个人金融信息保护标准的进一步升级

——简评《个人金融信息保护技术规范》

作者：蓝洁 任建南 安旭东

2020 年 2 月 13 日，中国人民银行发布了《个人金融信息保护技术规范》（JR/T 0171—2020，以下简称“《规范》”），该《规范》于同日开始实施。《规范》由中国人民银行提出，并由全国金融标准化技术委员会归口管理，多家金融行业相关组织与单位参与了起草工作。近年来，中国人民银行等监管部门持续加大对非法泄露买卖个人金融信息、银行卡盗刷、电信诈骗等违法行为的整治力度，同时加强对个人金融信息保护制度的研究。《规范》的发布做到了标准先行、技术先行，按照安全基本原则、安全技术要求、安全管理要求的框架，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。

尽管《规范》在性质上属于推荐性标准，但其对金融业机构建设个人金融信息保护架构的重要意义不言而喻，也为有关部门在未来的相关立法和执法提供了重要参考。因此，建议金融业机构以及其他相关机构按照《规范》的标准及时做好合规准备。

一、 个人金融信息保护的监管规定

在个人金融信息保护领域，我国目前尚未制定专门的法律或行政法规[1]。总体而言，与个人金融信息保护有关的专门针对性规定主要出现在一行两会制定的各类规范性文件中[2]，具体如下表格所列：

时间	部门	名称
2007 年 6 月	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	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
2010 年 6 月	中国银行业监督管理委员会	银行业金融机构外包风险管理指引
2011 年 1 月	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
2012 年 3 月	中国人民银行	中国人民银行关于金融机构进一步做好客户个人金融信息保护工作的通知
2013 年 8 月	中国银行业监督管理委员会	中国银行业监督管理委员会关于印发银行业消费者权益保护工作指引的通知
2016 年 12 月	中国人民银行	中国人民银行金融消费者权益保护实施办法[3]
2018 年 5 月	中国银行保险监督管理委员会	中国银行保险监督管理委员会关于印发银行业金融机构数据治理指引的通知

此外，相关主管部门会同国家标准化管理委员会、全国金融标准化委员会等单位牵头制定的与信息保护有关的国家标准、行业标准等技术指导性文件，也为相关机构在实践中提供了大量参考与借鉴，此类文件包括但不限于《金融行业信息系统信息安全等级保护实施指引》（JR/T 0071—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》（GB/Z 28828—2012）、《信息安全技术 信息技术产品供应方行为安全准则》（GB/T 32921—2016）等。

---

[1] 《民法总则》第 111 条、《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（法释〔2014〕11 号）确立了对于个人信息的民事法律保护以及侵权责任承担等救济形式。《刑法》第 253 条及《最高人民法院 最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释〔2017〕10 号）则从刑事角度提供了对个人信息的侵害行为规制和司法保护。

[2] 除一行两会所制定的针对性的规定之外，我国在不同领域的法律法规也对个人金融信息保护有所涉及，例如：（1）《商业银行法》（对存款人的保密义务）；（2）《反洗钱法》（对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息保密）；（3）《网络安全法》（对关键信息基础设施运营者及网络运营者涉及个人信息的收集、使用等进行规制，规定了网络运营者的个人信息保密义务）；（4）《征信业管理条例》（对征信涉及的个人信息的收集、使用等进行规制）；（5）《APP 违法违规收集使用个人信息行为认定方法》《个人信用信息基础数据库管理暂行办法》。

[3] 2019 年 12 月 27 日，中国人民银行发布了关于《中国人民银行金融消费者权益保护实施办法（征求意见稿）》公开征求意见的通知，截至目前该办法正在修订过程中。根据中国人民银行发布的起草说明，修订增补相关条款后，将《中国人民银行金融消费者权益保护实施办法》的主体内容升格为部门规章，拟以人民银行令形式发布实施。

此次发布的《规范》，在制定过程中也参考、引用了现行的部分监管规定与指导性文件，同时结合了金融业特点以及金融领域近年来不断发展的新技术与新模式，成为我国第一部专门针对个人金融信息保护的行业标准。

二、《规范》的主要内容

（一） 适用范围

《规范》明确**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。

根据《规范》第 3.1 条的规定，**金融业机构**包括两种：一种是指由国家金融管理部门监督管理的持牌金融机构，另一种是指涉及个人金融信息处理的相关机构。根据《规范》第 3.2 条，**个人金融信息**是指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。

从上述内容可以看出，《规范》的适用范围主要包括两大类：

- **传统意义上的持牌金融机构**，例如银行、城市信用合作社、农村信用合作社、证券公司、保险公司、金融资产管理公司、金融租赁公司等；
- **其他通过提供金融产品和服务或者其他渠道获取、加工和保存个人信息的机构**，例如第三方支付机构、为持牌金融机构提供信息技术服务的外包服务机构或外部合作机构等。

（二） 对个人金融信息的分类管理

《规范》还对个人金融信息内容进行了列举，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，并以“其他反映特定个人金融信息主体某些情况的信息[4]”作为兜底。

[4] 其他信息包括：（1）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；（2）在提供金融产品与服务过程中获取、保存的其他个人信息。

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，《规范》将个人金融信息**按照敏感程度由高到低分为 C3、C2、C1 三个类别**，并提出了不同的保护要求，大致归纳如下表所示：

信息类别	敏感程度	主要信息内容	保护要求示例
C3（用户鉴别信息）	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**	（1）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； （2）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； （3）用于用户鉴别的个人生物识别信息	不应共享、转让，不应公开披露，不应委托处理
C2（可识别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）	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**	（1）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； （2）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； （3）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）； （4）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； （5）用户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； （6）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； （7）其他能够识别特定主体的信息，如家庭地址等	除用户鉴别辅助信息外，经告知并征得同意后，可以共享、转让、公开披露，可以委托处理
C1（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）	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**	（1）账户开立时间、开户机构； （2）基于账户信息产生的支付标记信息； （3）C2 和 C3 类别信息中未包含的其他个人金融信息	经告知并征得同意后，可以共享、转让、公开披露，可以委托处理

《规范》还特别强调，**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。

（三） 对个人金融信息在生命周期各环节的防护要求

根据《规范》第 4.3 条的规定，个人金融信息生命周期是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。《规范》所要求的安全基本原则是，金融业机构应遵循 GB/T 35273—2017 的要求（即《信息安全技术 个人信息安全规范》，目前已被 GB/T 35273—2020 代替），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。

《规范》从**安全技术要求**和**安全管理要求**两个方面，对个人金融信息在生命周期各环节的保护提出了规范性的要求。我们将部分重点环节所涉及的要求简要提示如下：

1、对个人金融信息的委托收集与委托处理

现实中，金融业机构委托第三方收集和处理个人金融信息，例如将催收业务外包给第三方，是较为常见的业务安排，也是近年来各种违规风险的多发地带。《规范》明确，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，例如身份证号、手机号码等可识别特定个人身份的信息。可见，《规范》对这一类安排提出了更高的合规监管要求。

首先，《规范》要求，**金融业机构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**。这一规定将会对目前的一些外包业务模式带来影响。不过，《规范》并没有对“金融业相关资质”的具体含义作出明确解释，因此，金融业机构可以委托哪些第三方机构从事相关信息的收集，还有待进一步明确。

其次，对于金融业机构将收集到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）进行处理的行为，《规范》也提出了具体的技术要求，主要包括：

- 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《规范》中对于征得授权同意的例外所规定的情形；
- 要求处理 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；
- 对委托处理的信息采用去标识化脱敏处理，且不应仅使用加密技术；
- 应对委托行为进行安全影响评估，确保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；
- 应对第三方机构等受委托者进行监督，包括设置合同义务方面及安全检查评估方面；
- 应对外部嵌入或接入的自动化工具开展技术检测，并对其进行审计。

除依据上述相关要求开展委托处理工作之外，《规范》还要求对第三方机构等受委托者提出额外要求，大致包括：

- 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，并配合进行信息安全评估、采取补救措施，必要时终止信息处理；
- 未经书面授权，受委托者不应将个人金融信息再次委托给其他机构处理；
- 应协助响应个人金融信息主体的请求；
- 若处理过程中无法提供足够的信息安全保护水平或者发生安全事件，应当及时告知金融业机构、配合调查、采取补救措施，必要时终止信息处理；
- 委托关系解除时（或外包服务终止后）应按照金融业机构的要求销毁信息并在协商期限内承担保密责任；
- 应准确记录和保存委托处理个人金融信息的情况。

在安全策略上，《规范》要求金融业机构建立外包服务机构与外部合作机构管理制度，并提出了具体的要求。例如，要求通过协议或合同的方式约束该等机

构不应留存 C2、C3 类信息，存储个人金融信息的数据库不得交由外部合作机构运维，对外包服务机构与外部合作机构定期开展外部信息安全评估、现场检查，等等。

2、建立个人金融信息保护制度体系

《规范》从四个方面对个人金融信息保护制度体系的建设提出了较为细致的要求。

在安全制度体系的建立与发布方面，《规范》要求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。

在组织架构及岗位设置方面，《规范》要求设立个人金融信息保护责任人和个人金融信息保护责任机构，并明确其工作职责，包括但不限于：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、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。

在人员管理方面，《规范》的要求主要包括：在录用员工前应进行必要的背景调查，与所有可访问个人金融信息的员工签署相关保密协议；定期开展内外部培训和教育活动，保留相关记录；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。在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，并明示其继续履行有关信息的保密义务要求；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；定期开展专业化培训和考核。

在访问控制方面，《规范》还要求加强个人金融信息访问控制管理，并提出了较为具体的要求。

3、金融数据出境

在《金融信息技术规范》出台以前，与个人金融数据出境相关的规定主要出现在《网络安全法》《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》《中国人民银行金融消费者权益保护实施办法》等规范性文件中。此外，一些尚在制定中的规范性文件及国家标准，包括《个人信息和重要数据出

境安全评估办法（征求意见稿）》《个人信息出境安全评估办法（征求意见稿）》《信息安全技术 数据出境安全评估指南（征求意见稿）》等，也提出了更具针对性的要求。

《规范》要求，**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。

值得留意的是，根据《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》，在反洗钱和反恐怖融资领域要求金融机构保存获得的客户身份资料和交易信息，与《规范》中所述的个人金融信息存在重合之处。因此，相关机构在特定情况下向境外提供、传输相关信息时，还**应注意满足反洗钱和反恐怖融资等其他相关法规在信息保存与管理等方面的要求**[5]。

三、总结与展望

就在《规范》发布后不久，国家市场监督管理总局、国家标准化管理委员会于 2020 年 3 月 6 日正式发布了新版《信息安全技术 个人信息安全规范》（GB/T

[5] 例如《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》中要求评估境外金融机构接受反洗钱监管的情况和反洗钱、反恐怖融资措施的健全性和有效性，以书面方式明确本金融机构与境外金融机构在客户身份识别、客户身份资料和交易记录保存方面的职责。而《银行业金融机构反洗钱和反恐怖融资管理办法》《支付机构反洗钱和反恐怖融资管理办法》等相关法规也要求相关金融机构对在依法履行反洗钱和反恐怖融资义务获得的客户身份资料和交易信息严格依法保密。

35273-2020，以下简称“**《个人信息安全规范》**”），并定于 2020 年 10 月 1 日起实施。如前面所述，《规范》中已明确要求金融业机构应遵循《个人信息安全规范》的要求——即**《个人信息安全规范》是基本原则，《规范》是针对个人金融信息保护而制定的特别标准**。可以看出，《规范》和《个人信息安全规范》的发布，标志着我国对包括个人金融信息在内的个人信息安全保护标准进行了全面升级。

伴随着未来金融科技的不断发展，商业模式的层出不穷，相关行业的逐步开放，个人金融信息保护领域存在着诸多挑战。今年 4 月 1 日，证监会已如期取消了证券公司的外资股比限制，这也是近年来我国进一步扩大金融业对外开放大背景下的一个缩影。同时，在传统的持牌机构之外，相关主管部门也在加大对金融科技的监管力度，健全金融科技监管基本规则体系，打造包容审慎的金融科技创新监管工具。因此，在个人金融信息保护领域，及时关注法律规范与技术标准的更新，依法建立完备的内部制度体系，充分了解并控制实践中各个环节的合规风险，对于每一个境内外金融业机构而言都至关重要。