HANKUN
汉坤律师事务所
Han Kun Law Offices

汉坤专递

2020 年第 3 期（总第 155 期）

新法评述

1、《个人金融信息保护技术规范》重点解析

2、2020 版《个人信息安全规范》重点解析

新法评述

1、《个人金融信息保护技术规范》重点解析

作者：段志超丨杨铁成丨蔡克蒙丨李芳菲丨乔梦晶丨胡敏喆

2020 年 2 月 13 日，中国人民银行（“**央行**”）和全国金融标准化技术委员会发布了《个人金融信息保护技术规范（JR/T 0171-2020）》（“**《规范》**”）。《规范》在《网络安全法》和央行此前多部个人金融信息保护监管规定的基础上，从安全技术和安全管理角度对个人金融信息处理的全生命周期提出了系统具体要求。与现行法律法规相比，《规范》的可操作性更高，因此可以对金融机构和金融行业相关企业的合规实践起到重要的指导作用。本文将从企业合规角度解读《规范》要点，并重点关注《规范》在现行法规及标准基础上提出的新要求。

一、扩大的适用：从银行业金融机构到金融业机构

《规范》将其直接适用范围划定为“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”（“**金融业机构**”），这就意味着包括银行业金融机构、各类证券、基金、保险机构在内的广义的持牌金融机构，以及处理个人金融信息的相关机构（可能持牌或非持牌），例如第三方支付公司、金融科技公司等，都将直接适用《规范》。此外，由于行业间关联性以及对于金融业机构范围解释的空间，《规范》亦有可能对涉及个人金融数据的电商等行业产生间接影响。

另外，对于私募基金管理人（包括 PFM、QDLP、QDIE 等机构）来讲，尽管此类机构不属于严格意义上的持牌金融机构，但这些机构都需要在中国证券投资基金业协会登记备案，并接受其监管。如果私募基金管理人通过向客户提供金融产品、服务等渠道获取、保存或处理了任何客户的个人信息[1]，则该管理人应参照适用《规范》中的安全技术与管理要求。

相较而言，早先央行和中国银行保险监督管理委员会（“**银保监会**”）针对个人金融信息保护陆续出台的系列监管规定，主要包括《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》（2011 年 5 月 1 日生效）（“**《央行通知》**”）、《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》（2012 年 3 月 27 日生效）、《中国人民银行金融消费者权益保护实施办法》（2016 年 12 月 14 日生效）（“**《央行办法》**”）、《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》（2018 年 5 月 21 日生效）。多仅直接适用于银行业金融机构，只是在实践中参照适用于商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司以及征信机构等非银行业金融机构。

需要指出的是，本次发布的《规范》是金融行业推荐性标准，而非强制性标准。尽管《规范》作为推荐性标准不具有强制约束力，但我们不排除金融监管机构在开展监督检查或执法活动时将其作为重要参考，将《规范》视为金融业机构在个人金融信息保护方面的实践建议与操作指南。因此，我们建议金融业机构应遵

[1] 示例：客户的账户信息、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。

照《规范》中的相关标准与要求，以便在最大程度上规避与个人金融信息保护相关的任何法律或合规风险。

二、分级和场景化：个人金融信息的区别化监管要求

《规范》采取了“分类分级”和“场景化”的监管思路，根据信息泄露或被篡改后对个人信息主体的信息安全与财产安全的危害程度，将个人金融信息的敏感程度由高到低分为 C3、C2、C1 三个类别：

- C3 类主要为用户鉴别信息，其泄露后可能造成直接财产损害，包括但不限于：账户密码、银行磁道数据、芯片信息、卡片验证码、卡片有效期、用于用户鉴别的个人生物识别信息（如人脸识别、指纹识别）；
- C2 类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，其泄露后可能造成间接财产损害、造成歧视性待遇或危害信息安全，包括但不限于：账户信息、身份证件信息、用户鉴别辅助信息（如短信验证码）、个人财产信息、交易信息、KYC 信息、家庭住址；以及
- C1 类主要为金融业机构内部使用的个人金融信息，包括但不限于：开户时间、开户机构、支付标记信息等。

个人金融信息主体提供的家庭成员信息应当依据上述敏感程度进行归类。多种低级别的信息的经过组合、关联或者分析也有可能构成高敏感程度的信息。《规范》还首次提出了根据服务场景确定信息敏感程度和级别的要求。企业应根据具体服务场景以及有关信息在场景中的作用，对信息进行识别归类，采取有针对性的保护措施。

需要注意的是，C3 和 C2 类信息在《个人信息安全规范》中基本被归为个人敏感信息的范畴，而《规范》结合金融服务场景，对 C3 和 C2 类信息提出一些比《个人信息安全规范》项下个人敏感信息更高的保护要求。

- 禁止委托或授权无金融业相关资质的机构收集 C3 类、C2 类信息，收集 C3 类信息应当采取加密等技术措施，防止被未授权第三方获取；
- 传输 C3 类信息中的支付敏感信息应当采取符合行业技术标准及行业主管部门规定的控制措施；
- 原则上不应留存非本机构的 C3 类信息，如需留存，应当获得信息主体和账户管理机构的授权；
- 原则上禁止委托第三方机构处理 C3 类个人金融信息以及 C2 类个人金融信息中的用户鉴别辅助信息（如短信验证码）；
- 不应共享、转让和披露 C3 类信息和 C2 类信息中的用户鉴别辅助信息；以及
- 通过合同或协议约束外包服务机构与外部合作机构不应留存 C3 和 C2 类信息。

三、合法与必要：严格与灵活性兼具的个人金融信息收集规则

依法收集数据是后续依法处理数据的前提，因此《规范》从收集手段、数据来源、收集范围等维度对收集环节重点着墨。

对于直接收集的个人信息，金融业机构应避免通过默认授权、功能捆绑的方式强迫或误导个人金融信息主体提供信息。为避免隐秘收集个人金融信息，《规范》要求金融业机构在产品或服务上线发布前进行技术

检测，确保个人金融信息的收集、使用、共享等依法依规进行，通过隐私政策等予以披露。

对于间接收集的个人金融信息，金融业机构应要求信息提供方说明个人金融信息来源，并通过技术手段保证信息来源的可追溯性。金融业机构有义务确认信息来源的合法性，了解信息提供方已获得的授权内容。这些金融业机构需承担更高的审查义务，难以仅依赖与信息提供方的书面合同或保证免除自身责任。

就数据收集范围而言，《规范》对数据收集的“最小化要求”做出了阐释，允许金融业机构收集与实现和优化金融产品或服务、防范金融产品或服务的风险有直接关联的个人金融信息[2]。与此前相关监管规定中常用表述“不得收集与业务无关的信息”相比，《规范》的前述规定更为灵活，为以优化金融产品或服务为目的收集个人金融信息保留了一定灵活度，并照顾了金融业风控的特殊需求。

此外，《规范》还规定收集维护金融产品或服务的安全稳定运行所必需的个人金融信息（例如用于识别、处置金融产品或服务中的欺诈或被盗用的情形），或与用于履行国家法律法规及行业主管部门有关规定的义务相关的个人信息，可作为例外无需获得信息主体同意。这一规定为金融业机构收集为开展风控或履行反洗钱、反恐怖融资等而收集个人金融信息留下了更多空间。

四、脱敏、删除与销毁：更加明晰的个人金融信息应用和存储规则

实践中，许多金融业机构常常面临在产品开发中利用个人金融进行合规性的难题。考虑到个人金融信息的敏感性，《规范》要求金融业机构有效隔离开发测试环境和生产环境，在实际开发测试中应当对个人金融信息进行虚构或者去标识化，原则上不应使用个人真实的金融信息。值得关注的是，《规范》特别在附录中对信息屏蔽技术进行了规定和举例，金融业机构可将屏蔽后的信息运用于产品开发和测试活动。

此外，《规范》还规定个人金融信息的存储时限应当满足法律法规和行业主管部门的规定，符合为授权使用的目的所必需的最短时间要求。超出前述时限，或在个人金融信息主体依法要求删除的情况下，金融业机构应删除个人金融信息或对其进行匿名化处理。删除是指“使个人金融信息不可被检索、访问的过程”。实践中，值得探讨的是如果服务关系已经结束，授权所需目的已届满，但企业仍依法负有信息留存义务的情况下[3]，应如何处理个人信息。对此，我们认为金融业机构仍可继续留存个人信息，但不应对个人金融信息进行任何开发利用。

除删除外，《规范》还对信息销毁做出了规定，销毁是指“个人金融信息进行清除，使其不可恢复的过程”。因此，销毁较删除更为严格，主要适用于委托处理场景，即在委托第三方机构处理个人金融信息时，如果委托关系解除，受委托者有义务按照金融业机构的要求销毁个人金融信息并继续承担相应的保密责任。委托方金融业机构还应监督销毁存储介质的过程，要求保存销毁记录等。

五、《规范》对金融业机构外包活动的影响

1. 《规范》与金融业机构信息科技外包

出于提供金融产品或金融服务的业务需要，金融业机构可能会将原本由自身负责处理的信息科技活动委托或授权给服务提供商等第三方机构代为处理（“**信息科技外包**”）。在实践中，金融业机构的信

[2] 直接关联是指无该个人金融信息参与无法实现前述目的。

[3] 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》明确要求金融机构对客户身份资料和交易记录等至少保存五年。

息科技外包通常涵盖以下类型：

- 研发咨询类外包：科技管理及科技治理等咨询设计外包，规划、需求、系统开发、测试外包；
- 系统运行维护类外包：包括数据中心（灾备中心）、机房配套设施、网络、系统的运维外包，自助设备、POS 机等远程终端及办公设备的运维外包；以及
- 业务外包中的信息科技活动：市场拓展、业务操作、企业管理、资产处置等外包中的系统开发、运行维护和数据处理活动。

在以上三类金融业机构的信息科技外包场景中，第一类“研发咨询类外包”主要集中于企业科技管理架构设计和系统搭建；第二类“系统运行维护类外包”主要针对信息科技系统与设施的整体运维。上述两类外包活动一般不会深入企业实际业务，金融业机构通常不会委托外包服务机构具体参与到个人金融数据的处理。

与前两类相比，第三类“业务外包中的信息科技活动”与金融业机构实际业务活动之间的联系更为紧密。在此类信息科技外包活动中，金融业机构应特别注意外包服务范围是否涉及到委托第三方机构参与到任何个人金融数据的收集、传输、存储、使用、删除、销毁等环节的工作。

如涉及个人金融信息的委托处理，金融业机构应确保自身及外包服务机构除了遵守现行个人信息保护监管规定和国家标准中的安全管理与安全技术要求之外，还应当符合《规范》中针对个人金融信息委托处理的新增要求。

2. 《规范》中针对个人金融信息委托处理的具体要求

在《规范》出台前，《信息安全技术 个人信息安全规范》等国家标准针对个人信息的委托处理已设定了具体的安全管理与安全技术要求。针对金融产品及金融服务的行业特点，《规范》在适用法律法规与国家标准的基础上，对金融业机构委托处理个人金融信息的行为提出了更为细化的安全管理与技术要求，具体请参见下表：

类别	《规范》中针对个人金融信息委托处理的具体要求
委托行为的范围	委托行为不应超出个人金融信息主体授权同意的范围（无需征得授权同意的特殊情形除外）。
委托信息的范围	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。
委托信息的脱敏处理	对委托处理的信息应采用去标识化（不应仅使用加密技术）等方式进行脱敏处理，降低个人金融信息被泄露、误用、滥用的风险。
委托行为的个人金融信息安全影响评估	金融业机构应对委托行为进行个人金融信息安全影响评估（至少每年开展一次），并确保受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。
对受委托者的监督	金融业机构应对第三方机构等受委托机构进行监督，方式包括但不限于： ■ 通过合同等方式规定受委托者的责任和义务；以及 ■ 对受委托者进行安全检查和评估（至少每年开展一次）。
外部嵌入的自动化工	金融业机构应对外部嵌入或介入的自动化工具（如代码、脚本、接口、算法模

类别	《规范》中针对个人金融信息委托处理的具体要求
具的技术检测与审计	型、软件开发工具包等）开展技术检测，确保其个人金融信息收集、使用行为符合约定要求；并对其收集个人金融信息的行为进行审计，发现超出约定行为及时切断接入。
委托处理的记录	金融业机构应准确记录和保存委托处理个人金融信息的情况。

3. 《规范》对大数据、金融科技公司的影响

对委托处理个人金融信息的严格规范可以被视为央行、银保监会近期严格规范金融业机构与大数据公司、金融科技公司的政策延伸。目前实践中常见的金融业机构委托大数据公司、金融科技公司获取的借款人行为、电商购物、生活特征等进行验证，用于助贷、反欺诈、信审、催收的做法可能面临限制。大数据公司、金融科技公司向金融业机构提供上述服务前可能将面临金融业机构安全保障能力审查，以及监管部门统一设定的资质或准入门槛限制，可提供服务数据服务范围亦将缩窄。

六、《规范》对个人金融信息跨境传输的影响

（一）个人金融信息出境监管制度回顾

数据本地化以及数据出境相关的监管一直是金融业机构、尤其是跨国金融业机构在中国本土运营的合规重点之一。在本部分，我们将简要梳理并回顾与个人金融信息出境相关的核心监管要求。

1. 《中华人民共和国网络安全法》（“《网安法》”）
2016 年 11 月 7 日，全国人大常委会通过《网安法》，首次针对关键信息基础设施的运营者提出了数据本地化与数据出境安全评估的要求： ■ 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储；以及 ■ 因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。 另外，《网安法》明确，网络运营者未经被收集者同意，不得向他人提供个人信息，这意味着网络运营者向境外传输个人信息需要获得个人信息主体的同意。
2. 国家互联网信息办公室（“网信办”）
针对个人信息出境，网信办先后于 2017 年 4 月 11 日和 2019 年 6 月 13 日发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》和《个人信息出境安全评估办法（征求意见稿）》，旨在对个人信息出境安全评估的适用范围、评估内容、评估程序等做出规定。
3. 全国信息安全标准化技术委员会（“信安标委”）
信安标委在其 2017 年 11 月 30 日发布的《信息安全技术 个人信息安全规范》及其后续的征求意见稿中曾提出有关个人信息跨境传输的整体要求； ■ 在中华人民共和国境内运营中收集和产生的个人信息向境外提供的，个人信息控制者应遵循国家相关规定和相关标准的要求。 另外，信安标委还曾于 2017 年 5 月和 2017 年 8 月两度发布《信息安全技术 数据出境安全评估指南（征求意见稿）》，旨在对个人信息出境安全评估要点和流程等内容予以进一步细化。

4. 中国人民银行（“央行”）
在金融领域，央行对于金融业机构的个人金融信息保护采取了较为审慎的态度。央行于 2011 年 1 月 21 日发布《央行通知》。根据《央行通知》，银行业金融机构应遵守以下要求： ■ 在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行；以及 ■ 除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。 在《央行通知》发布五年后，央行于 2016 年 12 月 14 日印发《央行办法》，《央行办法》对在境内依法设立的为金融消费者提供金融产品和服务的银行业金融机构、提供跨市场、跨行业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提出更为严格的数据出境要求： ■ 境内金融机构为处理跨境业务且经当事人授权，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的，应当符合法律、行政法规和相关监管部门的规定；以及 ■ 境内金融机构通过签订协议、现场核查等有效措施，要求境外机构为所获得的个人金融信息保密。

（二）《规范》中针对个人金融信息跨境传输的具体要求

在相关适用法律法规与国家标准的基础上（如上述第（一）部分总结），《规范》对金融业机构个人金融信息本地化与跨境传输提出了更为细化的管理要求。具体要求请见下表：

类别	《规范》中针对个人金融信息跨境传输的规定
原则性要求	《规范》规定，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。
个人金融信息出境需满足的要求	《规范》提出，金融业机构可向境外机构（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，但需要同时满足以下要求： ■ 出于业务需要，确需向境外机构提供； ■ 应获得个人金融信息主体明示同意； ■ 应开展个人金融信息出境安全评估，并确保境外机构数据安全保护能力达到相关的安全要求； ■ 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；以及 ■ 应符合国家法律法规及行业主管部门的有关规定、办法与标准。

（三）个人金融信息跨境传输与反洗钱合规

值得注意的是，《规范》允许金融业机构向境外机构提供个人金融信息，但提供信息的行为必须同时符合国家法律法规及行业主管部门的有关规定、办法与标准。这意味着金融业机构在向境外机构提供个人金融信息时，也应同时关注我国金融业主管部门针对反洗钱与反恐怖主义融资的监管规定与要求。

在中国反洗钱监管制度下，除了全国人大常委会于 2006 年 10 月 31 日正式通过的《中华人民共和国反洗钱法》外，央行、银保监会等金融监管机构也陆续出台了一系列关于反洗钱与反恐怖主义融资的监管规定与要求，其中有两点值得注意：

(1) 根据央行等金融监管部门联合发布的《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》：

- 自然人客户的“身份基本信息”包括客户的姓名、性别、国籍、职业、住所地或者工作单位地址、联系方式，身份证件或者身份证明文件的种类、号码和有效期限；以及
- 客户的“交易记录”包括关于每笔交易的数据信息、业务凭证、账簿以及有关规定要求的反映交易真实情况的合同、业务凭证、单据、业务函件和其他资料。

(2) 针对客户身份资料和交易信息的保密与对外提供，我国金融监管部门也提出了严格的限制。根据《银行业金融机构反洗钱和反恐怖融资管理办法》、《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》、《支付机构反洗钱和反恐怖融资管理办法》等反洗钱监管规定，对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，相关金融机构及其工作人员应当予以保密；非依法律规定，不得向任何单位和个人提供。

我们注意到，在中国现行反洗钱监管制度下金融机构在开展业务活动中所获取的“客户身份资料和交易信息”与《规范》所定义的“个人金融信息”在很大程度上是重合的。这也为金融业机构在个人数据保护制度与反洗钱监管制度下的数据合规工作带来一定的挑战。

鉴于此，我们提示金融业机构在遵守个人金融信息保护与跨境传输相关法律法规与国家标准的同时，也应注意遵守央行、银保监会、证监会等金融监管部门在反洗钱领域出台的法规与监管要求，确保充分履行金融业机构的反洗钱合规义务。与此同时，随着我国个人信息保护与反洗钱监管制度的不断完善，我们也将进一步关注相关制度的修订情况，并及时与各位读者分享我们的观点。

2、2020 版《个人信息安全规范》重点解析

作者：段志超丨蔡克蒙丨胡敏喆[4]

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《信息安全技术 个人信息安全规范（GB/T 35273-2020）》（“**新版规范**”）。新版规范将于今年 10 月 1 日起正式生效，替代现行有效的《信息安全技术 个人信息安全规范（GB/T 35273-2017）》（“**旧版规范**”）。新版规范整体上延续了此前 2019 年 6 月和 10 月发布的两版《个人信息安全规范》征求意见稿的修改思路，系统地反映了监管部门近期对个人信息保护治理工作中提出的监管要求，针对个人信息收集不透明、强制和捆绑收集个人信息现象严重、个性化推送侵犯用户自主选择权、第三方隐秘收集信息缺乏控制、账号注销难、对生物识别信息的滥用和泄露频发等实践中个人信息保护疑难问题做出了有力回应。同时，我们也注意到新版规范相较旧版规范及此前征求意见稿在不少细节处进行了优化，更有助于合理开展个人信息保护工作。

本文尝试以问题为导向梳理和探讨新版规范的一些亮点，为企业合规提供概括性指南。

一、能读懂的通知 — 优化隐私设计提升透明度

自旧版规范实施以来，随着监管机构对隐私政策审查不断加强，很多企业的隐私政策已日趋规范，对个人信息处理情况做出了更加详实的披露，并为监管机构监督企业落实隐私的保护情况提供了有力的凭据。然而，隐私政策仍经常被批评篇幅冗长、晦涩难懂。新版规范优化了隐私政策的内容要求，并更加强调在隐私政策之外通过弹窗等交互界面实时告知用户，更有助于帮助用户理解个人信息处理情况，在知情基础上做出选择。

- 就形式而言，新版规范将“隐私政策”修改为“个人信息保护政策”[5]，意在明晰“隐私”和“个人信息”保护之间的区别，与《民法典（草案）》中对隐私和个人信息分别予以保护的思路保持一致。

- 从隐私政策内容要求上看，新版规范与此前征求意见稿相同，删除了对披露个人信息控制者注册地址、常用办公地点、负责人联系方式（替换为控制者联系方式）、个人信息收集频率、存储地点、使用 Cookie、网站信标、像素标签等同类技术情况等过于法律或技术的事项。这将有助于缩减隐私政策篇幅，提升隐私政策可读性。新版规范正式将此前征求意见稿提出的，且监管机构已通过《App 违法违规收集使用个人信息行为认定方法》等规范和执法实践提出的增强告知或实时告知要求纳入规范，包括个人敏感信息明确标识或突出显示，首次打开产品或服务、注册账号时通过弹窗展示隐私政策主要条款或核心内容，开启收集个人信息的扩展业务功能前通过弹窗等交互界面或设计告知功能所需个人信息等。这些增强告知的要求对企业产品的隐私设计提出了新的挑战。

二、分得开的同意 — 通过业务功能区分解决“最小必要”难题，强化用户控制力

如何落实数据收集的“必要性”和“最小化”原则是各国数据监管机构面临的共同挑战。这些原则在欧盟 GDPR 语境下被细化为三要素，即“充分性（adequate）”——个人信息足以实现处理目的，“相关性

[4] 实习生周莎莎对本文的写作亦有贡献。

[5] 出于习惯考虑，本文仍沿用“隐私政策”这一惯用概念。

（relevance）”——个人信息与目的具有合理关联，“限于必要（limited to what is necessary）”——仅应收集完成目的所需的最少信息[6]。

然而，这些原则和设计要求仍过于抽象，在我国隐私保护理念方兴的环境中难以对业务实践提供具体指导。对此，新版规范承继了此前征求意见稿在区分业务功能的基础上界定信息收集范围的思路，禁止企业将基本功能与扩展功能捆绑，防止企业通过“功能捆绑”强迫个人信息主体接受个人信息收集。具体而言：

- 应当逐一告知用户扩展业务功能，逐项获得用户明示同意后开启；
- 用户拒绝开启扩展业务功能收集个人信息，企业不得拒绝提供基本业务功能或者降低服务质量，并且不得在 48 小时内再次征得用户同意；
- 用户有权关闭或退出业务功能，相应的途径或方式应与选择使用该项业务功能的途径或方式一样方便。

新版规范以业务功能为基础确定个人信息收集范围的要求，未来辅以关于相关常用服务类型最小信息的相关标准，对企业落实“最小必要”原则提供了具体的操作指引。企业在收集扩展功能对应的个人信息时，需要在其启动时逐项明示以获取用户的同意，实践中该操作可能会在用户体验和业务设计上给企业提出更多的挑战。此外，新版规范保留了此前征求意见稿“不应将改善服务质量、提升个人信息主体体验、研发新产品单独作为基本业务功能”的要求。这是否意味着企业需要开发允许用户自主选择的“用户体验计划”，方可收集改善服务、产品研发所需的个人信息，以及企业是否可以将基本业务功能收集的个人信息用于前述目的，是否需就此再次征得用户明示同意，仍有待通过监管要求和行业实践加以逐步明确。

三、特殊数据的特殊规则 — 新增生物识别信息处理严格限制

近年来，对生物识别信息，特别是人脸识别信息的过度收集、泄露和滥用引发的诸多伦理、隐私和安全问题在国内外均引起了广泛关注。欧盟委员会甚至曾提出了五年内禁用人脸识别技术的禁令[7]，尽管该禁令在发布不久后即被删除，但也足以反映其对人脸识别的高度关注和谨慎态度。而一直以隐私监管宽松而著称的美国，已有数州提出或通过关于人脸识别的立法，且有著名科技公司因为未经授权将面部识别数据用于用户标签建议被诉，最终承担数亿美金的赔偿金。我国近期发布的《个人金融信息保护技术规范》《人脸识别线下支付行业自律公约（试行）》均对人脸识别信息等生物识别信息的处理提出了严格规范。在此背景下，新版规范对个人生物识别信息的处理在生命周期各阶段提出了具体要求。

- **收集**：在收集个人生物识别信息前，应当单独向个人信息主体告知收集和使用生物识别信息的目的、方式和范围、存储时间等规则，取得个人信息主体明示同意。
- **传输**：应当采用加密等安全措施，如需采用密码技术宜遵循密码管理相关国家标准。
- **存储**：应当采用加密等安全措施，将个人生物识别信息与个人身份信息分开存储，原则上不应存储原始个人生物识别信息。

[6] 此外，欧盟数据保护机构还提出了数据避免（data avoidance，如果数据处理可能实现其他目的应避免进行个人数据处理活动）；聚合（aggregation，应当尽可能使用聚合性数据，避免对特定主体进行识别）；pseudonymization（如无需直接识别数据主体的个人数据，应对个人数据进行假名化处理，并单独存储识别密钥）；匿名化与删除（anonymization and deletion，如果个人数据对于目的的实现不再必要，应当对个人数据进行技术处理或从系统中去除有关个人数据，使得个人信息主体不再被识别或者关联）等原则。

[7] https://www.telegraph.co.uk/news/2020/01/17/european-commission-mulls-ban-facial-recognition-technology/.

- **共享和转让**：原则上不应共享或转让个人生物识别信息，确需共享和转让的，仍应当单独向用户告知目的、信息类型等内容，并征得个人信息主体的明示同意。
- **披露**：不应公开披露个人生物识别信息。

前述合规要求对处理生物识别信息的技术公司构成了很大的合规挑战，这些公司往往不直接与客户交互，而仅向更“前端”的向用户提供服务的客户提供识别、验证服务，因此难以直接取得客户同意。提供生物识别信息识别和认证的企业需要与其客户共同制定或开发出符合新版规范要求的单独的信息采集或共享声明和同意方案。而对于在公共场所使用人脸识别系统用于人员分流、安全防护、甚至客流分析和个性化推荐等更难以取得明示同意的场景，如何落实新版规范的单独告知和同意要求则是相关企业亟需破解的合规难题。就现阶段而言，企业至少应按照规范要求，采取仅存储生物识别信息摘要信息，及时删除可提取个人生物识别信息的原始图像等措施，并在可能情况下尽可能实现在采集终端直接实现身份识别和认证功能。

四、打开的黑盒子 — 强化产品和服务提供者责任，约束第三方处理活动

第三方个人信息处理活动已经构成互联网产品生态的不可分割的环节。相比于个人信息控制者直接在提供产品或服务的过程中处理个人信息，第三方收集活动则较为隐蔽，用户无法追踪和感知信息的最终流向和使用目的。第三方采集的信息被用于与产品服务较为直接相关的场景，例如通过嵌入的 SDK 提供支付服务或地图服务，或用于对产品服务使用情况进行统计分析，进而基于用户行为向用户进行定向信息投放，甚至还可能被用于完全超出客户隐私预期的场景，例如用于信用评估。这些第三方应用的数据处理活动可能侵犯用户的知情权和自主选择权，并存在第三方借助网络产品或服务执行恶意操作，以及第三方数据泄露风险。鉴于此，我国监管机构此前征求意见稿中特别增加了关于“接入具备收集个人信息功能的第三方产品或服务”的规定，而去年出台的《App 违法违规收集使用个人信息行为认定方法》亦强化了直接向用户提供服务的互联网产品和服务个人信息控制者的责任，要求应当逐一列出委托的第三方或嵌入的第三方代码、插件等收集使用个人信息的目的、方式、范围。

新版规范延续了此前规定，从事前接入审查、告知同意、持续审计监管等维度全面加强产品和服务对接入或嵌入的第三方个人信息处理的监督审查责任。具体而言：

- **第三方接入前**：应当建立安全评估等机制，宜对第三方工具开展相关的技术检测；应当与第三方通过合同等形式明确双方安全责任，妥善留存合同与管理记录；
- **用户控制**：要求第三方自用户处获得收集个人信息的授权同意，并在必要情形中核验其实现的方式[8]。
- **第三方接入后**：向用户明确标识产品或服务由第三方提供，要求接入第三方建立个人权利响应机制并加强个人信息的安全管理。
- **发现未落实安全管理要求和责任时**：应当督促接入第三方及时整改，必要时及时停止接入。

此外，考虑到个人信息控制者权利和义务的平衡，相较此前的征求意见稿，新版规范删除了要求个人信息控制者“妥善留存、及时更新第三方权利响应机制”的要求，提出控制者仅在“必要情形下”对第三方获得用户授权同意的方式进行核验，一定程度上减轻了个人信息控制者的义务。

[8] 我们理解这一要求主要针对网页跳转、联合登陆等接入第三方服务场景，而对于第三方通过嵌入 SDK 等收集个人信息的，原则上应按照第 9.6 条由直接向用户提供网络产品或服务的个人信息控制者对用户进行告知并获得用户同意。

为了应对趋严的执法态势，企业需要对自身产品或服务中的第三方产品或服务进行详细摸排，及时删除或停止接入不必要或存在隐秘收集或滥用个人信息以及存在信息安全隐患的第三方产品或服务；若必须接入第三方产品或服务，应当向用户明确标识该产品或服务由第三方提供并详细披露第三方个人信息处理活动的具体情况。

五、多样选择 — 强化用户对个性化展示的控制力

个性化展示目前广泛应用于互联网广告、资讯推荐等领域。个性化推送在为用户节约搜索成本，更快地实现供需的匹配的同时，也引发对侵犯用户选择权，形成“信息茧房”，甚至是对数据主体造成歧视的担忧。

此次新版规范发布以前，多部法律法规已在这一方面做出了规范。例如 2019 年 1 月 1 日起实施的《电子商务法》要求电子商务经营者在根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项。2019 年 5 月发布的《数据安全管理办法（征求意见稿）》则规定，网络运营者利用用户数据和算法开展定向推送活动时，应当以明显方式标明“定推”字样，建立用户选择退出的机制并删除已经收集的设备识别码等用户数据和个人信息。

对此，新版规范继受了此前征求意见稿的规定，提升个性化展示的透明度和数据主体的控制力。

- 在向个人信息主体提供业务功能的过程中使用个性化展示，应显著区分个性化展示的内容和非个性化展示的内容；区分方式包括标明“个性化展示”或“定推”等字样，或区分栏目或版块进行展示；
- 在向个人信息主体提供电子商务服务的过程中，根据消费者的**兴趣爱好、消费习惯等特征**向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项；
- 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应为个人信息主体提供简单直观的退出或关闭的选项并在用户选择退出后，向个人信息主体提供删除或匿名化有关信息的选项；
- 个人信息控制者还应当建立个人信息的自主控制机制，保障个人信息主体调控个性化展示相关程度的能力。

值得注意的是，新版规范认为，个人信息控制者基于用户选择的地理位置展示搜索结果的行为不属于个性化展示。究其原因，可能在于基于用户选择的地理位置进行展示是建立在用户选择基础上（例如在 OTA 服务中基于用户位置选择展示周边酒店），相对透明直观，用户对此具有控制力。基于同样理由，我们认为如基于用户设置的年龄、性别等其他基本特征向其展示内容或对搜索结果进行排序，不因个人信息主体身份而进行“千人千面”展示的，同样不应被视为个性化展示。

为了顺应上述监管要求，企业应积极在产品开发过程中重视对个性化展示的隐私设计，设置个性化展示的显著标识，设置关闭按钮或专门的隐私仪表板，允许用户对个性化展示进行控制。

六、迷宫不再 — 账户注销更加方便

强化个人信息主体权利保护，特别是注销账号权利的保护是监管机构近期的执法重点之一。去年 11 月，工信部开展信息通信领域 App 侵害用户权益专项整治行动，将“为用户账号注销设置障碍”列为一项重要的检查要点。根据工信部随后发布的两批侵害用户权益 App 名单和 App 专项治理工作组发布的《61 款 App 存在收集使用个人信息问题的通告》，先后有 60 余款 App 存在账号注销难的问题，包括规定了最短使用期限、需要用户提交身份证照片、手持身份证照片等条件。2019 年 12 月 30 日，国家网信办、工信部、公安

部、市场监管总局还联合印发《App 违法违规收集使用个人信息行为认定方法》，再次重申，为注销用户账号设置不必要或不合理条件、未在 15 个工作日内响应用户权利的行为属于违法违规收集使用个人信息的行为。

在此背景下，新版规范首次将个人信息主体权利单独列为一章，并在此前征求意见稿基础上进一步细化了对个人信息主体注销账户权利的保护。

- 注销过程需要进行身份核验的，不应当提供多于注册、使用等服务环节收集的个人信息类型。如需注销核验过程需要收集个人敏感信息，应明确相关的处理措施，在达成目的后立即删除或做匿名化处理。
- 若多个产品或服务之间存在必要业务关联关系，而注销某个产品或服务的账户，会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，应向个人信息主体进行详细说明。
- 对于实践中“棘手”的多个产品或服务共用同一账号体系情况下的账号注销问题，新版规范规定企业可以将该产品或服务账号以外的信息做删除处理，及时切断账户体系与产品或服务的关联措施。
- 新版规范将此前征求意见稿的账号注销处理时限从十五天放宽至十五个工作日。

此外，值得注意的是，对于相应个人信息主体的请求，新版规范还建议企业直接在移动应用程序、网页、客户端软件中，设置便捷的交互式页面提供响应的功能或选项。此前，大量企业在实践中选择通过邮件、电话、客服聊天等人工方式响应个人信息主体的权利请求，而新版规范显然提出了更高的合规标准，便捷注销渠道的要求未来可能成为执法机关关注的重点。

七、结语

相较于《网络安全法》的提纲挈领，《个人信息安全规范》自实施以来即以其内容的丰富和可操作性引起实务界的瞩目，成为企业在个人信息保护实践中的重要指引以及相关监管机构执法的参照。同时，其非强制性国家标准的性质反而赋予了其在内容和尺度上的灵活性和开放性，既能响应数字化时代技术的快速迭代变革，着手解决新问题，又能兼顾隐私保护和企业实践的平衡，确保规则最终可以落地。

正基于此，我们预期《个人信息安全规范》的修订将是一个常规的过程，以期在充满不确定性和复杂性的数字时代背景下动态地寻找数据主体权利和数据流动效益之间的平衡。企业在密切关注规则变化，确保个人信息保护合规的同时，也应保持和监管部门的有效沟通，为合规实践中面临的问题寻找解决途径。

特别声明

汉坤律师事务所编写《汉坤专递》的目的仅为帮助客户及时了解中国法律及实务的最新动态和发展，上述有关信息不应被看作是特定事务的法律意见或法律依据，上述内容仅供参考。

如您对上述内容有任何问题或建议，请与汉坤律师事务所的下列人员联系：

北京　金文玉　律师：

电话：　+86 10 8525 5557

Email：　wenyu.jin@hankunlaw.com

上海　曹银石　律师：

电话：　+86 21 6080 0980

Email：　yinshi.cao@hankunlaw.com

深圳　王哲　律师：

电话：　+86 755 3680 6518

Email：　jason.wang@hankunlaw.com

香港　陈达飞　律师：

电话：　+852 2820 5616

Email：　dafei.chen@hankunlaw.com