君合研究简讯

JUNHE

2020 年 9 月 28 日

信息保护和网络安全法律热点问题

《金融消费者权益保护实施办法》强化消费者金融信息保护体系

2020 年 9 月 18 日，中国人民银行（以下简称“**央行**”）正式发布修订后的《中国人民银行金融消费者权益保护实施办法》（以下简称“**《2020 办法》**”）。

相较于央行 2016 年 12 月 14 日发布的《中国人民银行金融消费者权益保护实施办法》（银发〔2016〕314 号）（以下简称“**《2016 办法》**”），以及 2019 年 12 月 27 日发布的《2016 办法》修订版征求意见稿（以下简称“**《2019 草案》**”），《2020 办法》进行了若干修订与调整，进一步建立和完善金融消费者权益保护的基本制度。

此外，《2020 办法》在法律位阶上提升为部门规章并以人民银行令形式发布实施，这与作为部门规范文件的《2016 办法》相比将具有更高的效力层级。同时，在金融消费者信息保护方面，《2020 办法》结合并沿袭《民法典》、《网络安全法》等法律规定的内容，并基于当前银行业的消费者金融信息保护的现状和问题，进一步完善了消费者金融信息保护体系。就消费者金融信息保护方面的要点总结如下。

一、适用范围

根据《2020 办法》第 2 条规定，在中华人民共和国境内依法设立的为金融消费者提供金融产品或者服务的银行业金融机构（以下简称“**银行**”），以及在中华人民共和国境内依法设立的非银行支付机构（以下简称“**支付机构**”）适用本办法。

而《2016 办法》的适用主体除了银行业金融机构，还包括跨市场、跨行业提供交叉性金融产品和服务的其他金融机构以及非银行支付机构（以下合称“**金融机构**”）。从上述两个文件规定的适用主体范围来看，《2020 办法》与《2016 办法》相比进行了限缩，其排除了提供交叉性金融产品和服务的其他类别金融机构的适用，明确将适用主体限定于银行与支付机构。

具体到信息保护方面，《2020 办法》在第三章中围绕“消费者金融信息”的收集与处理规定了一系列的保护措施，其中，“消费者金融信息”是指“金融机构通过开展业务或者其他合法渠道获取、加工和存储的消费者信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或服务相关的信息”。而对应到《2016 办法》中，第三章规定的则为“个人金融信息”，具体指“金融机构通过开展业务或者其他渠道获取、加工和保存的个人信息”。对比上述两个术语的定义，除了《2020 办法》补充强调了消费者金融信息应系通过“合法”渠道获取与处理外，由于“个人金融信息”属于个人信息的范畴，而“消费者金融信息”的定义并未被限定仅包含消费者的个人信息，因此，从定义来看，“消费者金融信息”的涵盖范围更为宽泛。

二、消费者金融信息保护的重点要求

针对消费者金融信息的保护，《2020 办法》在第三章中做了详细规定，涵盖金融信息生命周期的大部分环节。在《2020 办法》与《2016 办法》比较的基础上，新修订的重点内容总结如下：

1、 消费者金融信息的处理

首先，《2020 办法》明确规定消费者金融信息的处理包括消费者金融信息的收集、存储、使用、加工、传输、提供、公开等。这与《民法典》第 1035 条中有关个人信息“处理”的定义和范围保持一致。

关于消费者金融信息的处理，《2020 办法》明确规定银行、支付机构应遵循“合法、正当、必要”的基本原则，这对《2016 办法》中的“收集个人金融信息时，应当遵循合法、合理、必要原则”做了细微调整，并且与《民法典》、《网络安全法》中规定的收集和使用个人信息的基本原则保持一致。该等变化也进一步表明“合法、正当、必要”已成为目前中国数据保护法律项下个人信息收集使用的基本原则。

2、 消费者金融信息的收集

《2016 办法》中并未明确规定个人金融信息收集的具体同意方式，《2020 办法》则规定，银行、支付机构处理消费者金融信息，应当经金融消费者或者其监护人明示同意。这项要求与金融行业推荐性标准《个人金融信息保护技术规范》（JR/T 0171—2020）[1]中所规定的“收集个人金融信息前应获得个人金融信息主体的明示同意”的要求具有一致性。从立法意义上看，这是首次在法规层面明确要求收集或处理消费者金融信息/个人金融信息前应当取得信息主体的“明示同意”。

此外，《2020 办法》还规定了收集消费者金融信息需向消费者履行的告知义务，包括要求银行与支付机构履行《消费者权益保护法》第 29 条中规定的明示义务；通过格式条款取得消费者金融信息收集、使用同意的，应当在格式条款中明确收集消费者金融信息的目的、方式、内容和使用范围等。

3、 消费者金融信息的跨境传输

《2016 办法》和《个人金融信息保护技术规范》均对个人金融信息的跨境传输有明确规定，具体包括：原则上在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行，但为处理跨境业务/业务需要并且在满足若干条件的前提下（包括但不限于取得个人金融信息主体的授权同意、通过签订协议等方式监督境外数据接收方）则可以向境外机构（含总公司、母公司或者分公司、子公司及其他为完成该业务所必需的关联机构）传输境内收集的相关个人金融信息。《2019 草案》同样规定了跨境传输消费者金融信息的类似要求和条件。

但是，《2020 办法》的正式生效版本却直接删除了有关消费者金融信息跨境传输的内容，完全未提及对数据出境的相关问题。考虑到金融监管部门一直以来对于消费者金融信息/个人金融信息的出境问题秉持较为严格的监管态度，加之近年来网信部门不断出台有关数据跨境传输的法规草案，关于消费者金融信息的跨境传输具体的监管制度设计仍有待进一步观察。

4、 消费者金融信息的使用

相比《2016 办法》，《2020 办法》补充规定银行、支付机构应当按照法律法规的规定和双方约定的用途使用消费者金融信息，不得超出范围使用。这项要求也与《民法典》、《网络安全法》中的相关规定保持一致，进一步强调银行、支付机构不得超出金融消费者的授权范围使用消费者金融信息，从而维护金融消费者的自主选择权。

5、 消费者金融信息内部管理制度

根据《2016 办法》，金融机构应建立个人金融信息数据库分级授权管理制度，并按照金融信息的重要性、敏感度及业务开展需要，合理确定本机构员工调取信息的范围、权限和程序。此外，金融机构应建立个人金融信息使用管理制度，涉及个人金融信息使用的，应采取严格的内部授权审批程序。

[1] 由中国人民银行于 2020 年 2 月 13 日发布，JR/T 0171—2020。

《2020 办法》则对前述制度做了相应的调整与整合，要求银行、支付机构建立“以分级授权为核心的消费者金融信息使用管理制度”，但具体内容与《2016 办法》基本一致。

此外，《2020 办法》还沿袭《2016 办法》的规定，要求银行、支付机构建立“消费者金融信息保护制度”。

上述规定进一步要求银行、支付机构应建立并完善机构内部的消费者金融信息保护的相关制度

6、 禁止强制授权

《2016 办法》明确要求金融机构不得将金融消费者授权或者同意其将个人金融信息用于营销、对外提供等作为与金融消费者建立业务关系的先决条件，但该业务关系的性质决定需要预先做出相关授权或者同意的除外。《2020 办法》则规定将消费者金融信息用于营销、用户体验改进或者市场调查的，应当以适当方式供金融消费者自主选择是否同意，不得作为提供金融产品或服务的先决条件。

从上述规定来看，相比于《2016 办法》，《2020 办法》持续体现了对金融消费者知情权与自主选择权的保护。但值得注意的是，《2020 办法》并未禁止银行、支付机构将金融消费者对其金融信息对外提供的授权作为向消费者提供金融产品与服务的先决条件，此处修订是否基于银行、支付机构将消费者金融信息对外提供往往是业务必须的实际情况，还是金融监管部门将在其他规范对此类信息的对外提供进行特别规制，目前尚不明晰。

7、 委托处理

《2016 办法》明确规定，金融机构保护消费者个人金融信息安全的义务不因其与外包服务供应商合作而转移、减免，并且金融机构应当充分审查、评估外包服务供应商保护个人金融信息的能力。但《2020 办法》却删除了此项要求，并未明确提到银行、支付机构在业务外包中需遵守的有关信息保护的义务及应承担的相关责任。我们注意到有关这方面的内容在《银行业金融机构外包风险管理指引》、《银行业金融机构信息科技外包风险监管指引》等规定中均有涉及，因此不排除《2020 办法》对委托处理内容的删除是考量了避免重复规定的原则。

8、 信息安全事件报告

根据《2016 办法》，在发生或者可能发生个人金融信息遗失、毁损、泄露或者篡改等情况时，应当立即采取补救措施，及时告知用户并向有关主管部门报告。但并未明确规定报告的主管部门及报告的时间。

《2020 办法》则明确规定：信息泄露、毁损、丢失可能危及金融消费者人身、财产安全的，应当立即向银行、支付机构住所地的中国人民银行分支机构报告并告知金融消费者；信息泄露、毁损、丢失可能对金融消费者产生其他不利影响的，应当及时告知金融消费者，并在 72 小时以内报告银行、支付机构住所地的中国人民银行分支机构。

从上述规定可以发现，《2020 办法》针对信息泄露事件的严重程度，分别详细规定了消费者信息事件报告的对象与时间，这不仅与《网络安全法》、《信息安全技术 个人信息保护规范》[2]中的要求保持一致，而且相较于《2016 办法》，也为银行和支付机构在发生消费者金融信息安全事件时履行报告义务提供了具有实操性的具体途径与方式。

9、 违反消费者金融信息保护相关义务的罚则

《2016 办法》并未对金融机构违反个人金融信息保护相关义务规定相应的罚则，而《2020 办法》则明确规定了相应的罚则及执法主体。根据《2020 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，央行或其分支机构在其职责范围内依据《中华人民共和国消费者权益保护法》第 56 条予以处罚。《2020 办法》对于相关罚则的明确在一定程度上解决了之前金融消费者信息保护违法成本较低的问题，也将进一步有效地督促银行和支付机构加强消费者金融信息的合

[2] 推荐性国家标准，GB/T 35273—2020。

规工作。

此外，值得注意的是，《中华人民共和国刑法》第 253 条规定，违反国家有关规定，向他人出售或者提供公民个人信息，可构成犯罪。而《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》中第 2 条规定，违反法律、行政法规、部门规章有关公民个人信息保护的规定的，应当认定为刑法第二百五十三条之一规定的“违反国家有关规定”。鉴于《2020 办法》目前已上升为部门规章，这意味着违反《2020 办法》中有关消费者金融信息的规定还可能会触发刑事犯罪的后果。

三、我们的观察

《2020 办法》的正式发布，体现了央行进一步规范银行、支付机构，切实保护金融消费者合法权益的工作重心。对于银行、支付机构而言，则应当严格落实《2020 办法》各项要求，承担起保护金融消费者合法权益的主体责任。

从信息保护的角度出发，《2020 办法》为银行和支付机构收集和处理消费者金融信息提供了详细和具体的要求和指引，也进一步强化了消费者金融信息的保护力度。相比于《2016 办法》与《2019 草案》，《2020 办法》结合了《民法典》、《网络安全法》等相关规定，对消费者金融信息保护体系进行了进一步的调整和完善，这也体现了金融监管部门一直以来对于金融消费者信息保护的重视。但《2020 办法》对消费者金融信息的跨境传输、业务外包等金融机构较为关注的问题并未做出明确规定，这在一定程度上也增加了相关合规工作的不确定性。未来，该《2020 办法》在执法实践中将如何具体适用，有待进一步观察。

随着国家对数据安全以及个人信息保护的监管不断深化，金融领域信息保护的立法工作和执法活动也正在逐步加强。中国人民银行自 2019 年以来发布了若干法规（草案）、通知和金融行业标准，从规范金融营销宣传行为、保护金融消费者权益、加强移动金融客户端应用软件安全管理等方面，加强和细化个人金融信息保护方面的监管要求。此外，除了涉及金融 App 违法违规收集使用个人信息的执法检查活动，针对银行机构违规查询、使用、泄露客户个人信息的处罚案例也频频引发社会公众的关注。

我们建议银行和支付机构严格按照《2020 办法》及相关金融行业标准的要求，严格做好消费者金融信息处理的合规工作。

董　潇　合伙人　电话：86 010 8519 1233　邮箱地址：dongx@junhe.com
郭　超　律　师　电话：86 010 8553 7733　邮箱地址：guoch@junhe.com
董俊杰　律　师　电话：86 010 8540 8722　邮箱地址：dongjj@junhe.com