华夏银行隐私与数据安全制度要点
（2026 年版）

一、目的

华夏银行股份有限公司（以下简称“华夏银行”“本行”）高度重视客户隐私保护和数据安全管理，致力于维护客户对本行的信任与认可。

本行严格遵守《中华人民共和国数据安全法》《中华人民共和国网络安全法》《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》等法律法规及监管规定，制定《华夏银行数据安全管理办法》《华夏银行数据安全管理实施细则》《华夏银行个人信息保护管理实施细则》等制度规范，明确数据安全管理要求，健全数据安全管理机制，有效防范数据安全风险，切实保护客户个人信息安全。

二、适用范围与管理架构

（一）适用范围

本政策适用于总行及境内各分支机构全部业务条线，以及向客户提供的所有产品和服务。

（二）组织架构与职责分工

本行构建与全行数据治理工作相适应的数据安全组织架构，数据安全组织分为三层——决策层、统筹管理层、执行层。

决策层是本行数据安全的最高决策机构，包括党委、董事会

和高级管理层；实施党委数据安全责任制，党委、董事会对本行数据安全工作负主体责任，党委、董事会主要负责人为数据安全第一责任人，分管数据安全的高级管理人员为直接责任人；高级管理层负责实施董事会确定的数据安全战略，建立全行数据安全体系，制定和实施问责机制与数据安全控制机制，组织评估数据安全的有效性和执行情况，并定期向党委、董事会报告；高级管理层委托下设的总行数据治理委员会履行高级管理层的数据安全工作职责。

统筹管理层采取管理、技术双牵头模式。总行数据管理部统筹推进数据安全管理工作，持续完善数据安全管理制度、数据分类分级保护机制，规范数据处理活动、开展数据安全影响评估，组织建立风险监测与事件应急响应机制、模拟数据安全事件应急演练，定期开展数据安全培训、不断提高全行数据安全意识；总行信息科技管理部统筹建立数据安全技术保护体系，建立数据安全技术架构和保护控制基线，制定数据安全技术标准规范，组织落实技术保护措施。

执行层包括总行各部门及各分支机构。执行层遵循“谁管业务、谁管业务数据、谁管数据安全”原则，严格落实数据安全管理要求，准确及时报送重要数据目录，认真执行数据全生命周期安全保护措施。

三、客户信息的收集与使用

（一）收集方式与范围

本行开展金融服务和经营管理时，可直接或间接从个人金融信息主体、企业客户及外部数据供应方采集个人信息。信息采集需明确合理的业务目的，仅采集业务所需信息，不采集与业务无关内容，不得采取强制、违规采购等方式收集信息。

（二）告知与授权同意流程

本行在收集个人信息前完整向客户告知全部法定处理事项并取得同意；处理敏感信息、未成年人信息，需额外告知相关影响并单独取得同意，同时对外公开清晰的信息处理规则。业务用途发生变更需重新获取客户同意，设置便捷撤回途径，不得以客户拒绝营销授权为由停止基础金融服务。

（三）敏感个人信息特别保护

本行对生物识别、金融账户、不满十四周岁未成年人等敏感个人信息采取加密、分库存储保护，原始生物影像非必要不采集；对外公开、共享敏感信息需事前开展影响评估并取得客户单独同意，身份鉴别数据禁止明文存储传输。

（四）收集使用的最小必要原则

本行信息采集、系统权限分配、对外提供信息均遵循最小必要原则，严格控制信息获取范围，按岗位分配对应访问权限，向第三方仅提供业务必需信息，不超范围采集、使用客户个人信息。

四、客户信息的对外提供与存储

（一）对外提供与第三方管理

本行严禁出租、出售客户个人信息，行内机构共享数据需签

订共享协议，委托第三方处理信息需签订合同明确权责、禁止转委托；批量敏感数据合作需提前向监管报备，未经客户同意，不得跨合作平台传递客户信息，营销推送提供退订渠道。

（二）客户信息存储与期限管理

业务产生的个人信息在境内存储，按数据等级落实差异化防护措施，规范操作日志留存年限；仅在业务最短存续期内保存信息，保存期满或业务终止后，对个人信息进行删除或匿名化处理。

（三）跨境数据传输管理

向境外提供个人信息，需完成出境安全评估并取得客户单独授权，向个人告知其向境外接收方行使信息权利的方式和程序等事项，并采取措施确保接收方达到个人信息保护法定标准的相关规定。

五、客户权利保障

（一）查阅权与获取个人信息副本

客户可通过线上渠道、线下网点核验身份后，查阅本人留存的个人信息；若客户需要本人信息副本，本行核实身份后可向客户提供本行留存的个人信息副本，法律法规、监管机构另有规定的除外。

（二）更正与补充权

客户发现留存信息存在错误、缺失的，可向本行申请更正，本行核验身份后对系统内对应信息完成更新。

（三）删除权与注销账户

客户使用本行各类服务期间，可主动申请解除对应服务、注销服务权限，该解约操作具备不可逆属性；完成服务注销即视为客户撤回针对该服务项下个人信息收集、处理的全部授权，本行自此不再基于该服务收集、使用其个人信息，并清除对应服务产生的全部个人信息，法律法规、监管规定另有存储要求的除外，撤回授权不影响此前依据客户授权已开展的信息处理行为。

（四）撤回授权同意

本行向客户提供撤回收集、使用其个人信息的授权同意的方法。撤回授权同意后，本行后续不应再处理相应的个人信息。但撤回同意的决定，不会影响此前基于已授权而开展的个人信息处理。

（五）响应时效与投诉渠道

如果客户使用本行产品或服务时遇到与个人信息保护相关的任何问题（包括问题咨询、投诉），可通过拨打本行 95577 客服热线、登录本行官方网站（www.hxb.com.cn)—在线客服或到本行各营业网点咨询或反映。受理问题后，本行会及时、妥善处理。一般情况下，本行将在 15 个自然日内受理并处理。如情况特别复杂或有其他特殊原因的，最长处理期限不超过 60 日。

六、数据安全保护措施

（一）加密与去标识化技术

本行建立了数据识别、加密和脱敏机制，通过敏感数据加密存储、数据脱敏、模糊化处理、截屏录屏限制等技术手段，在数

据传输和存储过程中调用加密机、密码键盘、签名验签服务器等密码设备，防止数据篡改、泄露、丢失；对人脸、声纹仅加密特征入库，不存储原始高清人脸大图，定期清除证件影像，仅留存脱敏结构化字段入库，保护数据主体权益。

（二）访问控制与权限管理

本行提供应用服务时，采取密码、人脸、短信验证码等多因素认证手段核实客户身份，进行用户认证和访问有效控制；进行数据分类管理，对生物特征、音视频、OCR原始影像等核心敏感数据独立隔离存储，与普通业务数据实施隔离管理，强化数据访问控制管理。

本行对人工智能模型研发全流程实施主动管控，所有AI模型、智能体应用及开发平台均采用本地化部署模式。本行数据严禁对外输出，不得作为外部人工智能模型训练、测试、验证等的数据源。

（三）数据安全风险评估

本行按年度组织总行及境内分支机构开展数据安全风险评估，梳理总结全行数据安全管理制度要求、数据分类分级、数据安全技术保护措施、数据访问与操作行为审计、数据安全评估、风险监测与突发事件处置、全行数据安全培训宣贯等重点领域的工作落实情况及优化举措，编制全行数据安全风险评估报告并报送上级单位。

（四）开发测试环境安全管理

本行明确敏感级及以上数据未经脱敏处理不得进入测试环境的原则，确保测试环境与生产系统隔离，防止数据泄露。

在主机安全层面，严格按照权限分级、最小权限、相互制约原则开展用户访问管控，对操作系统账户、应用层账户实行差异化分级管理，同步部署安全扫描工具并常态化更新病毒库与特征库，实现测试环境安全风险监控；在数据安全层面，执行生产环境至测试环境单向数据传输要求，禁止未脱敏敏感数据导入测试环境；在网络安全层面，开发测试网与生产、办公网严格依照安全规范隔离，互联网访问采用白名单管控。

七、数据安全事件应急响应

（一）应急预案制定与演练

本行制定了《华夏银行信息系统应急预案数据安全分册》，定期开展应急响应培训和应急演练。各分行建立分行信息科技事件应急管理机制，制定本机构数据安全事件应急报告流程，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。

（二）事件监测与处置流程

本行建立覆盖舆情、客户投诉、第三方管理、数据使用异常行为等内容的数据安全风险监测指标体系，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。同时，本行将数据泄露、仿冒欺诈等重要事件纳入舆情监测范围，实施 7×24 小时舆情监测，提高敏感舆情发现的精准性、全面性、有效性。

本行围绕数据篡改、数据泄露、数据破坏、数据非法获取、数据非法利用、违规数据共享六类应急处置场景，分类编制标准化的处置流程。针对每一类场景，细化处置规范，明确对应业务系统、应急场景、故障分级、预警识别关键字、处置方案、操作流程、恢复核验标准及预估处置时长等，统一处置标准，规范各环节操作步骤，有效提升数据安全事件识别与处置效率。

（三）客户告知与监管报告

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,以及本行采取的补救措施和个人可以采取的减轻危害的措施。数据安全事件首报后三个工作日内，补充报送数据安全影响评估报告；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。

在敏感或重要保障时期发生对国家、社会、公共利益、企业声誉造成严重影响或较大负面舆情的数据安全事件,以及勒索攻击类事件，在 30 分钟内口头报告监管机构，1 小时内书面报告。

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。