

# 浙商银行个人客户隐私政策

版本发布日期：2021年8月6日

版本生效日期：2021年8月6日

浙商银行股份有限公司（含业务经办机构、上级审批机构或管理机构，以下简称“本行”）本着业务必要、目的正当、明确授权、合法使用、保障安全等原则，致力于保护本行客户（简称“您”）的个人信息。

请您在注册及使用本行电子银行产品（或服务）及e家银小程序前，仔细阅读并确认本《隐私政策》。本《隐私政策》是本行电子银行及e家银小程序统一使用的一般性隐私条款，适用于本行门户网站、网上银行、浙商银行个人手机银行App（简称“个人手机银行App”）、微信银行、鸿蒙原子服务的产品和服务。本行将按照本《隐私政策》记录、存储、使用您的个人信息。为了保证对您的个人信息合法、合理、适度的记录、使用，请您仔细阅读本隐私政策并确认了解本行对您个人信息的处理规则。对本隐私政策中本行认为与您的权益存在重大关系的条款和个人敏感信息，本行采用粗体字进行标注以提示您特别注意。如您就本隐私政策点击或勾选“同意”并确认提交，即视为您同意本隐私政策。涉及具体的产品（或服务），本行记录和使用您个人信息的目的、方式和范围等还可能通过相应的产品（或服务）协议、

授权书等方式向您明示，并取得您的授权或同意，您有权针对本行具体产品（或服务）个人信息的处理表示拒绝。

本行不记录与业务无关的个人信息，不采取不正当方式记录个人信息，不变相强制记录个人信息。本行不以您不同意处理您的个人信息为由拒绝提供金融产品或者服务，但处理的金融信息属于提供金融产品或者服务所必需的除外。如您不能或者拒绝提供必要信息，致使本行无法履行反洗钱义务的，本行可根据《中华人民共和国反洗钱法》的相关规定对其金融活动采取限制性措施；确有必要时，本行可依法拒绝提供金融产品或者服务。

本《隐私政策》将帮助您了解以下内容：

- 一、本行如何记录和使用您的个人信息
  - 二、本行如何使用 Cookie 技术
  - 三、本行如何存储和保护您的个人信息
  - 四、本行如何共享、转让、公开披露您的个人信息
  - 五、您如何管理自己的个人信息
  - 六、本行如何处理未成年人的个人信息
  - 七、第三方使用您信息的情况
  - 八、本政策如何更新
  - 九、如何联系本行
- 一、本行如何记录和使用您的个人信息**
    - （一）本行如何记录您的个人信息**

为向您提供产品（或服务），并确保您在使用电子银行产品或服务（网上银行服务、手机银行服务、微信银行服务、浙商银行小程序服务、电话银行服务、自助设备服务、短信通知与验证服务）及 e 家银小程序时的安全，在您使用电子银行产品（或服务）及 e 家银小程序的过程中，本行会记录您在使用产品（或服务）过程中主动输入或因使用产品（或服务）而产生的信息：

1. 当您注册电子银行服务时，依据法律法规、监管部门、政府部门的规定本行会记录您的**手机号码、身份信息（比如您的身份证、军官证、护照等载明您身份的证件复印件或号码）、银行卡号**，并验证您的**银行卡密码**，以帮助您完成注册。若您已是本行电子银行注册客户则您可以使用电子银行注册手机号/卡（账）号/用户名直接登录，本行会记录您提供的登录信息并对信息进行验证核对。如您拒绝提供这些信息，您可能无法注册本行电子银行账号或无法正常使用本行的服务。

2. 当您使用本行电子银行产品或服务时，在下列情形中，您可能需要向本行提供或授权本行记录相应服务所需的用户信息，如您拒绝提供，您可能将无法使用相应功能或服务，但不影响您正常使用其他功能或服务。

（1）为了让您更安全、快速地登录个人手机银行 App，您可选择本行提供的**指纹、声纹、刷脸登录服务**，向本行提

供您的**指纹验证信息、声音或脸部图像信息**。您可通过“设置-登录管理-指纹/Face ID 登录、刷脸登录”开启或关闭此功能。

(2) 当您需要找回登录密码时，本行需要验证您的身份信息，包括**手机号码、短信动态码、证件类型、证件号码、银行卡号/账号、银行卡密码信息**。

(3) 当您使用本行消息提醒服务时，本行会记录您的**账户信息及交易信息**，以便及时向您发送账户资金变动及相关交易通知。

(4) 当您使用本行电子渠道提供的搜索服务时，本行会记录您的**搜索关键词信息**。当**搜索关键词信息**与您的其他信息结合可以识别您的个人身份时，本行将在此期间将您的**搜索关键词信息**作为您的用户信息，对其加以保护处理。

(5) 当您使用转账汇款付款功能时，您需要提供**收款方的姓名、银行卡卡号/账号、手机号码（当您需要把交易信息通知对方时）**。如您采用**刷脸、指纹**等生物识别方式办理转账汇款，系统将记录您相关生物信息。本行同时还会记录您的**相关收付款交易记录**以便于您查询。

(6) 当您使用个人手机银行 App、微信银行在商家进行消费时，本行需要按照法律法规、监管部门、政府部门的规定对商家进行防范套现或欺诈风险管理。因此，**本行将记录您的交易信息，包括交易金额、交易对象、交易商品、交易**

时间、订单信息（如有）。

（7）当您使用个人手机银行 App、微信银行、网上银行进行信用卡申请时，本行需要按照法律法规、监管部门、政府部门的规定记录您的相关信息，包括姓名、证件类型、证件号码、手机号码、联系地址。

（8）当您首次使用浙商银行小程序、e 家银小程序，或在浙商银行公众号绑定您的卡片信息时，本行需验证您的手机号、动态码、证件号码、账号、查询密码。

（9）当您使用账户开立、协议签约、工资提取、贷款申请功能或服务，为验证您的身份，确认您本人真实意愿，本行需要记录您的脸部图像信息、银行卡号、手机号码以及您录制的视频与声音。

（10）当您在个人手机银行 App、网上银行、自助设备开通并使用快捷支付功能时，本行需要您提供姓名、证件类型、证件号码、银行卡卡号、银行卡有效期、银行预留手机号信息，以便于验证身份。在您使用快捷支付功能时，本行需要记录您的交易信息以便于您查询。

（11）当您在个人手机银行 App 使用转账汇款、自助注册等需要验证手机动态码的特定业务场景时，本行需要通过运营商手机号认证服务，得知您正在使用个人手机银行 App 的手机号，作为您的登录信息；或通过运营商手机号认证服务，验证您正在使用个人手机银行 App 的手机号，是否和您

在本行预留手机号相符，用于核实您的身份，以保证您的信息和资金安全。

(12) 当您使用意见反馈功能提交意见建议时，本行会记录您提交的反馈意见和建议信息。

(13) 当您使用其他电子银行产品或服务时，本行会在渠道界面明示您需提供的信息，如您同意并提供，视为您授权本行记录、合理使用上述信息。

3. 当您使用电子银行产品或服务时，为了维护服务的正常运行，保障您的账号安全，本行会记录以下基础信息，包括您的设备型号、操作系统、唯一设备标识符、MAC 地址、手机银行软件版本号、登录 IP 地址、接入网络的方式、类型和状态、网络质量数据、设备加速器(如重力感应设备等)、操作日志、服务日志信息(如您在手机银行搜索、查看的信息、服务故障信息等日志信息)、地理位置信息、应用列表信息，这些信息是为您提供服务必须记录的基础信息，以保障您正常使用本行的服务。

4. 在向您提供服务的过程中，本行可能会使用具有相应业务资质及能力的第三方服务商提供的软件服务工具包(简称“SDK”)来为您提供服务，具体包括如下几种：

(1) 芯盾 SDK。当您使用设备绑定服务时，本行使用芯盾 SDK，该 SDK 需要获取您的手机终端唯一标志信息(IMEI 号)、电话权限、手机型号、系统类型、系统版本信息、地

理位置、IP 地址、设备信息、指纹、SIM 卡信息、网络信息、存储权限、MAC 地址、IMSI、UDID、UUID、IDFV、唯一设备标识符，用于实现设备绑定功能。

(2) 飞天诚信 SDK。当您使用 UKey 服务时，本行使用飞天诚信 SDK，该 SDK 需要获取您的蓝牙权限、(Android 需要定位权限、存储权限)、麦克风权限，用于使用 UKey 认证功能。

(3) 微博/腾讯 SDK。当您使用分享服务时，本行使用微博以及腾讯微信 SDK，用于实现一键分享功能。

(4) 手机号码认证 SDK。当您使用号码认证服务时，为了保障您的资金安全，防止账号被他人不法侵害，本行使用移动、联通、电信运营商提供的手机号认证 SDK，该 SDK 需要获取您的手机终端唯一标志信息 (IMEI)、IMSI、IDFV、存储权限、IP、设备信息、操作系统信息、网络类型信息、应用列表信息、SIM 卡信息、AndroidID、iOSBundleID，用于对手机号码进行认证。

(5) 神策 SDK。当您使用个人手机银行 App 时，为更好的为您服务，本行使用神策 SDK 对注册用户数、活跃用户数、启动次数、使用时长等行为做分析，该 SDK 需要获取您的 UUID、IDFA、IDFV、MAC 地址、唯一设备标识符、AndroidID、手机型号、系统类型、系统版本、网络类型、IP 地址、地理位置、设备信息、SIM 卡信息。

(6) 居民身份证网上功能凭证 SDK。当您使用网证服务时，为了便于您使用公安部第一研究所提供的“居民身份证网上功能凭证”（以下简称“网证”），本行使用居民身份证网上功能凭证 SDK，该 SDK 需要获取您的 UUID、AndroidID、iOSBundleID、存储权限、设备信息，以保障网证下载和存储的安全性。

(7) 一砂 SDK。当您使用指纹服务时，本行使用一砂 SDK，该 SDK 需要获取您的唯一设备标识符、iOSBundleID、手机型号、系统类型、指纹信息，用于指纹登录、支付等功能。

(8) 旷视 SDK。当您使用刷脸服务时，本行使用旷视 SDK，该 SDK 需要获取您的相机权限、存储权限、人脸信息，用于人脸识别服务。

(9) 科大讯飞 SDK。当您使用语音搜索、语音转账的语音文本识别服务时，本行使用科大讯飞 SDK，该 SDK 需要获取您的语音信息、存储权限、IP 地址、网络类型、UUID、麦克风权限，用于实现语音识别功能。

(10) 小米/华为/魅族推送 SDK。当您使用推送服务通知时，本行使用小米/华为/魅族推送 SDK，该 SDK 需要获取您的手机终端唯一标志信息（IMEI 号）、地理位置、存储权限、手机型号、IP 地址、设备信息、电话权限、UUID、MAC 地址、操作系统版本、AndroidID、iOSBundleID、Topic 订



阅、网络类型信息、SIM卡运营商、系统类型，用于实现App推送服务。

(11) 百度定位 SDK。当您使用网点查询、网点预约的基于位置的服务时，本行使用百度定位 SDK，该 SDK 需要获取您使用我行服务时的经纬度信息、蓝牙、麦克风、相机、设备信息、手机终端唯一标志信息、MAC 地址、IP 地址、定位权限、UUID、唯一设备标识符、操作系统信息、AndroidID、iOSBundleID、网络类型信息，用于实现定位功能。

(12) 腾讯 X5 SDK。当您使用浏览文件的服务时，本行使用腾讯 X5 SDK，该 SDK 需要获取您的手机存储权限、设备信息、系统类型、网络类型、IMEI、IMSI、MAC 地址、操作系统版本，用于查看浏览器（PDF，H5）的功能。

(13) Google 开源 zxing 开源包 SDK。当您使用相机扫描服务时，本行使用 Google 开源 zxing 开源包 SDK，该 SDK 需要获取您的相机权限、存储权限，可从相册选择二维码，用于使用二维码扫一扫功能。

(14) 银联 SDK。当您使用银联支付服务时，本行使用银联 SDK，该 SDK 需要获取您的地理位置、设备信息、网络类型，用于集成银联 HCE、无卡支付功能。

(15) 电子社保 SDK。当您使用电子社保卡的服务时，本行使用电子社保 SDK，该 SDK 需要获取您的姓名、手机号、证件号、手机系统版本号、手机厂商及型号、设备信息、设

备唯一 id、地理位置、相机、相册、存储信息、电话权限、网络环境、人脸、UUID、AndroidID 信息用于电子社保卡申领和查询服务。

(16) 云证通（中国金融认证中心 CFCA）SDK。当您使用云证通电子签名服务时，本行使用云证通（中国金融认证中心 CFCA）SDK，该 SDK 需要获取唯一设备标识符、设备厂商、设备型号、设备状态信息、设备制造商、操作系统版本号、AndroidID、MAC 地址，用于实现电子签名服务。

(17) 梆梆 SDK。当您使用个人手机银行 App 时，为了向您提供安全的 App 服务，本行使用梆梆 SDK，用于防止安卓 App 被破解、反编译、二次打包等威胁，该 SDK 获取您的系统悬浮窗权限信息。

(18) 文鼎创 SDK。当您使用蓝牙 UKey 服务时，本行使用文鼎创 SDK。该 SDK 需要获取您的地理位置、蓝牙、存储权限、设备信息、操作系统信息，用于实现蓝牙 UKey 验证功能。

(19) 微信登录 SDK。当您使用微信账号登录服务时，本行使用微信登录 SDK，该 SDK 需要从微信获取您授权共享的账户信息（头像、昵称、地区、性别），用于集成微信账号登录功能。

(20) 佰锐 SDK。当您使用在线营业厅服务时，本行使用佰锐 SDK。该 SDK 需要获取您的存储、麦克风、相机权限，

用于视频语音或保存视频文件及截图文件功能。

如您不同意上述第三方服务商记录前述信息，可能无法获得相应服务，但不影响您正常使用个人手机银行 App 的其他功能或服务。如您同意上述相关第三方服务商记录前述信息，若由第三方发生信息泄露的，由相关第三方服务商承担相应的法律责任，本行将积极提供必要协助。

5. 以下情形中，您可通过开启（关闭）您设备的相应权限实现对本行记录、处理您个人信息的授权（拒绝授权）：

（1）**设备状态**，用于确定设备识别码，以保证账号登录的安全性。如您拒绝授权，将无法登录相应 App，但这不影响您使用本行 App 用户未登陆状态下可用的功能。

（2）**存储权限**，用于缓存您在使用个人手机银行 App 过程中产生的文本、图像、视频等内容，如您拒绝授权，将无法登录个人手机银行 App，但这不影响您使用本行 App 用户未登陆状态下可用的功能。

（3）**摄像头**，如您开启该权限（同意授权），本行仅在使用扫一扫、刷脸登录/支付/转账/提升认证、上传身份证、识别银行卡、录像场景功能中使用摄像头。拒绝授权后，上述功能将无法使用。

（4）**相册**，如您开启该权限（同意授权），本行仅在电子回单保存、银行卡及身份证识别、分享功能中使用相册权限，获得的图片信息，加密后存储于数据库中。拒绝授权

后，上述功能将无法使用。

(5) **麦克风**，如您开启该权限（同意授权），本行仅在音频 UKey、语音搜索、语音转账服务中使用麦克风。拒绝授权后，上述功能将无法使用。

(6) **手机通讯录**，如您开启该权限（同意授权），本行仅在手机号转账、话费充值功能中，询问是否允许获取您的手机通讯录权限用于协助您通过通讯录快速选取电话号码而无需您手动输入。拒绝授权后，上述功能仍可使用，但需要手工输入手机号码。

(7) **地理位置**，如您开启该权限（同意授权），本行仅在网点查询、预约取号、城市定位、生活缴费功能中获取您所在的**地理位置**。本行系统后台保存您交易时**位置**信息。拒绝授权后，上述功能可能无法正常使用。

(8) **蓝牙**，用于蓝牙 UKey 服务，通过蓝牙将客户手机与第三方设备连接并交互。拒绝授权后，无法通过蓝牙激活第三方设备。本行系统后台不保存客户手机蓝牙配置信息。

(9) **网络通讯**，用于与服务端进行通讯。拒绝授权后，手机银行所有功能无法使用。本行系统后台保存客户交易时所使用设备的网络信息，包括 IP、端口信息。

(10) **剪切板**，用于转账快捷跳转、搜索粘贴识别功能，本行系统后台不保存您的剪切板内容。如您拒绝授权剪切板权限，本行手机银行将不读取剪切板内容，不影响您正常使

用个人手机银行 App 的其他功能。

(11) NFC (近距离无线通信技术)，用于银联 HEC 场景 (银联云闪付) 中使用。如您拒绝授权 NFC 权限，将无法使用**银联 HEC** 功能，但不影响您正常使用个人手机银行 App 的其他功能。

上述功能可能需要您在您的设备中向本行开启您的设备、存储空间、相机 (摄像头)、相册 (图片库)、地理位置 (位置信息)、麦克风、蓝牙、通讯录、网络通讯的访问权限，以实现这些功能所涉及的信息的记录和使用。请您注意，您开启这些权限即代表您授权本行可以记录和使用这些信息来实现上述功能，如您取消了这些授权，则本行将不再继续记录和使用您的这些信息，也无法为您提供上述与这些授权所对应的功能。

6. 当您首次个人手机银行 App 上进行人脸识别以核实身份时，本行会采集您的人脸信息，并将加密后存储于系统后台数据库中，用于业务办理过程留存、辅助识别和核实身份。对于某些品牌或型号的手机终端自身的本地生物特征认证功能，如人脸识别功能，其信息由手机终端提供商进行处理，本行不留存您应用手机终端相关功能的信息。

## 7. 其他

本行在向您提供其他产品或服务时，会另行向您说明信息记录的范围与目的，并征得您的同意后，方记录提供相应

服务所必要的您的信息。本行会按照本政策以及相应的产品（或服务）协议、授权书等使用、存储、对外提供及保护您的信息；如您选择不提供前述信息，不会影响您使用电子银行其他服务功能。

## （二）本行如何使用用户信息

1. 在向您提供本行的金融产品或服务时使用。

2. 为了使您知晓使用个人手机银行 App 服务的状态，本行会向您发送**服务提醒**。您可以通过手机系统设置中的通知设置关闭服务提醒，也可以通过通知设置重新开启服务提醒。

3. 为了保障服务的稳定性与安全性，本行会将您的信息用于身份验证、安全防范、诈骗监测、预防或禁止非法活动、降低风险、存档和备份用途。

4. 根据法律法规、监管部门、政府部门的要求向相关部门进行报告。

5. 在记录您的个人信息后，本行可能通过技术手段对您的信息数据进行去标识化处理，去标识化后的信息将无法识别信息主体。对该类去标识化的信息，您同意本行可直接使用并对用户数据库进行分析、使用，而无需获得您的授权。

6. 本行会对本行提供的金融服务和功能的使用情况进行统计，并可能会与公众或第三方共享这些统计信息，以展示本行的服务或功能的整体使用情况。但这些统计信息不包

含您的任何身份识别信息。

7. 当本行展示您的信息时，本行会采用包括内容替换、匿名化处理方式对您的信息进行脱敏，使这些信息不包含您的任何身份识别信息，以保护您的信息安全。

### （三）征得授权同意的例外

根据相关法律法规、监管部门及国家标准，在以下情形中，本行可能会依法记录并使用您的个人信息而无需征得您的同意：

1. 与国家安全、国防安全直接相关的。
2. 与公共安全、公共卫生、重大公共利益直接相关的。
3. 与犯罪侦查、起诉、审判和判决执行等直接相关的。
4. 所记录的个人信息是您自行向社会公众公开的且本行对该个人信息的使用符合该个人信息被公开时的用途。
5. 从合法公开披露的信息中记录个人信息，例如：合法的新闻报道、政府信息公开等渠道，且本行对该个人信息的使用符合该个人信息被公开时的用途。
6. 用于查找、预防或处理欺诈、安全或技术方面所必须。
7. 在法律法规要求或允许的范围内，保护生命、重大财产等重大合法权益免遭损害，但又无法即时得到您本人同意的。（事后本行会尽可能地补充通知您，且您可联系本行提出对信息进行删除等处理的相关要求。）
8. 法律法规、监管部门、政府部门规定的其他情形。

#### （四）本行从第三方获取您个人信息的情形

当您将第三方账户与您的个人手机银行 App 用户绑定时，如您希望通过第三方账户直接登录并使用本行的产品或服务，本行可能需从第三方（如微信、苹果、华为）获取您授权共享的账户信息（如头像、昵称）。

## 二、本行如何使用 Cookie 技术

为确保服务正常运转，本行会在您的计算机、移动设备上存储名为 Cookie 的小数据文件。Cookie 通常包含标识符、站点名称以及一些号码和字符。借助于 Cookie，网站和 App 能够存储您的偏好数据。本行不会将 Cookie 用于本政策所屬目的之外的任何用途。您可根据自己的偏好管理或删除 Cookie。您可以清除计算机或移动设备上保存的所有 Cookie，大部分网络浏览器都设有阻止 Cookie 的功能。但如果您这么做，则需要在每一次访问网站、个人手机银行 App 时更改用户设置。

## 三、本行如何存储和保护用户信息

### （一）存储

1. 您在国内或国外访问和使用本行电子渠道，所产生的个人信息将存储在中华人民共和国境内。

2. 本行仅在法律法规、监管部门、政府部门的规定要求的期限内，以及为实现本政策声明的目的所必须的期限内保留您的个人信息。例如：手机号码：当您需要使用手机银行



服务时，本行需要**持续保存您的手机号码**，以保证您正常使用该服务。

## （二）保护

1. 本行已使用符合业界标准的安全防护措施保护您提供的个人信息，防止数据遭到未经授权的访问、公开披露、使用、修改、损坏或丢失。本行会采取一切合理可行的措施，保护您的个人信息。例如：本行会使用加密技术确保数据的保密性；本行会使用受信赖的保护机制防止数据遭到恶意攻击；本行严格执行访问控制机制，确保只有授权人员才可访问个人信息。

2. 如本行提供的全部或部分浙商银行电子银行业务停止运营，本行将通过公告等形式向您告知，同时停止相关产品或服务对您个人信息的记录等操作，保护您的个人信息安全。如因技术故障、网络攻击、自然灾害及事故、人为因素等各种原因造成全部或部分浙商银行电子银行业务中断，本行将采取应急处置和恢复措施予以应对，尽快恢复服务。

3. 如发生个人信息安全事件，本行将按照法律法规的要求，及时采取措施进行化解，同时将事件相关情况通过邮件、信函、电话、推送通知等方式中的一种或多种告知您，或采取合理方式发布公告。同时，本行还将依据监管规定，上报个人信息安全事件处置情况。

**4. 请您理解，由于各种因素有可能出现本行无法合理预**

见、防范、避免、控制的意外情况。互联网并非绝对安全的环境，请使用复杂密码，协助本行保证您的账户安全。

#### 四、本行如何共享、转让、公开披露您的个人信息

##### （一）共享

本行不会向其他任何公司、组织和个人共享您的个人信息，但以下情况除外：

1. 如确因业务需要对外共享您的个人信息，本行会事先征得您的明示同意，并向您告知共享个人信息的目的、数据接收方的类型。涉及敏感信息的，本行还会告知您敏感信息的类型、数据接收方的身份，并事先征得您的明示同意。

2. 请您理解，本行可能会根据法律法规、监管部门、政府部门的规定及要求，共享您的个人信息。

3. 对本行与之共享个人信息的公司、组织和个人，本行会与其签署保密协议，要求他们按照本行的说明、本政策或其他任何相关的保密和安全措施来妥善处理个人信息。

4. 本行会对合作方获取有关信息的应用程序接口（API）、软件工具开发包（SDK）进行严格的安全检测，并与合作方约定严格的数据保护措施，令其按照本行的委托目的、服务说明、本隐私政策以及其他任何相关的保密和措施来处理个人信息。

5. 为向您的移动设备发送账户资金变动及相关交易通知，本行在征得您明示同意后，可能会向合作方（主要是推

送服务或移动设备厂商)提供您的部分账户信息及交易信息。

6. 当您在本行开展贷款或者担保等信用业务时,在获得您的明示授权后,本行会向依法设立的征信机构及其他相关合法机构查询、使用或提供您的信用、资产信息。本行依法对您的相关信息承担保密责任,并要求合作机构对您的相关信息承担保密责任。

## (二) 转让

1. 事先获得您的明确同意。

2. 根据法律法规或强制性的行政或司法要求。

3. 根据法律法规、监管部门、政府部门的规定和商业惯例,在合并、收购、资产转让中,如涉及到个人信息转让,本行会要求新的持有您个人信息的公司、组织继续受本隐私政策的约束,否则本行将要求该公司、组织重新向您征求授权同意。

## (三) 公开披露

1. 本行不会公开披露您的个人信息,如确需披露,本行会征求您的授权同意,并告知您披露个人信息的目的、类型。

2. 请您理解,在法律法规、监管部门、政府部门等强制性要求的情况下,本行可能会公开披露您的个人信息。

## (四) 征得授权同意的例外

根据相关法律法规、监管部门、政府部门的要求、国家

标准，以下情形中，本行可能会共享、公开披露用户信息无需事先告知或征得您的授权同意：

1. 与国家安全、国防安全直接相关的。
2. 与公共安全、公共卫生、重大公共利益直接相关的。
3. 与犯罪侦查、起诉、审判和判决执行等直接相关的。
4. 出于维护您或他人的生命、财产等重大合法权益但又无法即时得到您本人同意的，事后会尽可能的补充通知您，且您可联系本行提出对您的信息进行删除等处理的相关要求。

5. 所记录的个人信息是您自行向社会公众公开的且本行对该个人信息的使用符合该个人信息被公开时的用途。

6. 从合法公开披露的信息中记录个人信息，例如：合法的新闻报道、政府信息公开等渠道，且本行对该个人信息的使用符合该个人信息被公开时的用途。

7. 法律法规、监管部门、政府部门规定的其他情形。

## 五、您如何管理用户信息

按照我国相关的法律法规、监管部门、政府部门的規定，本行保障您对自己的个人信息行使以下权利：

### （一）访问、管理您的个人信息

您有权通过本行营业网点、网上银行、个人手机银行App、微信银行、电话银行等渠道查询或根据各渠道的功能，更正、更新您的个人信息，法律法规、监管部门、政府部门

另有规定的除外。为了获得更完整的服务功能，请您及时更新您的个人信息。在您修改个人信息之前，本行会验证您的身份。

您登陆个人手机银行 App 后，可以在“设置”中，进行个人信息设置、登录设置、支付设置、限额设置、安全设置。

个人信息设置--为客户提供居住地址、工作信息的修改功能，并可修改预留手机号，可下载身份证网证。支持查询个人基本信息及客户经理、电子银行注册信息。

登录设置--可对手势登录、微信登录、刷脸登录、FaceID 登录、登录密码进行设置。

支付设置--可对指纹支付、刷脸转账、快捷支付、银联支付授权管理、刷脸付进行设置。

限额设置--可对转账限额、扫码/取款限额、ATM/POS 限额、银联免密免签、银联在线支付限额、云闪付支付限额进行设置。

安全设置--为客户提供多种使用个人手机银行 App 的安全服务，确保银行账户的安全。主要功能包括：密码管理、账户安全（借记卡、信用卡的账户管理操作）、UKey 管理、云证书管理、设备与应用管理。

## （二）删除您的个人信息

您在本行的产品或服务页面中可以直接删除的信息，包括绑定的银行卡（点击“账户管理-账户删除”来删除绑定

的二、三类账户）、消息记录（点击“消息中心-清空消息”来删除消息记录）、意见反馈记录（点击“意见反馈-我的意见”中的删除按钮删除）。当您从本行的服务中删除信息后，本行可能不会立即在备份系统中删除相应的信息，但会在备份更新时删除这些信息。

如您发现本行记录、使用您个人信息的行为，违反了法律法规规定或违反了与您的约定，您可联系本行，要求删除相应的信息。

如本行决定响应您的删除请求，本行还将同时通知从本行获得您个人信息的第三方，要求其及时删除，除非法律法规另有规定，或这些实体获得您的独立授权。

### （三）改变您授权同意的范围或撤回您的授权

您可以通过手机系统权限设置、个人手机银行 App 的“设置-安全中心-设备与应用管理-App 应用权限”功能改变部分您授权本行继续记录个人信息的范围或撤回您的授权。但您撤回同意的决定，不会影响此前基于您的授权而开展的个人信息记录。

您可通过“设置”中的“隐私政策”功能，查看当前的隐私政策或者撤销同意隐私政策。撤销同意政策将在下次启动后生效，不影响本次登录过程中个人手机银行 App 的使用。撤销后如您之后仍需使用个人手机银行 App，请在下次启动 App 时查看并同意隐私政策使用。

#### （四）注销电子渠道用户

如您为本行网上银行或手机银行用户，您可以通过本行网上银行或个人手机银行 App 注销您相应渠道的用户。您注销电子银行用户的行为是不可逆行为，一旦您注销该渠道的用户，本行将无法继续通过该渠道记录您的个人信息。

您可以自主选择卸载或停止使用个人手机银行 App 客户端，以阻止本行获取您的个人信息。请您注意，仅在手机设备中删除个人手机银行 App 时，本行不会注销您的电子银行用户。

登录个人手机银行 App 后，您可通过在“设置-安全中心-注销手机银行”的方式进行注销手机银行操作。您也可登录个人网银，在“设置-渠道设置-我的手机银行-注销”进行注销手机银行操作。

#### （五）响应您的上述请求

为保障安全，您可能需要提供书面请求，或以其他方式证明您的身份。本行可能会先要求您验证自己的身份，然后再处理您的请求。请您理解，对于某些无端重复、给他人合法权益带来风险或者非常不切实际的请求，本行可能会予以拒绝。若系统未及时响应您的相应操作，需人工处理的，本行会在承诺时限内（承诺时限不得超过 15 个工作日，无承诺时限的，以 15 个工作日为限）完成核查和处理。

尽管有上述约定，但按照法律法规要求，如涉及以下情形本行将可能无法响应您的请求：

1. 与国家安全、国防安全相关的。
2. 与公共安全、公共卫生、重大公共利益相关的。
3. 与犯罪侦查、起诉、审判和判决执行等相关的。
4. 有充分证据表明您存在主观恶意的。
5. 涉及本行商业秘密的。
6. 其他按照法律法规规定无法响应的合理情形。

#### 六、本行如何处理未成年人信息

如果没有监护人的同意，未成年人不得创建自己的用户账户。如您为未成年人，请您的监护人仔细阅读本指引，并在征得您的监护人同意的前提下使用本行的服务或向本行提供信息。对于经监护人同意而记录的您的个人信息，本行只会在法律法规、监管部门、政府部门允许、监护人明确同意或者保护您权益所必要的情况下使用。

#### 七、第三方使用您信息的情况

当您在个人手机银行 App 中使用第三方提供的服务时，第三方可能获取您的部分个人信息及其他提供第三方服务所必须的信息，如 e 家银商城（手机号、证件类型、证件号码）、医保电子凭证（证件类型、证件号码、姓名、手机号、人脸照片）、银联授权支付（证件号码、证件类型、卡号、卡有效期）、银联相关如信用卡（证件号码、证件类型、姓



名、卡号、家庭地址、工作地址)；在经过您的明示授权后，第三方可获取您的以上信息。如您拒绝第三方在提供服务时使用或者传递上述信息，可能导致您无法在个人手机银行 App 中使用该第三方的相应服务，但这不影响您使用个人手机银行 App 的其他功能。

对于您在使用第三方提供的服务时主动提供给第三方的相关信息，本行将视为您允许该第三方获取上述此类信息；对于您在使用第三方服务时产生的信息，请您与该第三方自行依法约定上述信息的使用事项。

您理解，第三方提供的服务由该第三方独立运营并独立承担全部责任。因第三方所提供的服务或其使用您的信息产生的纠纷，或其违反相关法律法规或本隐私政策约定，或您在使用其服务过程中遭受的损失，请您与该第三方协商解决。对于需由第三方解决的问题，本行将尽商业上的合理的努力推动第三方解决。

## 八、本政策如何更新

根据国家法律法规、监管部门、政府部门的规定变化及服务运营需要，本行可能会对本政策及相关规则不定期地进行修改，修改后的内容会通过本行门户网站、网上银行、手机银行渠道公布。建议您关注本行相关公告、提示信息及协议、规则等内容的变动。本政策更新后，个人手机银行 App 将在启动使用 App 时提示您再次确认同意。您知悉并确认，

如您不同意更新后的内容，应立即停止使用相应服务；如您继续使用本行产品（或服务），即表示您已充分阅读、理解并愿意受更新后的政策约束。涉及整合、下线等此类对您的权利产生重要影响的，本行将增选短信、电话等方式进行补充通知。

## 九、如何联系本行

如您对本隐私政策有任何疑问、意见或建议，请联系本行全国统一服务电话 95527，官方网站（WWW.CZBANK.COM），个人手机银行 App “在线客服”、“意见反馈”（该方式仅支持开通本行手机银行或网上银行的客户），微信公众号的“在线客服”以及本行各营业网点进行咨询或反映。本行会及时处理您的意见、建议及相关问题。

本行设有个人信息保护工作人员，您可以通过发送邮件至 [95527@czbank.com](mailto:95527@czbank.com) 的方式与其联系。

一般情况下，本行将在十五个工作日内回复。如果您对我们的答复不满意，特别是如果您认为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、公安及市场监管等监管部门进行投诉或举报，您还可以通过向被告住所地有管辖权的法院提起诉讼来寻求解决。

请您在勾选“同意”之前仔细阅读本《隐私政策》，确保对其内容特别是字体加黑内容的含义及相应的法律后果已全部知晓并充分理解。您勾选“同意”并确认提交即视为

您接受本《隐私政策》并给予本行相应授权，本行将按照相关法律法规、监管部门、政府部门的规定及本政策来记录、使用、存储和保护您的个人信息。

公司名称：浙商银行股份有限公司

注册地址：中国浙江省杭州市萧山区鸿宁路 1788 号