君合专题研究报告
JUNHE

2021年4月21日

个人金融信息合规系列

——金融机构应如何处理个人金融信息

前言

随着《网络安全法》、《民法典》、《个人信息安全规范》的推广实施，如何合法处理个人信息成为企业合规的重要课题。在金融领域，个人金融信息的泄露不仅严重损害消费者个人权益，更有可能影响行业的正常运营，对此，中国人民银行先后制定实施了以下部门规章、行业规范：2019年11月1日实施《金融消费者权益保护实施办法》（中国人民银行令〔2020〕第5号，以下简称“**《金融消保办法》**”）、2020年2月13日公布实施《个人金融信息保护技术规范》（JR/T 0171—2020，以下简称“**《金融信息保护规范》**”）、2021年4月8日公布实施《金融数据[1]安全-数据生命周期安全规范》（JR/T 0223-2021，以下简称“**《金融数据安全规范》**”）。

上述三个规范文件中，《金融消保办法》属于部门规章，明确规定金融机构对消费者的个人金融信息的保护义务。《金融信息保护规范》、《金融数据安全规范》属于金融行业推荐性规范，虽然不具有强制力，但作为金融机构安全核查及评估的规范指引，构成金融监管实务中的重要参考依据。本文拟以《金融信息保护规范》为基础，结合《金融消保办法》、《金融数据安全规范》的相关规定，梳理个人金融信息的特殊保护要求，为金融机构处理个人金融信息提供参考。

一、近期个人金融信息违规处罚概况

近期，工业和信息化部（以下简称“**工信部**”）、中国人民银行加大了对侵害个人金融信息行为的处罚力度。根据《中国银行保险报》统计，2019年以来，工信部共点名通报444款App侵犯用户权益，其中涉及金融机构的有21款，覆盖银行、支付机构、网贷公司和基金等多种金融机构[2]。据《中国个人金融信息保护执法白皮书（2020）》不完全统计，2020年中国人民银行对于 “个人金融信息”违规行为共发出181张罚单（详见下表）[3]。

[1] 根据《金融数据安全-数据生命周期安全规范》，金融数据是指金融机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类数据，包括个人金融信息。

[2] https://baijiahao.baidu.com/s?id=1687318889193102056&wfr=spider&for=pc

[3] https://mp.weixin.qq.com/s/MMXctYUd1MSR2Uu2Re1vLw

处罚概况	截至2020年10月25日，涉及“个人金融信息”的行政处罚共181笔，总金额超过人民币1.8亿元。
主要违法行为	a) 未经审批查询个人金融信息 b) 未按规定保存客户身份资料和交易记录 c) 侵害消费者个人信息依法得到保护的权利等
处罚对象	银行、证券公司、支付机构、消费金融公司等

二、规制对象及个人金融信息分类

1、 规制对象

根据《金融信息保护规范》，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。具体而言，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。

《金融信息保护规范》规定，“金融业机构”是指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。由此可见，除了传统的持牌金融机构（比如银行、证券基金公司、保险公司等），处理个人金融信息的相关企业（比如第三方支付机构、金融科技公司等）也属于《金融信息保护规范》的规制对象。与此相比，《金融消保办法》的规制对象为银行、支付机构。

2、 信息分类

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，个人金融信息按敏感程度从高到低分为C3、C2、C1三个类别（详见下表）。

信息类别	定义及范围
C3 类别	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。
	a) 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。 b) 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。 c) 用于用户鉴别的个人生物识别信息。
C2 类别	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，
	a) 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。 b) 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。 c) 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。 d) 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。 e) 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。 f) 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。 g) 其他能够识别出特定主体的信息，如家庭地址等。
C1 类别	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。
	a) 账户开立时间、开户机构； b) 基于账户信息产生的支付标记信息； c) C2 和C3 类别信息中未包含的其他个人金融信息。

需要注意的是，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。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），金融机构应提升相应的信息传输、存储保障手段。

3、 与金融数据安全级别的关系

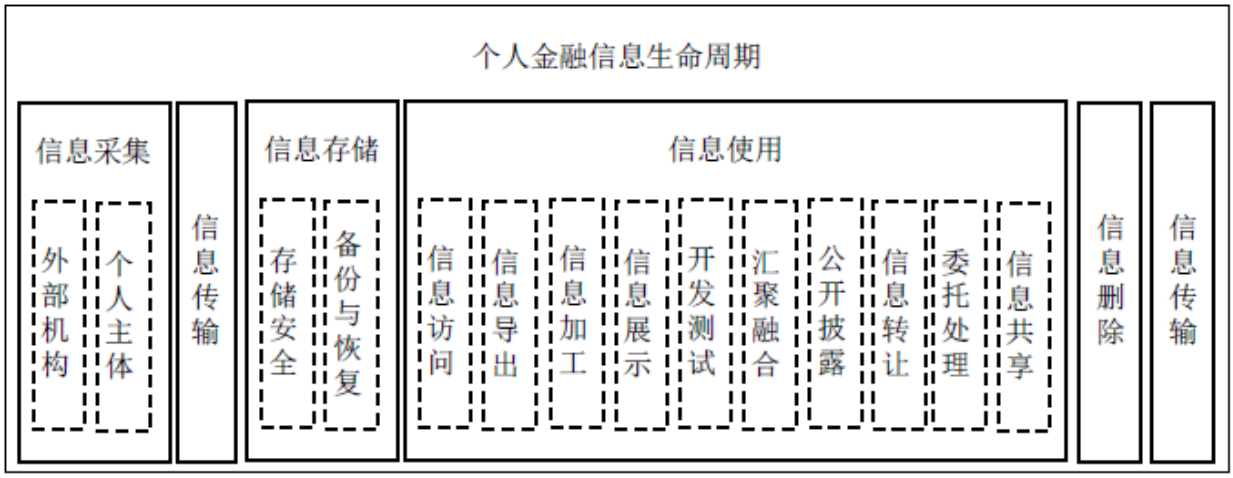
《金融数据安全规范》根据安全性遭到破坏后的影响范围和影响程度，将金融数据的安全级别由高到低划分为5级、4级、3级、2级、1级，并规定了相应的处理措施（详见下表）。需要注意的是，金融数据安全级别分类与上述个人金融信息的三级分类存在交叉，但相关规范没有规定5个安全级别与个人金融信息的三个分类如何对应。

安全级别	处理原则	备注
1级	公开数据，原则上无保密性要求，其安全防护应参考本文件有关完整性及可用性安全要求	涉及个人金融信息的内容，除满足本文件要求外，还应按照《金融信息保护规范》相关要求执行。
2级至4级	应在平衡安全需求与业务需求的基础上，根据数据安全级别不同，有侧重地采取适当的安全防护措施。 -2级数据应优先考虑业务需求 -4级数据应优先考虑安全需求	
5级	按照国家及行业主管部门的有关要求执行保护	

三、个人金融信息特殊处理规则

1、 个人金融信息生命周期

根据《金融信息保护规范》，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(详见下表)。



2、 信息处理的“明示同意”原则

《金融信息保护规范》规定，“明示同意”是指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。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。

关于处理个人金融信息需要获取的同意类型，《金融信息消保办法》第29条明确规定，“银行、支付机构处理消费者金融信息，应当遵循合法、正当、必要原则，经金融消费者或者其监护人明示同意”。《金融信息保护规范》也延续这一思路，规定在个人金融信息的收集、使用（对外共享、转让、公开披露、汇聚融合）、跨境提供等生命周期各环节，金融机构均应事先取得个人金融信息主体的明示同意。

(1) 收集：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。

(2) 汇聚融合：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。

(3) 使用：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信息的，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。

(4) 共享转让：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。

(5) 境外提供：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，应获得个人金融信息主体明示同意。

3、 C3、C2 类别信息的特殊要求

基于对个人金融信息的分类，《金融信息保护规范》对敏感度较高的C3、C2类信息的处理规定了更高的保护要求，金融业机构在制定个人信息保护制度、隐私政策、用户服务协议等时应予以高度关注。

(1) 收集：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。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。

(2) 传输：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。

(3) 存储：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。

(4) 委托处理：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。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。

(5) 加工处理：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。

四、个人金融信息的安全评估

个人金融信息安全影响评估是指，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。

《金融信息保护规范》规定，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）。根据《金融信息保护规范》，金融机构应从以下层面建立、实施个人金融信息评估制度。

1、评估制度建立。应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，应每年至少开展一次评估。

2、评估涉及的个人金融信息生命周期。金融业机构应依据制定的安全影响评估制度，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。

3、信息系统评估。金融业机构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。

4、敏感个人金融信息评估。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。

5、安全事件处理评估及补救。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，同时制定补救措施更新应急预案。

实务中，金融业机构可以在专家的协助下自行组织开展个人金融信息安全影响评估，也可委托外部安全评估机构执行。

五、侵害个人金融信息的罚则及合规建议

1、 处罚规则

根据《金融消保办法》第60条的规定，银行、支付机构侵害消费者金融信息依法得到保护的权利的，中国人民银行或分支机构应当依据《消费者权益保护法》第56条予以处罚（违规行为及处罚措施详见下表）。

违法行为	处罚措施
(1) 未经消费者明示同意，收集、使用其金融信息的。 (2) 收集与业务无关的消费者金融信息，或者采取不正当方式收集消费者金融信息的。 (3) 未公开收集、使用消费者金融信息的规则，未明示收集、使用消费者金融信息的目的、方式和范围的。 (4) 超出法律法规规定和双方约定的用途使用消费者金融信息的。	**1、** 由工商行政管理部门或其他部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处以违法所得一倍以上十倍以下的罚款；没有违法所得的，处以五十万元以下的罚款。 **2、** 情节严重的，责令停业整顿、吊销营业执照。

(5) 未建立以分级授权为核心的消费者金融信息使用管理制度，或者未严格落实信息使用授权审批程序的。 (6) 未采取技术措施和其他必要措施，导致消费者金融信息遗失、毁损、泄露或者被篡改，或者非法向他人提供的。	**3、** 其他有关法律、法规对处罚机关和处罚方式有规定的，依照规定执行。

需要特别注意的是，由于金融机构及其工作人员在业务过程中比较容易获取消费者的个人金融信息，如果存在非法获取、提出或者提供个人金融信息的行为，可能构成犯罪并受到从重处罚。根据最高法、最高检《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》第五条，非法获取、出售或者提供“通信内容、征信信息、财产信息五十条以上的”或者“通信记录、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的”，即达到刑事立案的追诉标准。此外，从事金融等行业的工作人员如果将履行职责或者提供服务过程中获得的个人敏感信息出售或者非法提供给他人的，将会受到“从重处罚”。

2、 开展合规自查

按照《金融信息保护规范》的要求，在外部专家的协助下，梳理涉及个人金融信息的业务模式、金融服务场景，对公司个人信息管理制度、个人信息保护规定、隐私政策、用户协议、委托处理及外部合作协议等文件进行全面的合规自查，及时发现问题并改正。

3、 建立并完善个人金融信息管理制度

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。

(1) 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。

(2) 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。

(3) 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。

(4) 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。

4、 完善金融App合规

首先，根据《移动金融客户端应用软件备案管理办法（试行）》，金融机构在客户端软件App上架之前，应当办理App备案。实务中，从2019年开始，中国互联网金融协会总共公布八批移动金融客户端应用软件实名备案名单，截至2021年4月1日共有912款App通过备案[4]。

其次，金融机构应按照与App收集处理个人信息有关的指引，核查并完善App《隐私政策》、《用户协议》有关个人金融信息的后台处理规则以及前端设置。比如，优化App界面，便于消费者更容易访问隐私政策；以字体加粗、标星号、颜色等方式显著标识敏感信息类型，明示告知消费者个人信息处理规则等。

再次，App应在最小必要范围内收集处理个人金融信息、并在收集处理前获得消费者的同意（关于收集处理个人信息的必要范围、以及获得同意的详细要求，可以参考我们在《君合法律评论》的App合规系列研究文章）。

结语

根据全国人大常委会消息， 2021年4月26日至29日将在北京举行十三届全国人大常委会第二十八次会议，对《个人信息保护法草案》进行第二次审议。根据此前公布的草案征求意见稿，对于侵害

[4] https://mp.weixin.qq.com/s/k4No-oFa6-95p4FigZGmSw

个人信息的行为，草案从罚款数额、对单位负责人员等的处罚等方面规定了更为严厉的罚则[5]，例如“情节严重的，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款”、“对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款”。如果《个人信息保护法》正式制定，将对金融业机构处理个人金融信息提出更高的要求，需要业界高度重视并进一步关注最新的规制动向。

杨锦文　合伙人　电话：86 10 8553 7608　邮箱地址：yangjw@junhe.com
高　健　律　师　电话：86 10 8519 1359　邮箱地址：gaojian@junhe.com
李圆圆　律　师　电话：86 10 8540 8665　邮箱地址：liyuanyuan@junhe.com

[5] 《个人信息保护法草案》第 62 条第六十二条　违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，由履行个人信息保护职责的部门责令改正，没收违法所得，给予警告；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。
有前款规定的违法行为，情节严重的，由履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。