ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0171—2020

个人金融信息保护技术规范

Personal financial information protection technical specification

2020－02－13 发布　　2020－02－13 实施

中国人民银行　　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由中国人民银行提出。

本标准由全国金融标准化技术委员会（SAC/TC 180）归口。

本标准起草单位：中国人民银行科技司、中国人民银行郑州中心支行、北京银联金卡科技有限公司、中国银行股份有限公司、中国银联股份有限公司、网联清算有限公司、浙江蚂蚁小微金融服务集团股份有限公司、拉卡拉支付股份有限公司、中国金融电子化公司、中国人民银行武汉分行、中国工商银行股份有限公司、中国农业银行股份有限公司、中国建设银行股份有限公司、中国平安保险（集团）股份有限公司、北京中金国盛认证有限公司、北京软件产品质量检测检验中心、中金金融认证中心有限公司、信息产业信息安全测评中心、华泰证券股份有限公司、中国人民保险集团股份有限公司、财付通支付科技有限公司、中国支付清算协会、中国互联网金融协会、建信金融科技有限责任公司。

本标准主要起草人：李伟、李兴锋、张宏基、关晓辉、刘雨露、汤沁瑾、郭琳诤、赵战勇、熊继承、渠韶光、孟飞宇、高强裔、陈聪、居崑、陈雪秀、公丽丽、徐艳姣、牛小伟、王欢、展昭、强群力、郭林、杨萌、陈俊、李意、冯坚坚、唐凌、黄本涛、魏猛、刘琼瑶、赵旭、孙垚、周利华、母延燕、王家炜、张扬、蔡嘉勇、刘洋、孙鹏亮、聂丽琴、刘力慷、牛跃华、陈伟、王秀君、任凤丽、谢宗晓、董亚南、张旭刚、刘健、董晶晶、张嵩、于晓雪、吴永强、陆家有、石竹君、于沛、侯晓晨、田然、王泽航、何伟明、梁伟韬。

引　言

个人金融信息是个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化，是金融业机构在提供金融产品和服务的过程中积累的重要基础数据，也是个人隐私的重要内容。个人金融信息一旦泄露，不但会直接侵害个人金融信息主体的合法权益、影响金融业机构的正常运营，甚至可能会带来系统性金融风险。为加强个人金融信息安全管理，指导各相关机构规范处理个人金融信息，最大程度保障个人金融信息主体合法权益，维护金融市场稳定，编制本标准。

个人金融信息保护技术规范

1 范围

本标准规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

本标准适用于提供金融产品和服务的金融业机构，并为安全评估机构开展安全检查与评估工作提供参考。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2010 信息安全技术 术语

GB/T 31186.2—2014 银行客户基本信息描述规范 第2部分：名称

GB/T 31186.3—2014 银行客户基本信息描述规范 第3部分：识别标识

GB/T 35273—2017 信息安全技术 个人信息安全规范

JR/T 0068—2020 网上银行系统信息安全通用规范

JR/T 0071 金融行业信息系统信息安全等级保护实施指引

JR/T 0092—2019 移动金融客户端应用软件安全管理规范

JR/T 0149—2016 中国金融移动支付 支付标记化技术规范

JR/T 0167—2018 云计算技术金融应用规范 安全技术要求

3 术语和定义

GB/T 25069—2010、GB/T 35273—2017界定的以及下列术语和定义适用于本文件。

3.1

金融业机构 financial industry institutions

本标准中的金融业机构是指由国家金融管理部门监督管理的持牌金融机构，以及涉及个人金融信息处理的相关机构。

3.2

个人金融信息 personal financial information

金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。

注1：本标准中的个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反映特定个人某些情况的信息。

注2：改写GB/T 35273—2017，定义3.1。

3.3

支付敏感信息 payment sensitive information

支付信息中涉及支付主体隐私和身份识别的重要信息。

注：支付敏感信息包括但不限于银行卡磁道数据或芯片等效信息、卡片验证码、卡片有效期、银行卡密码、网络支付交易密码等用于支付鉴权的个人金融信息。

3.4

个人金融信息主体 personal financial information subject

个人金融信息所标识的自然人。

注：改写GB/T 35273—2017，定义3.3。

3.5

个人金融信息控制者 personal financial information controller

有权决定个人金融信息处理目的、方式等的机构。

注：改写GB/T 35273—2017，定义3.4。

3.6

收集 collect

获得个人金融信息的控制权的行为。

注1：收集行为包括由个人金融信息主体主动提供、通过与个人金融信息主体交互或记录个人金融信息主体行为等自动采集行为，以及通过共享、转让、搜集公开信息等间接获取个人金融信息等行为。

注2：如金融产品或服务提供者提供工具供个人金融信息主体使用，提供者不对个人金融信息进行访问的，则不属于本标准所称的收集。例如手机银行客户端应用软件在终端获取用户指纹特征信息用于本地鉴权后，指纹特征信息不回传至提供者，则不属于用户指纹特征信息的收集行为。

注3：改写 GB/T 35273—2017，定义 3.5。

3.7

公开披露 public disclosure

向社会或不特定群体发布信息的行为。

[GB/T 35273—2017，定义3.10]

3.8

转让 transfer of control

将个人金融信息控制权由一个控制者向另一个控制者转移的过程。

注：改写GB/T 35273—2017，定义3.11。

3.9

共享 sharing

个人金融信息控制者向其他控制者提供个人金融信息，且双方分别对个人金融信息拥有独立控制权的过程。

注：改写GB/T 35273—2017，定义3.12。

3.10

个人金融信息安全影响评估 personal financial information security impact assessment

针对个人金融信息处理活动，检验其合法合规程度，判断其对个人金融信息主体合法权益造成损害的各种风险，以及评估用于保护个人金融信息主体的各项措施有效性的过程。

注：改写GB/T 35273—2017，定义3.8。

3.11

支付账号 payment account

具有金融交易功能的银行账户、非银行支付机构支付账户及银行卡卡号。

注：改写JR/T 0149—2016，定义3.1。

3.12

支付标记 payment token(Token)

作为支付账号等原始交易要素的替代值，用于完成特定场景支付交易。

[JR/T 0149—2016，定义3.2]

3.13

磁道数据 track data

一磁、二磁和三磁定义的必备或可选的数据元。

注：磁道数据可以在物理卡的磁条上，也可以被包含在集成电路或者其他媒介上。

[JR/T 0061—2011，定义3.20]

3.14

卡片验证码 card verification number；CVN

对磁条信息合法性进行验证的代码。

[JR/T 0061—2011，定义8.7]

3.15

卡片验证码2 card verification number 2；CVN2

在邮购或电话订购等非面对面交易中对银行卡卡片合法性进行验证的代码。

[JR/T 0061—2011，定义8.8]

3.16

动态口令 one-time-password (OTP), dynamic password

基于时间、事件等方式动态生成的一次性口令。

[GM/Z 0001—2013，定义2.15]

3.17

短信动态密码 SMS dynamic code

短信验证码 SMS code

后台系统以手机短信形式发送到用户绑定手机上的随机数，用户通过回复该随机数进行身份认证。

[JR/T 0088.1—2012，定义2.44]

3.18

客户法定名称 customer's legal name

在法律上认可的客户名称。

注1：客户法定名称一般记录在国家授权部门颁发给客户的证件上，本标准客户主要指自然人客户。

注2：改写GB/T 31186.2—2014，定义3.2。

3.19

证件类识别标识 legal discriminating ID

由国家法定有权部门颁发，能够唯一确定客户的且具有法律效力的标识。

注1：证件类识别标识是外源性数据。外源性数据意味着数据的使用者不是数据的所有者，数据在产生、变更、废止后可能不为数据的使用者所知悉。

注2：本标准的使用者因本身业务需求而产生的内部证件类标识，不应在使用者外部使用，也不具有法律效力。

注3：改写GB/T 31186.3—2014，定义3.2。

3.20

未经授权的查看 unauthorized reading

未得到信息的所有者或有权授权人授权对信息的查看。

注1：未经授权的查看可能是善意的，也可能是恶意的；信息处理者无意泄露的未经授权的查看为信息泄露事件；攻击者通过使相关安全措施无效的措施有意获取的未经授权的查看为信息窃取事件。

注2：非法查看是对未经授权的查看的一种不严谨但在特定的语境下并无二义性的提法。

3.21

未经授权的变更 unauthorized altering

未得到信息的所有者或有权授权人授权对信息的变更。

注1：未经授权的变更典型地分为未经授权的增加（即增加全新的内容）、未经授权的更改（即修改现有的内容）或未经授权的删除（即删除原有的内容）三种情况，也可能是三种情况的组合。

注2：未经授权的变更可能是善意的，也可能是恶意的；往往表现为信息篡改事件、信息假冒事件、信息丢失事件等。

注3：非法变更是对未经授权的变更的一种不严谨但在特定的语境下并无二义性的提法。

3.22

明示同意 explicit consent

个人金融信息主体通过书面声明或主动作出肯定性动作，对其个人金融信息进行特定处理作出明确授权的行为。

注1：肯定性动作包括个人金融信息主体主动作出声明（电子或纸质形式）、主动勾选、主动点击“同意”“注册”“发送”“拨打”、主动填写或提供等。

注2：改写GB/T 35273—2017，定义3.6。

3.23

匿名化 anonymization

通过对个人金融信息的技术处理，使得个人金融信息主体无法被识别，且处理后的信息不能被复原的过程。

注 1：个人金融信息经匿名化处理后所得的信息不属于个人金融信息。

注 2：改写 GB/T 35273—2017，定义 3.13。

3.24

去标识化 de-identification

通过对个人金融信息的技术处理，使其在不借助额外信息的情况下，无法识别个人金融信息主体的过程。

注 1：去标识化仍建立在个体基础之上，保留了个体颗粒度，采用假名、加密、加盐的哈希函数等技术手段替代对个人金融信息的标识。

注 2：改写 GB/T 35273—2017，定义 3.14。

3.25

删除 delete

在金融产品和服务所涉及的系统中去除个人金融信息的行为，使其保持不可被检索、访问的状态。

注：改写GB/T 35273—2017，定义3.9。

4 个人金融信息概述

4.1 个人金融信息内容

个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息和其他反映特定个人金融信息主体某些情况的信息，具体如下：

a) 账户信息指账户及账户相关信息，包括但不限于支付账号、银行卡磁道数据（或芯片等效信息）、银行卡有效期、证券账户、保险账户、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等。

b) 鉴别信息指用于验证主体是否具有访问或使用权限的信息，包括但不限于银行卡密码、预付卡支付密码；个人金融信息主体登录密码、账户查询密码、交易密码；卡片验证码（CVN 和 CVN2）、动态口令、短信验证码、密码提示问题答案等。

c) 金融交易信息指个人金融信息主体在交易过程中产生的各类信息，包括但不限于交易金额、支付记录、透支记录、交易日志、交易凭证；证券委托、成交、持仓信息；保单信息、理赔信息等。

d) 个人身份信息指个人基本信息、个人生物识别信息等：

- 个人基本信息包括但不限于客户法定名称、性别、国籍、民族、职业、婚姻状况、家庭状况、收入情况、身份证和护照等证件类信息、手机号码、固定电话号码、电子邮箱、工作及家庭地址，以及在提供产品和服务过程中收集的照片、音视频等信息；
- 个人生物识别信息包括但不限于指纹、人脸、虹膜、耳纹、掌纹、静脉、声纹、眼纹、步态、笔迹等生物特征样本数据、特征值与模板。

e) 财产信息指金融业机构在提供金融产品和服务过程中，收集或生成的个人金融信息主体财产信息，包括但不限于个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金存缴金额等。

f) 借贷信息指个人金融信息主体在金融业机构发生借贷业务产生的信息，包括但不限于授信、信用卡和贷款的发放及还款、担保情况等。

g) 其他信息：

- 对原始数据进行处理、分析形成的，能够反映特定个人某些情况的信息，包括但不限于特定个人金融信息主体的消费意愿、支付习惯和其他衍生信息；
- 在提供金融产品与服务过程中获取、保存的其他个人信息。

4.2 个人金融信息类别

根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为C3、C2、C1三个类别。具体如下：

a) C3 类别信息主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害，包括但不限于：
   - 银行卡磁道数据（或芯片等效信息）、卡片验证码（CVN 和 CVN2）、卡片有效期、银行卡密码、网络支付交易密码；
   - 账户（包括但不限于支付账号、证券账户、保险账户）登录密码、交易密码、查询密码；
   - 用于用户鉴别的个人生物识别信息。
b) C2 类别信息主要为可识别特定个人金融信息主体身份与金融状况的个人金融信息，以及用于金融产品与服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害，包括但不限于：
   - 支付账号及其等效信息，如支付账号、证件类识别标识与证件信息（身份证、护照等）、手机号码。
   - 账户（包括但不限于支付账号、证券账户、保险账户）登录的用户名。
   - 用户鉴别辅助信息，如动态口令、短信验证码、密码提示问题答案、动态声纹密码；若用户鉴别辅助信息与账号结合使用可直接完成用户鉴别，则属于 C3 类别信息。
   - 直接反映个人金融信息主体金融状况的信息，如个人财产信息（包括网络支付账号余额）、借贷信息。
   - 用于金融产品与服务的关键信息，如交易信息（如交易指令、交易流水、证券委托、保险理赔）等。
   - 用于履行了解你的客户（KYC）要求，以及按行业主管部门存证、保全等需要，在提供产品和服务过程中收集的个人金融信息主体照片、音视频等影像信息。
   - 其他能够识别出特定主体的信息，如家庭地址等。
c) C1 类别信息主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响，包括但不限于：
   - 账户开立时间、开户机构；
   - 基于账户信息产生的支付标记信息；
   - C2 和 C3 类别信息中未包含的其他个人金融信息。

个人金融信息主体因业务需要（如贷款）主动提供的有关家庭成员信息（如身份证号码、手机号码、财产信息等），应依据C3、C2、C1敏感程度类别进行分类，并实施针对性的保护措施。

两种或两种以上的低敏感程度类别信息经过组合、关联和分析后可能产生高敏感程度的信息。同一信息在不同的服务场景中可能处于不同的类别，应依据服务场景以及该信息在其中的作用对信息的类别进行识别，并实施针对性的保护措施。

4.3 个人金融信息生命周期

个人金融信息生命周期指对个人金融信息进行收集、传输、存储、使用、删除、销毁等处理的整个过程，各环节描述如下：

a) 收集：对个人金融信息主体各类信息进行获取和记录的过程。
b) 传输：个人金融信息在终端设备、信息系统内或信息系统间传递的过程。
c) 存储：个人金融信息在终端设备、信息系统内保存的过程。
d) 使用：对个人金融信息进行展示、共享和转让、公开披露、委托处理、加工处理等操作的过程。
e) 删除：使个人金融信息不可被检索、访问的过程。
f) 销毁：对个人金融信息进行清除，使其不可恢复的过程。

5 安全基本原则

金融业机构应遵循 GB/T 35273—2017 的要求，以“权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与”的原则，设计并实施覆盖个人金融信息全生命周期的安全保护策略。

6 安全技术要求

6.1 生命周期技术要求

6.1.1 收集

应根据信息类别确定个人金融信息收集方案。具体技术要求如下：

a) 不应委托或授权无金融业相关资质的机构收集 C3、C2 类别信息。
b) 应确保收集信息来源的可追溯性。
c) 应采取技术措施（如弹窗、明显位置 URL 链接等），引导个人金融信息主体查阅隐私政策，并获得其明示同意后，开展有关个人金融信息的收集活动。
d) 对于 C3 类别信息，通过受理终端、客户端应用软件、浏览器等方式收集时，应使用加密等技术措施保证数据的保密性，防止其被未授权的第三方获取。
e) 通过受理终端、客户端应用软件与浏览器等方式引导用户输入（或设置）银行卡密码、网络支付密码时，应采取展示屏蔽等措施防止密码明文显示，其他密码类信息宜采取展示屏蔽措施。
f) 在网络支付业务系统中，应采取具有信息输入安全防护、即时数据加密功能的安全控件对支付敏感信息的输入进行安全保护，并采取有效措施防止合作机构获取、留存支付敏感信息。
g) 在停止提供金融产品或服务时，应及时停止继续收集个人金融信息的活动。

6.1.2 传输

个人金融信息传输过程的参与方应保证信息在传输过程中的保密性、完整性和可用性，具体技术要求如下：

a) 应建立相应的个人金融信息传输安全策略和规程，采用满足个人金融信息传输安全策略的安全控制措施，如安全通道、数据加密等技术措施。
b) 传输个人金融信息前，通信双方应通过有效技术手段进行身份鉴别和认证。
c) 通过公共网络传输时，C2、C3 类别信息应使用加密通道或数据加密的方式进行传输，保障个人金融信息传输过程的安全；对于 C3 类别中的支付敏感信息，其安全传输技术控制措施应符合有关行业技术标准与行业主管部门有关规定要求。
d) 应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的安全传输；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全传输保障手段。
e) 个人金融信息传输的接收方应对接收的信息进行完整性校验。

f) 应建立有效机制对个人金融信息传输安全策略进行审核、监控和优化，包括对通道安全配置、密码算法配置、密钥管理等保护措施的管理和监控。

g) 应采取有效措施(如个人金融信息传输链路冗余)保证数据传输可靠性和网络传输服务可用性。

6.1.3 存储

个人金融信息存储的具体技术要求如下：

a) 不应留存非本机构的银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN和CVN2）、银行卡密码、网络支付密码等C3类别信息。若确有必要留存的，应取得个人金融信息主体及账户管理机构的授权。

b) 应根据个人金融信息的不同类别，采用技术手段保证个人金融信息的存储安全；低敏感程度类别的个人金融信息因参与身份鉴别等关键活动导致敏感程度上升的（如，经组合后构成交易授权完整要素的情况），应提升相应的安全存储保障手段。

c) C3类别个人金融信息应采用加密措施确保数据存储的保密性。

d) 受理终端、个人终端及客户端应用软件均不应存储银行卡磁道数据（或芯片等效信息）、银行卡有效期、卡片验证码（CVN和CVN2）、银行卡密码、网络支付密码等支付敏感信息及个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必需的基本信息要素，并在完成交易后及时予以清除。

e) 采取必要的技术和管控措施保证个人金融信息存储转移过程中的安全性。

f) 应将去标识化、匿名化后的数据与可用于恢复识别个人的信息采取逻辑隔离的方式进行存储，确保去标识化、匿名化后的信息与个人金融信息不被混用。

g) 在停止运营时，应依据国家法律法规与行业主管部门有关规定要求，对所存储的个人金融信息进行妥善处置，或移交国家与行业主管部门指定的机构继续保存。

6.1.4 使用

6.1.4.1 信息展示

提供业务办理与查询等功能的应用软件，对个人金融信息展示具体技术要求如下：

a) 依据国家法律法规与行业主管部门有关规定要求，对通过计算机屏幕、客户端应用软件、银行卡受理设备、自助终端设备、纸面（如受理终端打印出的交易凭条等交易凭证）等界面展示的个人金融信息应采取信息屏蔽（或截词）等处理措施，降低个人金融信息在展示环节的泄露风险。

注1：关于信息屏蔽（或截词）的使用方式，参见附录A。

注2：金融业机构柜面打印的凭证依据有关规范执行。

b) 处于未登录状态时，不应展示与个人金融信息主体相关的C3类别信息。

c) 处于已登录状态时，个人金融信息展示的技术要求如下：

- 除银行卡有效期外，C3类别信息不应明文展示。
- 对于银行卡号、手机号码、证件类识别标识或其他识别标识信息等可以直接或组合后确定个人金融信息主体的信息应进行屏蔽展示，或由用户选择是否屏蔽展示，如需完整展示，应进行用户身份验证，并做好此类信息管理，防范此类信息泄露风险。
- 涉及其他个人金融信息主体的信息时，除以下情况外，宜进行屏蔽展示：

——其他方主动发起的活动包含的信息，此种情况需展示必要的信息以供活动接收方对活动内容进行确认，例如：其他方发起的交易、其他方发起的收付款、保险保费代收。

——与其他方已建立信任关系（间接授权），此时需活动发起方确认发起活动的必要信息

的正确性（或活动发起方需接收活动结果信息，并确认活动已正确完成），例如：向其他方收款，其他方已付款；向其他方申请代付，其他方同意付款或者其他方在自己业务应用范围内的联系人。

——其他法律法规要求的情况。

应用软件的后台管理与业务支撑系统，对个人金融信息展示具体技术要求如下：

a) 除银行卡有效期外，C3 类别信息不应明文展示。
b) 应采取技术措施防范个人金融信息在展示过程中泄露或被未经授权的拷贝。
c) 后台系统对支付账号、客户法定名称、支付预留手机号码、证件类或其他类识别标识信息等展示宜进行屏蔽处理，如需完整展示，应做好此类信息管理，采取有效措施防范未经授权的拷贝。
d) 后台系统不应具备开放式查询能力，应严格限制批量查询。
e) 对于确有明文查看需要的业务场景可以保留明文查看权限，后台系统应对所有查询操作进行细粒度的授权与行为审计。

应防止通过散列碰撞等方法推导出完整的数据，若使用“截词”的方式进行部分字段的屏蔽处理，不应用散列代替字段被截词的部分。

6.1.4.2 共享和转让

个人金融信息在共享和转让的过程中，应充分重视信息转移或交换过程中的安全风险，具体技术要求如下：

a) 在共享和转让前，应开展个人金融信息安全影响评估，并依据评估结果采取有效措施保护个人金融信息主体权益。
b) 在共享和转让前，应开展个人金融信息接收方信息安全保障能力评估，并与其签署数据保护责任承诺。
c) 支付账号及其等效信息在共享和转让时，除法律法规和行业主管部门另有规定外，应使用支付标记化（按照 JR/T 0149—2016）技术进行脱敏处理（因业务需要无法使用支付标记化技术时，应进行加密），防范信息泄露风险。
d) 应部署信息防泄露监控工具，监控及报告个人金融信息的违规外发行为。
e) 应部署流量监控技术措施，对共享、转让的信息进行监控和审计。
f) 应根据“业务需要”和“最小权限”原则，对个人金融信息的导出操作进行细粒度的访问控制与全过程审计，应采取两种或两种以上鉴别技术对导出信息操作人员进行身份鉴别。
g) 应定期检查或评估信息导出通道的安全性和可靠性。
h) 使用外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）进行信息共享与转让时，应定期检查或评估信息共享工具、服务组件和共享通道的安全性和可靠性，并留存检查或评估结果记录。
i) 应执行严格的审核程序，并准确记录和保存个人金融信息共享和转让情况。记录内容应包括但不限于日期、规模、目的、范围，以及数据接收方基本情况与使用意图等，并应确保对共享和转让的信息及其过程可被追溯。
j) 应采取有效技术防护措施，防范信息转移过程中被除信息发送方与接收方之外的其他个人、组织和机构截获和利用。

6.1.4.3 公开披露

个人金融信息原则上不得公开披露。金融业机构经法律授权或具备合理事由确需公开披露时，具体技术要求如下：

a) 应事先开展个人金融信息安全影响评估，并依据评估结果采取有效的保护个人金融信息主体权益的措施。
b) 不应公开披露个人生物识别信息。
c) 应准确记录和保存个人金融信息的公开披露情况，包括公开披露的日期、规模、目的、内容、公开范围等。

6.1.4.4 委托处理

金融业机构因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理时，具体技术要求如下：

a) 委托行为不应超出已征得个人金融信息主体授权同意的范围或遵循 7.1 中对于征得授权同意的例外所规定的情形，并准确记录和保存委托处理个人金融信息的情况。
b) C3 以及 C2 类别信息中的用户鉴别辅助信息，不应委托给第三方机构进行处理。转接清算、登记结算等情况，应依据国家有关法律法规及行业主管部门有关规定与技术标准执行。
c) 对委托处理的信息应采用去标识化（不应仅使用加密技术）等方式进行脱敏处理，降低个人金融信息被泄露、误用、滥用的风险。
d) 应对委托行为进行个人金融信息安全影响评估，并确保受委托者具备足够的数据安全能力，且提供了足够的安全保护措施。
e) 应对第三方机构等受委托者进行监督，方式包括但不限于：
   - 依据 7.2.1 的要求，通过合同等方式规定受委托者的责任和义务；
   - 依据 7.4.2 的要求，对受委托者进行安全检查和评估。
f) 应对外部嵌入或接入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展技术检测，确保其个人金融信息收集、使用行为符合约定要求；并对其收集个人金融信息的行为进行审计，发现超出约定行为及时切断接入。

6.1.4.5 加工处理

个人金融信息在加工处理的过程中，具体技术要求如下：

a) 应采取必要的技术手段和管理措施，确保在个人金融信息清洗和转换过程中对信息进行保护，对 C2、C3 类别信息，应采取更加严格的保护措施。
b) 应对匿名化或去标识化处理的数据集或其他数据集汇聚后重新识别出个人金融信息主体的风险进行识别和评价，并对数据集采取相应的保护措施。
c) 应建立个人金融信息防泄露控制规范和机制，防止个人金融信息处理过程中的调试信息、日志记录等因不受控制的输出而泄露受保护的信息。
d) 应具备信息化技术手段或机制，对个人金融信息滥用行为进行有效的识别、监控和预警。
e) 应具备完整的个人金融信息加工处理操作记录和管理能力，记录内容包括但不限于日期、时间、主体、事件描述、事件结果等。

6.1.4.6 汇聚融合

个人金融信息汇聚融合的技术要求如下：

a) 汇聚融合的数据不应超出收集时所声明的使用范围。因业务需要确需超范围使用的，应再次征得个人金融信息主体明示同意。
b) 应根据汇聚融合后的个人金融信息类别及使用目的，开展个人金融信息安全影响评估，并采取有效的技术保护措施。

6.1.4.7 开发测试

个人金融信息在开发测试过程中的具体技术要求如下：

a) 应对开发测试环境与生产环境进行有效隔离。
b) 开发环境、测试环境不应使用真实的个人金融信息，应使用虚构的或经过去标识化（不应仅使用加密技术）脱敏处理的个人金融信息，账号、卡号、协议号、支付指令等测试确需信息除外。

6.1.5 删除

个人金融信息在删除过程中的具体技术要求如下：

a) 应采取技术手段，在金融产品和服务所涉及的系统中去除个人金融信息，使其保持不可被检索和访问。
b) 个人金融信息主体要求删除个人金融信息时，金融业机构应依据国家法律法规、行业主管部门有关规定以及与个人金融信息主体的约定予以响应。

6.1.6 销毁

个人金融信息在销毁过程中的具体技术要求如下：

a) 应建立个人金融信息销毁策略和管理制度，明确销毁对象、流程、方式和要求。
b) 应对个人金融信息存储介质销毁过程进行监督与控制，对待销毁介质的登记、审批、介质交接、销毁执行等过程进行监督。
c) 销毁过程应保留有关记录，记录至少应包括销毁内容、销毁方式与时间、销毁人签字、监督人签字等内容。
d) 存储个人金融信息的介质如不再使用，应采用不可恢复的方式（如消磁、焚烧、粉碎等）对介质进行销毁处理；存储个人金融信息的介质如还需继续使用，不应只采用删除索引、删除文件系统的方式进行信息销毁，应通过多次覆写等方式安全地擦除个人金融信息，确保介质中的个人金融信息不可再被恢复或者以其他形式加以利用。
e) 云环境下有关数据清除应依据 JR/T 0167—2018 的 9.6 执行。

6.2 安全运行技术要求

6.2.1 网络安全要求

承载与处理个人金融信息的信息系统应符合国家网络安全相关规定与 GB/T 22239—2019、JR/T 0071 的要求。存储个人金融信息的数据库应处于金融业机构可控网络内，并进行有效的访问控制。

6.2.2 Web 应用安全要求

涉及C2、C3类别信息的Web应用的安全技术要求如下：

a) 应具备对网站页面篡改、网站页面源代码暴露、穷举登录尝试、重放攻击、SQL 注入、跨站脚本攻击、钓鱼、木马以及任意文件上传、下载等已知漏洞的防范能力。
b) 处理个人金融信息相关的 Web 应用系统与组件上线前应进行安全评估。
c) 应具备对处理个人金融信息的系统组件进行实时监测的能力，有效识别和阻止来自内外部的非法访问。

6.2.3 客户端应用软件安全要求

与个人金融信息相关的客户端应用软件及应用软件开发工具包（SDK）应符合 JR/T 0092—2019、JR/T 0068—2020 客户端应用软件有关安全技术要求，并在上线前进行安全评估。

6.2.4 密码技术与密码产品要求

使用的密码技术及产品应符合国家密码管理部门与行业主管部门要求。

7 安全管理要求

7.1 安全准则

7.1.1 收集

个人金融信息收集的方式包括但不限于通过柜面、信息系统、金融自助设备、受理终端、客户端应用软件等渠道获取。金融业机构应遵循合法、正当、必要的原则，向个人金融信息主体明示收集与使用个人金融信息的目的、方式、范围和规则等，获得个人金融信息主体的授权同意，并满足以下要求：

a) 收集个人金融信息的基本规则如下：
   - 不应欺诈、诱骗，或以默认授权、功能捆绑等方式误导强迫个人金融信息主体提供个人金融信息；
   - 不应隐瞒金融产品或服务所具有的收集个人金融信息的功能；
   - 不应通过非法渠道间接获取个人金融信息；
   - 不应收集法律法规与行业主管部门有关规定明令禁止收集的个人金融信息。

b) 收集个人金融信息应遵循最小化要求，收集个人金融信息的目的应与实现和优化金融产品或服务、防范金融产品或服务的风险有直接关联。直接关联是指无该个人金融信息参与无法实现前述目的。

c) 收集个人金融信息时授权同意的具体要求如下：
   - 收集个人金融信息前，应向个人金融信息主体明确告知金融产品或服务需收集的个人金融信息类别，以及收集、使用个人金融信息的规则（如：收集和使用个人金融信息的目的、收集方式、自身的数据安全能力、对外共享、转让、公开披露的规则、投诉与申诉的渠道及响应时限等），并获得个人金融信息主体的明示同意。
   - 间接获取个人金融信息时，应要求个人金融信息提供方说明个人金融信息来源，并对其个人金融信息来源的合法性进行确认；应了解个人金融信息提供方已获得的授权内容，包括使用目的，个人金融信息主体是否授权同意转让、共享、公开披露等情况；因业务需要金融业机构确需超出原授权范围处理个人金融的，应在使用个人金融信息前，征得个人金融信息主体的明示同意。

d) 以下情形收集使用个人金融信息无需征得个人金融信息主体的授权同意：
   - 与履行国家法律法规及行业主管部门有关规定的义务相关的；
   - 与国家安全、国防安全直接相关的；
   - 与公共安全、公共卫生、重大公共利益直接相关的；
   - 与犯罪侦查、起诉、审判和判决执行等直接相关的；
   - 出于维护个人金融信息主体或其他主体的生命、财产等重大合法权益但又很难得到本人同意的；
   - 个人金融信息主体自行向社会公众公开的；
   - 根据个人金融信息主体要求签订和履行合同所必需的；
   - 从合法公开披露的信息中收集个人金融信息的，如合法的新闻报道、政府信息公开等渠道；
   - 用于维护所提供的金融产品或服务的安全稳定运行所必需的，例如识别、处置金融产品或服务中的欺诈或被盗用等。

7.1.2 存储

个人金融信息的存储时限应满足国家法律法规与行业主管部门有关规定要求，并符合个人金融信息主体授权使用的目的所必需的最短时间要求。超过该期限后，应对收集的个人金融信息进行删除或匿名化处理。

7.1.3 使用

个人金融信息在信息展示、共享与转让、公开披露、委托处理、加工处理、汇聚融合等方面，应遵循6.1.4.1—6.1.4.6的要求，并满足以下要求：

a) 除法律法规与行业主管部门另有规定或开展金融业务所必需的数据共享与转让（如转接清算等）外，金融业机构原则上不应共享、转让其收集的个人金融信息，确需共享、转让的，应充分重视信息安全风险，具体要求如下：
   - 应向个人金融信息主体告知共享、转让个人金融信息的目的、数据接收方的类型，并事先征得个人金融信息主体明示同意，共享、转让经去标识化处理（不应仅使用加密技术）的个人金融信息，且确保数据接收方无法重新识别个人金融信息主体的除外。
   - 应帮助个人金融信息主体了解数据接收方对个人金融信息的存储、使用等情况，包括个人金融信息主体的权利，例如访问、更正、删除、注销账户等；在法律法规规定、行业主管部门有关规定及个人金融信息主体约定的范围内，个人金融信息主体行使其个人金融信息控制权利，金融业机构应配合响应其请求。
   - C3 类别信息以及 C2 类别信息中的用户鉴别辅助信息不应共享、转让。
   - 转接清算、登记结算等情况，应依据国家有关法律法规与行业主管部门有关规定与技术标准执行。
   - 当因收购、兼并、重组、破产等情况，对个人金融信息主体提供金融产品或服务的金融业机构主体变更而发生个人金融信息共享、转让时，具体要求如下：
     ——金融业机构将其提供的金融产品或服务移交至其他金融业机构的情况，应使用逐一传达（或公告）的方式通知个人金融信息主体。
     ——承接其金融产品或服务的金融业机构，应对其承接运营的金融产品或服务继续履行个人金融信息保护责任；如变更其在收购、兼并重组过程中获取的个人金融信息使用目的，应重新获得个人金融信息主体明示同意（或授权）。
b) 金融业机构原则上不应公开披露其收集的个人金融信息，经法律授权或具备合理理由确需公开披露个人金融信息的，具体要求如下：
   - 应向个人金融信息主体告知公开披露个人金融信息的目的、类别，并事先征得个人金融信息主体的同意，并向其告知涉及的信息内容；
   - 承担因公开披露个人金融信息对个人金融信息主体合法权益造成损害的相应责任；
   - C3 类别信息，以及 C2 类别信息中的用户鉴别辅助信息不应公开披露。
c) 因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（包含外包服务机构与外部合作机构）处理的，具体要求如下：
   - 依据 6.1.4.4 开展委托处理工作。
   - 应对第三方机构等受委托者提出如下要求：
     ——应严格按照金融业机构的要求处理个人金融信息，如因特殊原因受委托者未能按照要求处理个人金融信息，应及时告知金融业机构，并配合金融业机构进行信息安全评估，并采取补救措施以保护个人金融信息的安全，必要时应终止其对个人金融信息的处理；

——未经书面授权，受委托者不应将其处理的个人金融信息再次委托给其他机构进行处理；

——应协助响应个人金融信息主体的请求；

——如受委托者在处理个人金融信息过程中无法提供足够的信息安全保护水平或发生安全事件，应及时告知金融业机构，配合进行信息安全评估与安全事件调查，并采取补救措施以保护个人金融信息的安全，必要时应终止其对个人金融信息的处理；

——在委托关系解除时（或外包服务终止后），受委托者应按照金融业机构的要求销毁其处理的个人金融信息，并依据双方协商的期限承担后续的个人金融信息保密责任；

——应准确记录和保存委托处理个人金融信息的情况。

d) 在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，应在境内存储、处理和分析。因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，具体要求如下：

- 应符合国家法律法规及行业主管部门有关规定；
- 应获得个人金融信息主体明示同意；
- 应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；
- 应与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除、案件协查等职责义务。

e) 以下情形中，金融业机构共享、转让、公开披露个人金融信息无需征得个人金融信息主体的授权同意：

- 与履行法律法规及行业主管部门规定的义务相关的；
- 与国家安全、国防安全直接相关的；
- 与公共安全、公共卫生、重大公共利益直接相关的；
- 与犯罪侦查、起诉、审判和判决执行等直接相关的；
- 出于维护个人金融信息主体或其他主体的生命、财产等重大合法权益但又很难得到本人同意的；
- 个人金融信息主体自行向社会公众公开的；
- 从合法公开披露的信息中收集个人金融信息的，如合法的新闻报道、政府信息公开等渠道。

7.2 安全策略

7.2.1 安全制度体系建立与发布

金融业机构应建立个人金融信息保护制度体系，明确工作职责，规范工作流程。制度体系的管理范畴应涵盖本机构、外包服务机构与外部合作机构，并确保相关制度发布并传达给本机构员工及外部合作方。相关制度应至少包括个人金融信息保护管理规定、日常管理及操作流程、外包服务机构与外部合作机构管理、内外部检查及监督机制、应急处理流程和预案。具体要求如下：

a) 制定个人金融信息保护管理规定，提出本机构个人金融信息保护工作方针、目标和原则。

b) 开展个人金融信息分类分级管理。应针对不同类别和敏感程度的个人金融信息，实施相应的安全策略和保障措施。

c) 建立日常管理及操作流程。应对个人金融信息的收集、传输、存储、使用、删除、销毁等环节提出具体保护要求，制定个人金融信息时效性管理规程，确保符合法律法规和行业主管部门有关规定。

d) 建立信息系统分级授权管理机制。应在不影响履行反洗钱等法定义务的前提下，制定本机构人员个人金融信息调取权限与使用范围，并制定专门的授权审批流程。

e) 建立个人金融信息脱敏（如屏蔽、去标识、匿名化等）管理规范和制度，应明确不同敏感级别个人金融信息脱敏规则、脱敏方法和脱敏数据的使用限制。

f) 依据国家与行业有关标准，建立个人金融信息安全影响评估制度，应定期（至少每年一次）开展个人金融信息安全影响评估。

g) 建立外包服务机构与外部合作机构管理制度，包括但不限于：

- 应对个人金融信息生命周期过程中相关的外包服务机构与外部合作机构进行审查与评估，评估其个人金融信息的保护能力是否达到国家、行业主管部门与金融业机构的要求；应通过协议或合同的方式，约束外包服务机构与外部合作机构不应留存 C2、C3 类别信息；对于 C2 类别信息中的支付账号等信息，若因清分清算、差错处理等业务需要确需留存，金融业机构应明确其保密义务与保密责任，并应根据安全要求落实安全控制措施，并将有关资料留档备查；对可能访问个人金融信息的外包服务机构、外部合作机构及其人员，金融业机构应要求外包服务机构与外部合作机构向有关人员传达个人金融信息保护安全要求，与其签署保密协议，并对协议履行情况进行监督。
- 不应将存储个人金融信息的数据库交由外部合作机构运维。
- 应定期对外包服务机构与外部合作机构的个人金融信息保护措施落实情况进行确认，确认的方式包括但不限于外部信息安全评估、现场检查等。
- 国家法律法规与行业主管部门另有规定的，按照相关要求执行。

h) 建立个人金融信息安全检查及监督机制。应建立个人金融信息安全日常检查机制和工作流程、定期评估个人金融信息管理方面存在的不足，及时调整检查机制和工作流程。

i) 应将个人金融信息泄露等相关事件处理纳入机构信息安全事件应急处置工作机制，制定专门的流程和预案。定期评估应急处理流程和预案，及时保障、有效应对个人金融信息安全事件，降低安全事件造成的损失及不利影响。

j) 建立个人金融信息投诉与申诉处理程序，明确投诉与申诉受理部门、处理程序，对个人金融信息主体要求更正或删除金融业机构收集其个人金融信息的情况，应受理、核实，并依据国家与行业主管部门要求予以处理。

k) 明确个人金融信息共享、存储、使用和销毁的期限，具备个人金融信息存储时效性的控制能力。

7.2.2 组织架构岗位设置

组织架构及岗位设置具体要求如下：

a) 应建立个人金融信息保护组织架构，明确机构各层级内设部门与相关岗位个人金融信息保护职责与总体要求。

b) 应明确个人金融信息保护责任人和个人金融信息保护责任机构，并履行以下工作职责：

- 负责制定和管理本机构个人金融信息安全管理制度；
- 制定、实施、定期更新隐私政策和相关规程；
- 监督本机构内部，以及本机构与外部合作方个人金融信息安全管理；
- 开展信息安全管理内部审计、分析处理信息安全相关事件；
- 组织开展个人金融信息安全影响评估，提出个人金融信息保护的对策建议；
- 组织在金融产品或服务上线发布前进行技术检测，避免未知（与金融产品或服务功能及隐私政策不符）的个人金融信息收集、使用、共享等处理行为；
- 公布投诉与申诉方式等信息并及时受理个人金融信息有关的投诉、申诉。

c) 应明确在提供金融产品和服务的过程中知悉个人金融信息的岗位，并针对相关岗位明确其个人金融信息安全管理责任与保密责任，如不得未经授权的复制、存储、使用个人金融信息，不得向他人出售或者以其他形式未经授权的共享、转让、披露个人金融信息等。

7.2.3 人员管理

对涉及个人金融信息相关人员的安全管理，具体要求如下：

a) 录用员工前，应进行必要的背景调查，并与所有可访问个人金融信息的员工签署保密协议，或在劳动合同中设置保密条款。
b) 应定期开展内外部个人金融信息保护培训与意识教育活动，并保留相关记录。
c) 在发生人员调离岗位时，应立即调整和完成相关人员的个人金融信息访问、使用等权限的配置，并明确有关人员后续的个人金融信息保护管理权限和保密责任；若有关人员调整后的岗位不涉及个人金融信息的访问与处理的，应明确其继续履行有关信息的保密义务要求。
d) 与员工终止劳动合同时，应立即终止并收回其对个人金融信息的访问权限，并明确其继续履行有关信息的保密义务要求。
e) 系统开发人员、系统测试人员与运维人员之间不应相互兼岗。
f) 应定期（至少每年一次）或在隐私政策发生重大变化时，对个人金融信息处理岗位上的相关人员开展个人金融信息安全专业化培训和考核，确保相关人员熟练掌握隐私政策和相关规程。

7.3 访问控制

加强个人金融信息访问控制管理，具体要求如下：

a) 应根据“业务需要”和“最小权限”原则，进行个人金融信息相关的权限管理，严格控制和分配访问、使用个人金融信息的权限。
b) 对于可访问和处理个人金融信息的系统应设置基于角色的访问控制策略，禁止账户共用。
c) 传输、处理、存储个人金融信息的系统默认用户权限应为“拒绝所有访问”。
d) 对个人金融信息使用的权限管理应设置权限指派、回收、过期处理等安全功能。
e) 对存储或处理个人金融信息的系统或设备进行远程访问时，应通过专线、VPN 等方式访问，个人金融信息不应在远程访问设备上留存。
f) 应对生产网络、开发测试网络、办公网络以及相关非生产网络进行访问控制。
g) 应对个人金融信息访问与个人金融信息的增删改查等操作进行记录，并保证操作日志的完整性、可用性及可追溯性，操作日志包括但不限于业务操作日志、系统日志等；系统运维管理类日志不应记录个人金融信息。
h) 应对存储个人金融信息的数据库及操作日志实施严格的用户授权与访问控制。
i) 存储或处理个人金融信息的相关物理设备或介质应在获得审批授权后方可移入或移出机房受控区域，留存有 C2、C3 类别信息的物理设备或介质移入或移出区域应具有同等的安全保障措施。

7.4 安全监测与风险评估

7.4.1 监控与审计

监控与审计具体要求如下：

a) 应识别并记录包括但不限于管理员用户、业务用户对个人金融信息的访问。
b) 应对个人金融信息数据交换网络流量进行安全监控和分析，并存储匹配安全规则的数据，以备事件溯源。

c) 日志文件和匹配规则的数据应至少保存 6 个月，应定期对所有系统组件日志进行审计，包括但不限于存储、处理或传输个人金融信息的系统组件日志、执行安全功能的系统组件日志（如防火墙、入侵检测系统、验证服务器等）、安全事件日志等。

d) 应采取技术手段对个人金融信息全生命周期进行安全风险识别和管控，如恶意代码检测、异常流量监测、用户行为分析等。

7.4.2 安全检查和评估

金融业机构应对个人金融信息生命周期全过程进行安全检查和评估，范围包括金融业机构以及与其合作的第三方机构（包含外包服务机构与外部合作机构）。

个人金融信息的安全检查和评估具体要求如下：

a) 应依据制定的个人金融信息安全影响评估制度，在个人金融信息委托处理、共享与转让、公开披露等过程中，执行个人金融信息安全影响评估活动，并将评估报告归档保存。个人金融信息安全影响评估可由金融业机构自行组织开展，也可委托外部安全评估机构执行。

b) 应每年至少开展一次对涉及收集、存储、传输、使用个人金融信息的信息系统进行安全检查或安全评估，包括但不限于以下方式及其组合：

- 对信息系统进行信息安全评估、漏洞扫描和渗透测试，并及时采取补救措施；
- 在信息系统组件或运行环境发生重大变更（或发现新的高安全等级威胁和漏洞）时，重新进行信息安全风险评估；
- 将个人金融信息保护纳入金融业机构内部安全审计工作，定期开展安全审计，形成审计报告，并根据审计结果完善制度、流程。

c) 对于个人金融信息中的支付信息部分，应采取自行评估或委托外部机构进行检查评估，金融业机构以及与其合作的第三方机构应每年至少开展一次支付信息安全合规评估，对评估过程中发现的问题及时采取补救措施并形成报告存档备查。

d) 出现个人金融信息泄露事件，造成一定经济损失（或社会影响）时，应及时委托外部安全评估机构重新进行相关安全评估与检查活动，并将结果报送行业主管部门。

7.5 安全事件处置

安全事件处置具体要求如下：

a) 应制定个人金融信息安全事件应急预案，明确安全事件处置流程和岗位职责。

b) 应定期组织内部相关人员进行个人金融信息保护应急预案相关培训和应急演练。

c) 发生个人金融信息遗失、损毁、泄露或被篡改等安全事件后，应及时采取必要措施进行处置，控制事态发展，消除安全隐患，并及时告知受影响的个人金融信息主体，告知的内容应符合 GB/T 35273—2017 关于安全事件告知内容的规定，告知的方式包括但不限于：

- 以邮件、信函、电话、推送消息等方式及时告知受影响的个人金融信息主体；
- 难以逐一告知个人金融信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。

d) 发现因系统漏洞或人为原因造成个人金融信息泄露时，应立即采取有效措施防止风险扩大，并向行业主管部门报告。

e) 应记录事件内容，分析和鉴定事件产生的原因，评估事件可能造成的影响，制定补救措施，并按国家与行业主管部门规定及时进行报告。

f) 应建立投诉与申诉管理机制，包括跟踪流程，并在规定的时间内，对投诉、申诉进行响应。

g) 根据相关法律法规与行业主管部门有关规定的变化情况以及事件处置情况，及时评估并更新应急预案。

附 录 A
（资料性附录）
信息屏蔽

信息屏蔽指对某些敏感信息通过既定规则屏蔽（或截词）全部（或部分）敏感信息，实现对敏感信息展示的可靠保护。通过信息屏蔽可使信息本身的安全等级降级，从而可以在开发、测试和其他非生产环境以及外包或云计算环境中安全地使用脱敏后的信息集。借助信息屏蔽（或截词）技术，屏蔽敏感信息，并使屏蔽的信息保留其原始个人金融信息格式和属性，以确保应用程序可在使用脱敏个人金融信息的开发与测试过程中正常运行。

注：截词的目的在于永久删除某条信息的某个数据段，仅存储部分数据（如仅保留银行卡卡号不超过前六位和后四位数）。

对外输出的任何个人金融信息原则上应事先做屏蔽（或截词）等脱敏处理（已经获得用户明示同意以及根据法律法规要求需要对外输出的信息除外），脱敏处理包括但不限于：

——模糊化：指通过隐藏（或截词）局部信息令该个人金融信息无法完整显示，包括但不限于：

- 具体名称 ID 化（如：以 12345 代替客户法定名称或 ID），具体 ID 哈希化，金额、笔数去绝对值化（如：区间分段、个位数及小数点取整等）、星号模糊化；
- 信息隐藏规则（缺省）：显示前 1/3 和后 1/3（向下取整），其他用*号代替，这样保留了部分信息，并且保证了信息的长度不变性，对信息持有者更易辨别，如手机、身份证号码等。

——不可逆：指无法通过样本信息倒推真实信息的方法，包括但不限于：

- 使用匿名、差分隐私等技术对真实信息进行处理，使其无法被识别，且处理后的信息不能被复原；
- 不应通过信息拼接、关联得到完整的敏感信息记录；
- 不应通过局部占比的信息得到全量信息。

针对特定类型信息的隐藏规则示例详见表A.1。

表 A.1 个人金融信息隐藏规则及示例

敏感信息类型	信息范围	展示规范
银行卡信息	银行卡卡号	显示前 6 位+*（实际位数）+后 4 位。如： 622575******1496
个人身份信息	1）身份证号码、军官证号码、护照号码	使用缺省信息隐藏规则，如隐藏出生日期，身份证号码屏蔽后 6 位
	2）客户法定名称（姓名）	隐藏部分字符
	3）手机号码	除区号外，至少隐藏中间四位 大陆：显示前 3 位 +****+后 4 位。如：137****9050 香港、澳门：显示前 2 位＋****+后 2 位。如：90****85 台湾：显示前 2 位＋****+后 3 位。如：90****856 其他海外地区：使用缺省隐藏规则
	4）固定电话号码	推荐的规范：显示区号和后 2 位

敏感信息类型	信息范围	展示规范
	5）电子邮箱	@前面的字符显示前3位，3位后显示3个*，@后面完整显示如：con***@111.com 如果少于三位，则全部显示，@前加***，例如tt@111.com则显示为tt***@111.com

参 考 文 献

[1] GB/T 13016—2018 标准体系构建原则和要求

[2] GB/T 13017—2018 企业标准体系表编制指南

[3] GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第1部分：简介和一般模型

[4] GB/T 25000.10—2016 系统与软件工程 系统与软件质量要求和评价(SQuaRE) 第10部分：系统与软件质量模型

[5] GB/T 26237.1—2010 信息技术 生物特征识别数据交换格式 第1部分：框架

[6] GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统 个人信息保护指南

[7] GM/Z 0001—2013 密码术语

[8] JR/T 0061—2011 银行卡名词术语

[9] JR/T 0088.1—2012 中国金融移动支付 应用基础 第1部分：术语

[10] JR/T 0156—2017 移动终端支付可信环境技术规范

[11] ISO/IEC 19785-2：2006 Information technology—Common biometric exchange formats framework—Part 2：Procedures for the operation of the biometric registration authority

[12] ISO/IEC 27018：2014 Information technology—security techniques—Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[13] ISO/IEC 29100：2011 Information technology—Security techniques—Privacy framework

[14] 中国人民银行.中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知(银发〔2011〕17号)，2011-01-21

[15] 中国人民银行.中国人民银行关于银行业金融机构进一步做好客户个人金融信息保护工作的通知(银发〔2012〕80号)，2012-03-27

[16] 征信业管理条例(国务院令 第631号)，2013-01-21

[17] 中国人民银行.中国人民银行关于进一步加强银行卡风险管理的通知(银发〔2016〕170号)，2016-06-13

[18] 中国人民银行.中国人民银行关于印发《中国人民银行金融消费者权益保护实施办法》的通知(银发〔2016〕314号)，2016-12-14

[19] 中国人民银行.中国人民银行关于印发《金融科技(FinTech)发展规划(2019—2021年)》的通知(银发〔2019〕209号)，2019-08-19

[20] 金融机构客户身份识别和客户身份资料及交易记录保存管理办法(中国人民银行 中国银行业监督管理委员会 中国证券监督管理委员会 中国保险监督管理委员会令〔2007〕第2号)，2007-06-21