于未经您授权的用途。在委托关系解除时，受托公司不再保存个人信息。

（五）根据相关法律法规及国家标准，在以下情形中，我们可能会依法共享、转让、公开披露您的个人信息无需征得您的同意：

1、履行法律法规规定的义务相关的；

2、与国家安全、国防安全直接相关的；

3、公共安全、公共卫生、重大公共利益直接相关的；

4、与犯罪侦查、起诉、审判和判决执行等直接相关的；

5、出于维护您或其他个人的生命、财产等重大合法权益但又很难得到您本人同意的；

6、您自行向社会公众公开的个人信息；

7、从合法公开披露的信息中收集的个人信息，例如：合法的新闻报道、政府信息公开等渠道。

四、我们如何保护和保存您的个人信息

（一）我们保护您个人信息的技术与措施

我们非常重视个人信息安全，但互联网环境并非百分之百安全。我们承诺不会将您的信息恶意出售或免费共享给任何第三方且会尽量采取一切符合行业标准和惯例的措施保护您的个人信息。

1、数据安全技术措施

我们会采用符合业界标准的安全防护措施以及行业内通行的安全技术来防止您的个人信息遭到未经授权的访问、修改,避免您的个人信息泄露、损坏或丢失：

（1）采取加密技术对您的个人信息进行加密存储。

（2）我们的网络服务采取了传输层安全协议等加密技术，通过 https 等方式提供浏览服务，确保您的个人信息在传输过程中的安全。

（3）在使用您的个人信息使用时，例如个人信息展示、个人信息关联计算，我们会根据《个人金融信息保护技术规范》（JR/T 0171-2020）采用包括模糊化、不可逆在内的多种数据脱敏技术增强个人信息在使用中的安全性。

（4）我们存储您个人数据的系统从安全管理、策略、过程、网络体系结构等诸多方面保障交易及个人信息安全。

2、为保护个人信息采取的其他安全措施

我们通过建立数据分类分级、数据安全策略、安全开发规范来管理规范个人信息的存储和使用：

（1）我们采用严格的数据访问权限和多重身份认证技术控制和保护个人信息，通过与信息接触者签署严格的保密协议、监控和审计机制来对数据进行全面安全控制，避免数据被违规使用。

（2）我们采用代码安全检查、数据访问日志分析技术进行个人信息安全审计。

（3）我们还会举办安全和隐私保护培训课程，加强员工对于保护个人信息重要性的认识。

3、安全事件处置

（1）为应对个人信息泄露、损毁和丢失等可能出现的风险，我们制定了多项制度，明确安全事件、安全漏洞的分类分级标准及相应的处理流程。我们为安全事件建立了专门的应急响应团队，按照安全事件处置规范要求，针对不同安全事件启动安全预案，进行止损、分析、定位、制定补救措施、联合相关部门进行溯源和打击。

（2）一旦发生个人信息安全事件，我们将按照法律法规的要求，及时向您告知安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、您可自主防范和降低风险的建议、对您的补救措施等。我们同时将及时将事件相关情况以邮件、信函、电话、推送通知等方式告知您，难以逐一告知个人信息主体时，我们会采取合理、有效的方式发布公告。同时，我们还将按照监管部门要求，主动上报个人信息安全事件的处置情况。

（二）您个人信息的保存

1、我们在中华人民共和国境内收集和产生的个人信息将存储在中华人民共和国境内。如部分服务涉及跨境业务，我们需要向境外机构传输境内收集的相关个人信息的，我们会按照法律法规和相关监管部门的规定执行，向您说明个人信息出境的目的以及涉及的个人信息类型，征得您的同意，并通过签订协议、现场核查等有效措施，要求境外机构为所获得的您的个人信息保密。

2、我们仅在法律法规要求的期限内，以及为实现本政策声明的目的所必须的时限内保留您的个人信息。关于个人敏感信息，比如人脸照片，我们将在实现认证功能后删除您的人脸照片原始图像。其他个人敏感信息（比如身份证照片、银行卡信息）以及个人敏感信息以外的其他个人信息（比如电话号码），我们将保存至您的账号注销之日，我们承诺这是为了保证您作为拉卡拉消费者的权益所必需的最短期间，当您的个人信息超出该期限后，我们会对您的个人信息进行删除或匿名化处理。法律法规另有规定的除外。

3、如果我们终止服务或运营，我们会至少提前三十日通知您，并在终止服务或运营后对您的个人信息进行删除或匿名化处理。

五、您如何管理您的个人信息

我们非常重视您对个人信息的关注，并尽全力保护您对于您个人信息访问、更正、删除以及撤回同意的权利，以使您拥有充分的能力保障您的隐私和安全。您的权利包括：

1、访问和更正您的个人信息

（1）对于您在使用我们的产品与/或服务过程中产生的个人信息需要访问或更正，请随时通过本政策中的联系方式联系我们。我们会在接收到您需求的十五个工作日内进行处理。

（2）您无法访问和/或更正的个人信息：您的部分个人信息我们还无法为您提供访问和/或更正的服务，这些信息主要是为了保证交易安全满足相关强制性法律法规要求所收集的您的设备信息、您使用金融产品时产生的个人信息。上述信息我们会在您的授权范围内按照相关法律法规的规定进行使用，您无法变更或自主删除。

2、删除您的个人信息

您在我们的产品与/或服务页面中可以修改或直接删除您的部分信息。您也可以向我们提出删除申请。一旦您删除信息后，我们即会对此类信息进行删除或匿名化处理，法律法规另有规定的除外。

在以下情形中，您可以向我们提出删除个人信息的请求：

（1）如果我们处理个人信息的行为违反法律法规；

（2）如果我们收集、使用您的个人信息，却未征得您的同意；

（3）如果我们处理个人信息的行为违反了与您的约定；

（4）如果您注销了拉卡拉服务账号；

（5）如果我们终止服务及运营。

若我们决定响应您的删除请求，我们会根据您的要求及相关法律法规的要求进行后续删除处理并向您进行结果反馈。

3、管理您的授权范围

如您想改变授权范围或取消向第三方共享信息的授权，您可通过您的硬件设备进行修改，或在我们的产品与/或服务页面中自行操作，或联系我们的客服进行处理。您也可以通过注销账号的方式，永久撤回我们继续收集您个人信息的全部授权。当您取消信息收集的授权后，我们将不再收集该信息；在您取消向第三方共享信息的授权后，我们将不再在该业务场景下向该第三方提供信息。

请您理解，每个业务功能需要一些基本的个人信息才能得以完成，当您撤回同意或取消授权后，我们将无法继续为您提供撤回同意或取消授权所对应的服务，但您撤回同意或取消授权的决定，不会影响我们此前基于您的授权而开展的个人信息处理。

4、注销账户

您可以通过我们的产品与/或服务页面中的指示或者联系我们的客服申请注销您的拉卡拉服务账号，我们将在 15 个工作日内处理完。您注销账户后，我们将停止为您提供产品与/或服务，我们将删除您的个人信息，但基于已经或可能发生的民事争议处理需要作为证据留存的以及法律法规或监管机构对个人信息存储时间另有规定的除外。

5、个人信息副本的获取

您有权获取您的个人信息副本，您可以联系您的客户经理或者我们的客服进行申请。

6、尽管有上述约定，但按照相关法律法规及国家标准，在以下情形中，我们可能无法响应您的请求：

（1）与个人信息控制者履行法律法规规定的义务相关的；

（2）与国家安全、国防安全直接相关的；

（3）与公共安全、公共卫生、重大公共利益直接相关的；

（4）与犯罪侦查、起诉、审判和执行判决等直接相关的；

（5）有充分证据表明您存在主观恶意或滥用权利的；

（6）出于维护您或其他个人的生命、财产等重大合法权益但又很难得到您本人授权同意的；

（7）响应您的请求将导致您或其他个人、组织的合法权益受到严重损害的；

（8）涉及商业秘密的；

（9）您的账户中存有未办结的业务，如账户还有余额或有债务未清偿。

7、投诉与申诉

您可以通过本政策提供的联系渠道联系我们，并就您在使用服务过程中发生的事项进行投诉，也可以通过该渠道就我们对您的信息进行的自动处理进行申诉。我们将在十五个工作日内进行处理。

六、未成年人的个人信息保护

1、我们非常重视对未成年人个人信息的保护。您应当为十八周岁以上、符合中华人民共和国法律规定的具有完全民事权利和民事行为能力，能够独立承担民事责任的人。如您不具备上述资格，您应立即停止在我们平台的注册程序、停止使用我们平台服务。

2、对于经父母或法定监护人同意而收集未成年人个人信息的情况，我们只会在受到法律允许、父母或监护人明确同意或者保护未成年人所必要的情况下使用或公开披露此信息。

3、如果我们发现自己在未事先获得可证实的父母或法定监护人同意的情况下收集了未成年人的个人信息，则会设法尽快删除相关数据。

七、通知和修订

1、为给您提供更好的服务以及随着我们业务的发展，本政策也会随之更新。但未经您明确同意，我们不会削减您依据本政策所应享有的权利。我们会通过在我们的平台、移动端上发出更新版本并在生效前通过公告或以其他适当方式提醒您相关内容的更新，也请您访问我们的平台或移动端以便及时了解最新的个人信息保护政策。

2、对于重大变更，我们还会提供更为显著的通知（我们会通过包括但不限于 APP 推送通知、APP 公告、弹窗提示、发送邮件/短信或在浏览页面做特别提示等方式，说明个人信息保护政策的具体变更内容）。**本政策所指的重大变更包括但不限于：**

（1）我们的基本情况发生变化，例如：兼并、收购、重组引起的所有者变更；

（2）收集、存储、使用个人信息的范围、目的、规则发生变化；

（3）对外提供个人信息的对象、范围、目的发生变化；

（4）您访问和管理个人信息的方式发生变化；

（5）数据安全能力、信息安全风险发生变化；

（6）用户询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式发生变化；

（7）其他可能对您的个人信息权益产生重大影响的变化。

八、如何联系我们

我们设立了信息安全部作为个人信息保护的专职部门，并配有信息保护负责人。如果您对本政策有任何疑问、意见或建议，可以通过以下渠道联系我们的信息保护负责人：

（1）客服热线 95016；

（2）“拉卡拉 95016 官方客服”公众号在线客服；

（3）发送电子邮件至 info-sec@lakala.com。

我们将尽快审核所涉问题，并在十五个工作日内予以回复。如果您对我们的回复不满意，特别是我们的个人信息处理行为损害了您的合法权益，您还可以向网信、电信、公安及工商监管部门进行投诉或举报，或者通过向被告住所地有管辖权的法院提起诉讼来寻求解决方案。

拉卡拉人脸信息验证授权协议

《拉卡拉人脸信息验证授权协议》（以下简称“本协议”）是拉卡拉支付股份有限公司（以下简称“我们”）与您就“人脸信息验证”相关事项订立的有效合约。请您先仔细阅读并充分理解本协议全部内容。如您对本协议内容及页面提示信息有疑问，请勿进行下一步操作。

1、为了遵守个人用户实名制管理规定（反洗钱/反电信网络诈骗）和为您提供安全服务的需要，您同意并授权我们收集和使用您的人脸照片进行人脸识别以进行身份认证，并同意以加密传输方式将其共享给提供验证服务的第三方机构进行一致性比对并输出核验结果；您同意并授权第三方机构使用您的个人信息用于验证服务并以加密传输的方式向我们返回核验结果。如果您不提供上述信息则无法使用根据中国相关法律法规必须进行实名制管理的相关服务。

2、我们将开启您的摄像头使用商汤人脸识别 SDK 获取您的人脸照片信息用于人脸识别服务，我们将在使用您的人脸照片实现认证功能后删除您的人脸照片原始图像。

3、双方在履行本协议的过程中，如发生争议，应友好协商解决。协商不成的，任何一方均可向被告住所地有管辖权的人民法院提起诉讼。

4、特别提示：如您对本协议有任何疑问、意见或建议，可以通过以下方式联系我们：（1）客服热线 95016；（2）在线客服；（3）发送电子邮件至 info-sec@lakala.com。受理您的问题后，我们会及时、妥善处理。一般情况下，我们将在 15 个工作日内给予答复。

人脸信息属于敏感个人信息，处理活动对您个人权益影响重大，一旦泄露或者非法使用将可能对您的人身及财产安全造成危害。请您在点击“同意”之前仔细阅读本协议，确保对其内容特别是字体加黑内容的含义及相应法律后果已全部知晓并充分理解。您点击“同意”并确认提交即视为您接受本协议。