

个人金融信息保护技术规范

JR/T 0171—2020

目 次

前言.....	II
引言.....	III
1 范围.....	1
2 规范性引用文件.....	1
3 术语和定义.....	1
4 个人金融信息概述.....	5
5 安全基本原则.....	7
6 安全技术要求.....	7
7 安全管理要求.....	12
附录 A（资料性附录） 信息屏蔽.....	18
参考文献.....	20

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程序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) 财产信息指金融业态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、公积金缴存金额等。
- f) 借贷信息指个人金融信息主体在金融业态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：

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

<https://d.book118.com/558131120036006054>