浙商银行股份有限公司隐私及数据安全管理政策制度要点（2025年版）

一、目的

浙商银行股份有限公司（以下简称“浙商银行”“本行”）高度重视客户隐私及数据安全管理，致力于维护本行与客户之间的信任。本行严格遵守《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国消费者权益保护法》《网络数据安全管理条例》《中国人民银行业务领域数据安全管理办法》《银行业保险业数据安全管理办法》等法律法规和监管制度，制定《浙商银行数据安全管理办法》《浙商银行信息系统生产数据索取管理办法》《浙商银行外部数据管理办法》《浙商银行个人App用户隐私政策》《浙商银行个人网银用户隐私政策》《浙商银行小程序个人客户隐私政策》等管理制度，遵循合法、正当、必要、诚信原则处理数据与客户信息，切实保障客户个人隐私的安全。

二、适用范围

本政策适用于浙商银行总行及境内各级机构全部业务条线，以及向客户提供的所有产品和服务。

三、管理架构

本行建立与业务发展目标相适应的数据安全治理体系及管理制度，构建覆盖数据全生命周期和应用场景的安全保护机制，以保障本行数据安全。

本行实施数据安全责任制。总行党委、董事会对本行数据安全工作负主体责任。总行党委书记、董事长为本行数据安全第一责任人，分管数据安全的领导班子成员为本行数据安全直接责任人。各级机构各部门主要负责人是第一责任人，分管数据安全负责人是直接责任人，逐级压实责任。

董事会负责指导、督促高级管理层有效执行和落实数据安全工作。高级管理层及下设信息科技管理委员会、数据治理委员会负责组织建设数据安全治理体系、落实数据安全管理工作，审议数据安全管理流程及制度，审批与数据安全相关的重大事项，指导、协调突发性数据安全事件的应急处置。总行科技管理部及其次一级部门数据管理部、科技研发部、系统运行部负责数据安全归口管理和数据安全技术保护。总行条线管理部门、党委宣传部、风险管理部、内控合规与法律部、社会责任与消费者权益保护部、审计部等负责履行各自的数据安全管理职责。

四、定义

数据：是指任何以电子或者其他方式对信息的记录，由一条

或多条记录组成，每条记录对应的数据结构可以是单一数据项或者多个数据项的组合。

数据处理：是指对数据的收集、存储、使用、加工、传输、提供、共享、转移、公开、删除、销毁等。

个人信息：是指个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

个人信息的处理：包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

敏感个人信息：是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

五、数据安全管理

（一）数据安全管理原则

本行数据安全管理以保护国家安全、政治安全、金融安全、公共利益，保障本行、客户、其他组织的合法权益为目标，遵循“依法合规，分类分级，最小够用，全程可控，动态控制，全员参与”的原则。

依法合规原则：开展数据处理活动，应遵守法律法规，尊重

社会公德和伦理，遵守商业道德和职业道德，诚实守信。

分类分级原则：根据数据安全级别，明确优先级，合理规划、分配资源。

最小够用原则：仅处理满足数据处理目的所需要的最少数据类型和数量，杜绝过度收集、误用、滥用数据。

全程可控原则：采取与数据安全级别相匹配的安全管控机制和技术措施，确保数据在全生命周期各环节的保密性、完整性和可用性。

动态控制原则：数据安全控制策略和安全防护措施应基于业务需求、安全环境属性、系统用户行为、数据规模等因素实施实时和动态调整。

全员参与原则：数据安全管理是全行每个部门、每位员工的基本职责之一。

（二） 数据保护措施

1.将数据保护融入产品和服务开发

本行通过建立事前风险评估机制、强化开发阶段安全管控、严格隔离开发测试环境数据、规范人工智能模型部署等全流程措施，将数据保护融入产品和服务开发，确保数据安全保护措施贯穿业务全过程。

一是建立事前评估机制，涉及敏感数据的产品和信息系统设

计前，开展数据安全事项风险评估和个人信息保护影响评估。评估内容包括数据处理的合法性、必要性，对个人权益的影响及安全风险，所采取的保护措施合法性、有效性以及是否与风险程度相适应。

二是在系统开发阶段，开展架构技术评审、安全需求澄清和安全测试，保障数据保护措施落实到位。评审和测试内容包括数据加密、敏感数据脱敏、用户权限管控等技术措施，个人金融信息保护开发安全规范要求落实情况，危害数据安全漏洞处置等。

三是采用技术措施确保开发测试环境数据与生产环境数据的有效隔离；敏感级及以上数据原则上未经脱敏处理不进入开发测试环境，因特殊原因无法脱敏处理的，履行审批手续，严格控制数据的获取和使用范围、使用对象、使用期限及数据总量等，并采取与生产环境一致的安全保护管理和技术措施，确保开发测试数据安全。

四是在人工智能模型研发过程进行主动管理，人工智能模型采用本地化方式部署，本行数据不会用于外部人工智能模型训练、测试或验证等。

2.访问控制/加密技术

本行建立覆盖网络、邮件、终端的数据防泄露体系，配置内网数据外发加密（RSA+AES 算法）、敏感数据外发审批、征信

数据外发阻断的管控策略，通过正则表达式、关键字、文件名等识别规则，对通过电子邮件、物理介质等方式向外传输的文件进行扫描和拦截，防范数据泄露。

针对敏感级及以上数据的访问，落实权限管理、访问控制、加密、脱敏或过程监督检查等措施。一是部署数据脱敏工具和API动态脱敏系统，通过敏感字段扫描、识别，及加密、替换、掩码屏蔽等技术对敏感数据进行脱敏，针对用户角色配置脱敏策略，从接口侧控制敏感数据访问，落实业务应用系统数据展示动态脱敏和安全管控。二是建设统一身份认证系统，统一管控业务系统用户，通过实名认证绑定、分级授权、权限管控、访问IP控制等措施，防范非授权访问，落实数据访问闭环管理，并对生产环境等重点场景数据访问行为实施检查或审计，保障使用过程中数据的安全性。

3.数据泄露风险管理

本行为应对数据泄露风险，采取数据安全风险评估、外部数据安全风险隔离、数据安全风险监测等主动措施。本行制定《浙商银行数据安全应急预案（2025年版）》，建立数据安全事件应急管理机制，各级机构组织协调，联动子公司、服务提供商、第三方合作机构，及时有效、妥善处置风险隐患及安全事件。

主动措施:

本行在处理对数据主体有较大影响的活动时，事先开展数据安全风险评估。数据安全评估根据数据处理目的、性质和范围，按照法律法规和伦理道德规范要求，分析数据安全风险和对数据主体权益影响，评估数据处理的必要性、合规性，评估数据安全风险及防控措施的有效性。

在与第三方数据合作时，本行落实与外部的安全风险隔离，与外部机构的数据交互通过集中管理的OPENAPI接口或银企直联技术实施，依据“业务必需、最小权限”原则，采取有效措施对接口设计、开发、服务、运行等进行安全管理。

建立覆盖全行各级机构的数据安全风险监测、预警、评估、响应、通报与处置的组织架构和管理流程，对数据安全风险进行有效监测，主动评估风险，防止数据篡改、破坏、泄露、非法利用等安全事件发生。

数据安全归口管理部门制定并发布全行数据安全事件总体应急预案，定期开展应急响应培训和应急演练。各分行建立分行本级信息科技事件应急管理机制，根据当地实际，制定本机构数据安全事件应急报告流程和应急联系人名单，并通过测试、演练等方式验证数据安全事件应急处置的有效性。

被动措施:

发生数据安全事件后，各级机构启动信息科技事件报告机制，

根据事件安全等级，在发生事件2小时内口头向监管机构报告，发生事件24小时内提交正式书面报告。同时按照合同、协议等有关约定履行客户及合作方告知义务。发生特别重大数据安全事件时，每2小时将处置进展情况上报，直至处置结束。发生或者可能发生个人信息泄露、篡改、丢失的，除立即采取补救措施外，同时通知个人，并根据监管要求报送当地监管机构。通知内容包括发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；本行采取的补救措施和个人可以采取的减轻危害的措施。数据安全事件处置结束后，在五个工作日内将事件及其处置的评估、总结和改进报告报送监管机构。

发生数据安全事件或使用的网络产品和服务存在安全缺陷、漏洞时，本行将立即开展调查评估，及时采取补救措施，防止危害扩大，并要求网络产品和服务提供商进行改正。

六、客户信息的收集、使用和留存

（一）客户信息的收集和使用

本行承诺不会从第三方收集个人数据（经本人同意或法律另有要求的除外）。本行收集个人信息的方式包括：

1.提供金融服务时，客户主动提供的信息，包括：业务办理填写、授权同意书签署等。

2.客户业务办理过程中自动采集的信息，包括：交易行为数

据、设备与环境信息、生物识别验证结果等。

3.第三方机构信息共享，包括：向征信机构、信用管理公司、资信评估机构或有关法律、监管机构许可的类似机构收集客户的信用信息和行为信息；向政府机构、司法机关及公共事业单位收集与服务相关的必要信息；经客户授权，向合法留存客户信息的自然人、法人以及其他组织收集与本行提供的服务相关的必要信息；法律、行政法规规定的或经客户许可的其他方式。

4.技术手段自动化收集，包括：Cookie 与日志分析、数据资产扫描工具、风控系统监测等。

本行收集个人信息限于实现金融业务处理目的的最小范围，不过度收集个人信息，不利用所收集的个人信息从事违法违规活动。处理个人信息前，将真实、准确、完整地向个人告知其个人信息的处理目的、处理方式、处理的个人信息种类、保存期限，个人行使其信息权利的申请受理和处理程序，以及法律法规规定应当告知的其他事项，并以清单等形式列明收集和对外提供个人信息的目的、方式、种类以及数据接收方信息。

（二）客户信息的留存

本行承诺不会出于完成交易/服务以外的目的向第三方出租、出售或提供个人数据。委托第三方处理个人信息时，在合同或者协议条款内明确受托方对个人信息的保护义务、保护措施、期限

以及未经本行同意受托方不得转委托他人处理个人信息等，并严格监督受托方以约定的处理目的、处理方式等处理个人信息，与第三方传输个人敏感数据采用数据加密、安全信道等措施确保安全，防范数据滥用和泄露风险。

本行按照国家、行业有关规定及与客户的约定进行客户个人信息删除或匿名化处理，达到使用期限的及时进行删除与销毁。

七、客户对个人信息的控制

银行客户对个人信息的控制权核心体现为访问权、修改权、删除权三项基本权利，其实现方式、法律依据及实操限制如下:

（一）客户对个人信息的获取/访问权

1.客户可以通过本行柜面、手机银行 App 渠道查询个人信息。

客户登录手机银行 App 后，可以在“全部-设置”中，进行个人信息查询。“全部-设置-个人中心”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。上述操作本行将实时满足客户的请求。

2.客户可以通过以下路径获取客户的个人信息副本。

客户可以登录浙商银行手机银行 App 进入“设置-个人中心”，获取客户的姓名、证件类型、证件号码、国籍、性别、手机号码、证件到期日、经常居住地、职业、工作单位（如客户已经录入）;

登录浙商银行个人网银进入“设置-客户信息管理”获取个人信息；如客户需要个人信息的副本，可以通过本政策文末提供的方式联系本行，在核实客户的身份后，本行将向其提供在本行的服务中的个人信息副本（包括基本资料、身份信息），但法律法规另有规定的或本政策另有约定的除外。

（二）客户对个人信息的修改权

客户有权通过本行柜面、手机银行 App 渠道更正、补充、更新个人信息，法律法规、监管部门及政府部门另有规定的除外。客户有责任及时更新客户的个人信息，在修改个人信息之前，本行会验证其身份。

如客户觉得客户的其他个人信息不完整或不准确，也可以联系本行，本行将验证客户的身份并及时更正、补充客户的个人信息。

（三）客户对个人信息的删除权

在符合法律法规规定的情形下，客户有权要求银行删除其个人信息：

1.如果本行处理个人信息的行为违反法律法规；

2.如果本行收集、使用客户的个人信息，却未征得客户的同意；

3.如果本行处理个人信息的行为违反了与客户的约定；

4.如果客户不再使用本行的产品或服务，或客户注销了手机银行 App 账号;

5.如果本行不再为客户提供产品或服务。

如本行决定响应客户的删除请求，本行还将同时通知从本行获得客户的个人信息的实体，要求其及时删除，除非法律法规、监管部门及政府部门另有规定，或这些实体另行获得客户的单独授权。

当客户从本行的服务中删除个人信息后，本行可能不会立即在备份系统中删除相应的个人信息，但会在备份更新时删除这些个人信息。在个人信息未删除前，本行将停止除存储和采取必要的安全保护措施之外的处理。

八、能力建设

（一）员工隐私及数据安全培训

本行由总行科技管理部负责定期组织开展数据安全宣贯培训，提升员工数据安全保护意识与技能，培训覆盖本行所有员工（包含劳动合同工、劳务派遣工以及兼职员工），培训内容包括数据安全制度解读、个人信息保护案例、常见数据安全风险与防控对策等，定期组织全行人员签订《浙商银行网络与数据安全工作责任书》。各级机构对涉及访问本行数据的外包人员开展数据安全方面的教育与培训，并与其签署保密协议。

（二）信息安全管理体系认证

本行积极开展信息安全管理体系认证，以提升隐私及数据安全管理水平。截至2024年末，本行通过ISO 27001信息安全管理体系认证、ISO 27701隐私信息管理体系认证、ISO 20000信息技术服务管理和ISO 22301业务连续性管理等体系认证以及开发运维一体化（DevOps）持续交付成熟度、能力成熟度模型集成三级（CMMI3）软件成熟度等管理标准认证，认证的业务范围包括全行范围内的信息系统开发、测试、运行和维护。

同时，本行持续加强信息安全管理的规范性和体系化建设。已经通过北京国家金融科技认证中心有限公司的“金融网络安全能力成熟度”第四等级优秀级认证，该项认证以我国《金融网络安全 网络安全能力成熟度模型》作为基准，体现了浙商银行在信息安全方面优秀的管理水平。

（三）供应商和业务伙伴数据安全管理

对产生重大数据安全风险、事件、案件的第三方合作机构，本行将暂缓或停止与其合作，并追究其法律责任。

本行制定《浙商银行信息科技外包风险管理办法》，将第三方合作数据纳入信息科技外包管理，明确服务提供商的准入标准，明确服务合同或协议中关于双方数据安全责任义务的要求，对重要外包的备选服务提供商开展深入尽职调查，调查内容包括供应

商内部管理制度和流程建设情况、网络和信息安全保障能力、遵守国家和监管相关法律法规要求的情况、应急处置能力等。合作过程中，定期评估数据安全风险，评估内容包括数据交互与传输安全风险、合作机构数据安全保护履职情况、承载数据合作的系统平台安全保护情况。

（四）客户隐私保护知识教育

开展客户隐私保护知识教育是法定义务，并是提升客户信任、降低数据泄露风险的关键举措。有效的教育应帮助客户理解其个人信息价值、面临的威胁、自身权利及保护方法。

本行通过公众号、网点宣传和教育等形式，积极开展消费者权益保护或宣传个人隐私保护相关措施，如“3.15”金融消费者权益保护教育宣传活动|个人信息守护好，守牢隐私勿泄露等系列公众号推文。

九、数据安全审计

本行由总行审计部负责数据安全审计，负责全行数据安全及其风险管理审计工作，以及发生重大数据安全事件后及时开展专项审计。

本行至少每三年由总行审计部开展一次数据安全全面审计。最近一次审计时间为2024年，未发现重大风险隐患。本行每年委托第三方机构开展包括网络安全和防病毒在内的信息科技审

计，2024 年审计未发现数据安全方面的问题。

根据 ISO 27001 信息安全管理体系认证、ISO 27701 隐私信息管理体系认证要求，本行每年开展认证审核或监督审核。2024 年，ISO 27001 再认证审核和 ISO 27701 监督审核未发现数据安全方面的问题。