君合研究简讯

JUNHE

2020 年 2 月 25 日

信息保护和网络安全法律热点问题

《个人金融信息保护技术规范》发布

2020 年 2 月 13 日，金融行业标准《个人金融信息保护技术规范》（JR/T 0171—2020）（以下简称“**《规范》**”）发布。《规范》围绕个人金融信息收集、传输、存储、使用、删除、销毁等生命周期各环节，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。《规范》的正式发布，为金融业机构收集和处理个人金融信息提供了参照标准，也进一步提升了个人金融信息的保护力度。

一、《规范》的适用对象

《规范》适用于提供金融产品和服务的金融业机构。根据《规范》的规定，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。从该定义可以看出，除了传统意义的持牌金融机构外，其他机构只要涉及到个人金融信息处理的，例如为持牌金融机构提供信息技术服务的外包服务机构或与其有业务合作的外部合作机构，均适用于本《规范》中的个人金融信息保护要求。

二、个人金融信息的内容和类别

《规范》旨在保护个人金融信息的安全，基于此，《规范》对“个人金融信息”的定义、具体内容以及类别均做出详细规定。

根据《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。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。在此基础上，《规范》对于前述各种类型的个人金融信息均进行详细列举。

《规范》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，将个人金融信息按照敏感程度分为 C3、C2、C1 三个类别，分别对应的危害程度为“严重危害”、“一定危害”、“一定影响”。其中：

1、 C3 类别信息主要指用户鉴别信息。例如银行卡磁道数据（或芯片等效信息）、账户登录密码、用于用户鉴别的个人生物识别信息等。

2、 C2 类别信息主要指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。例如支付账号及其等效信息、账户登录用户名、用户鉴别辅助信息等。

3、 C1 类别信息主要指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。例如账户开立时间、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。

此外，同一信息在不同的服务场景中可能处于不同的类别，需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、安全技术要求

《规范》所提出的个人金融信息安全技术要求包括生命周期技术要求和安全运行技术要求两个方面。个人金融信息因其类别的不同，相对应的安全技术要求和安全管理要求可能也存在差异。

生命周期技术要求包括个人金融信息在收集、传输、存储、使用、共享和转让、公开披露、委托处理、加工处理、汇聚融合、开发测试、删除、和销毁等各个环节的技术要求。《规范》针对前述各环节规定了非常详细的具体要求，其中值得关注的点包括：

1、 不得委托或授权无金融业相关资质的机构收集 C2、C3 类别信息；应采取技术措施，引导个人金融信息主体阅读隐私政策并获得其明示同意后收集其个人金融信息。

2、 应根据个人金融信息的不同类别采取不同的传输和安全措施，采用不同的信息展示技术。

3、 个人金融信息的共享和转让前应进行充分的安全评估。

4、 个人生物识别信息不得披露。

5、 受委托处理个人金融信息的第三方机构不应超出信息主体授权同意的范围处理个人金融信息，C3 及 C2 类别信息中的用户鉴别信息不得委托第三方机构进行处理。

6、 应建立个人金融信息销毁策略和管理制度。

此外，《规范》还从网络安全、Web 应用安全、客户端应用软件安全、密码技术与密码产品等四个方面提出了与个人金融信息相关的安全运行技术要求。

四、安全管理要求

《规范》中的个人金融信息安全管理主要包括安全准则、安全策略、访问控制、安全监测与风险评估、安全事件处置五个方面。

以“安全准测”为例，其详细规定了个人金融信息的收集、存储、使用等环节的安全管理要求，其中值得注意的点包括：

1、 个人金融信息的收集应符合最小化要求，并获得用户的明示同意；间接获取个人金融信息时，应确认金融信息来源的合法性，因业务需要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重新征得信息主体同意。

2、 个人金融信息原则上不得转让、共享或公开披露，确需转让、共享或公开披露的，应满足一定的安全要求；此外，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。

3、 委托处理个人金融信息的第三方机构应严格按照金融业机构的要求处理个人金融信息。

4、 个人金融信息确需出境的，应征得信息主体的同意，并进行相应的安全评估。

“安全策略”包括安全制度体系的建立与发布、组织架构岗位设置、人员管理等方面的要求；“访问控制”包括对个人金融信息访问的控制管理要求；“安全检测与风险评估”规定金融业机构对个人金融信息安全进行监控、审计、安全检查和评估的义务；“安全事件处置”则规定金融业机构应制定个人金融信息安全事件应急预案、及时向国家与行业主管部门报告等义务。

五、我们的观察

目前我国尚未有关于个人金融信息保护的专门立法，相关规定散见于《网络安全法》、《关于加强金融消费者权益保护工作的指导意见》、《中国人民银行金融消费者权益保护实施办法》、《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》等各项法律法规及规范性文件中。《个人金融信息保护技术规范》作为全国金融标准化技术委员会第一部专门针对个人金融信息的行业标准，将为金融业机构处理个人金融信息、监管部门的执法行动提供更加体系化与专业化的参考标准。

我们也注意到，中国人民银行正在起草制定《个人金融信息（数据）保护试行办法》（以下简称“**《试行办法》**”）。根据此前新闻报道对于《试行办法》部分内容的披露[1]，我们发现《试行办法》与《规范》在内容方面具有一定程度上的一致性，例

[1]参见《南方都市报》文章《大数据行业巨震：监管将一刀切禁止个人金融信息收集？》，作者熊润淼。

如均对未取得金融相关资质的机构收集个人金融信息进行限制，而从监管意义上看这两个文件均释放出金融监管部门计划加强个人金融信息监管的信号。关于《规范》与《试行办法》之间的联系和区别，以及各自在未来监管实践中所发挥的作用，还需待《试行办法》正式发布后再做进一步的观察。

总体而言，《规范》的发布实施有助于规范金融业机构个人金融信息保护工作，对现有的个人金融信息的保护规定提供了相应细节和具体的补充，对防范各类金融交易风险、保护金融消费者合法权益具有重要意义。从监管的角度看，《规范》的发布进一步体现出金融监管机构加强个人金融信息保护力度的监管态度。而从具体内容上看，《规范》对个人金融信息进行分类，并针对不同类别的信息分别提出安全保护要求，也体现了《规范》的科学性和合理性。对于《规范》在执法实践中将如何具体适用，有待进一步观察。

董　潇　合伙人　电话：86 010 8519 1718　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