汉坤法律评述

2021 年 11 月 22 日

HANKUN
汉坤律师事务所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

银行金融法律

《数安条例（征求意见稿）》对金融行业的影响评述

作者：权威 | 夏迎雨 | 郑博

2021 年 11 月 14 日，国家互联网信息办公室（以下简称“**网信办**”）对外发布《网络数据安全管理条例（征求意见稿）》（以下简称“**《数安条例（征）》**”），并对外公开征求意见。

《数安条例（征）》从个人信息保护、重要数据安全、数据跨境安全管理、互联网平台运营者义务等核心维度对《中华人民共和国网络安全法》（以下简称“**《网安法》**”）《中华人民共和国数据安全法》（以下简称“**《数安法》**”）《中华人民共和国个人信息保护法》（以下简称“**《个保法》**”）项下的相关合规要求进行了全面细化，并在此基础上调整和增设了大量更严格的合规要求。

由于《数安条例（征）》项下的部分合规要求在《网安法》、《个保法》、《数安法》的基础上更为复杂且较大程度地提升了严厉程度，若《数安条例（征）》按现行版本生效，则对各类金融行业从业机构的个人信息和数据安全合规工作都将造成广泛而深远的影响。但考虑到当前版本的《数安条例（征）》的部分内容在合理程度、与上位法的衔接关系等方面仍存在一定的可商榷之处，其正式生效的版本将在多大程度上保留当前版本的内容仍有待观察。

在本文中，我们将对金融行业相关主体在《数安条例（征）》下的重点关注内容进行介绍，并对其潜在影响进行概述。

一、关注要点概述

（一）大幅提升《个保法》《数安法》下的合规要求，金融监管机关或将设专职部门负责个人信息及数据安全监管

就《数安条例（征）》的适用对象及适用地域范围而言，其在原则上与《个保法》《数安法》保持一致的前提下做了适当的扩大。在规制内容上，其规制事项并未局限于“网络数据安全”领域，而是同时作为《网安法》《数安法》以及《个保法》的下位法从个人信息保护、重要数据安全、数据跨境安全管理、互联网平台运营者义务等几个核心维度全面地细化和加强了《个保法》和《数安法》项下的合规要求，并加入了大量新增的报告、评估和前置同意类型的合规管控措施。

就其适用范围及现有内容而言，《数安条例（征）》将对于包括金融行业在内的全类型市场主体造成广泛的影响，并将进一步加大各类市场主体在数据安全、个人信息保护领域的合规义务。尤其值得注意的是，《数安条例（征）》第 55 条要求包括金融行业在内的**八大类关键行业的主管部门需要明确本行业安全保护工作机构和人员**，意味着未来“一行两会”可能会针对相关数据安全合规工作新设或指定对应的监管机构。长期以来，金融机构的监管压力主要来自于行业主管机关，即“一行两会”。而对于“一行两会”外的其他政府机关设定的监管要求，受限于有限的监管力量以及对金融业务的有限理解，可能难以对金融机构形成全面的管束，如果未来“一行两会”根据《数安条例（征）》的要求设置或指定专岗负责金融机构的个人信息保护及数据安全监管工作，并将其融入针对金融机构的日常监管、检查和评分之中，则对于金融机构的合规压力将完全不同于往日。

（二）数据安全相关监管机关对金融业主体开展的资本运作具备更多元的管控能力

《数安条例（征）》在《网络安全审查办法（征求意见稿）》的基础上进一步丰富了“网络安全审查”的适用情形，明确“赴港上市”、“汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台运营者实施合并、重组、分立”活动如“可能影响国家安全”的，亦需要进行网络安全审查申报。类似地，《数安条例（征）》还进一步要求涉及重要数据和一百万人以上个人信息的数据处理者在发生合并、重组、分立等情况时，需要向网信部门进行报告。

通过前述行政流程的设置，监管机关将基于数据安全角度的管控对市场主体开展的资本运作活动具备更多元的监管权利。在金融业机构未来开展诸如金融牌照收购、股权结构重组以及境外上市等活动时，亦有可能受限于前述的网络安全审查及报告的要求，需在实施相关项目时将其风险及流程要求同步纳入考虑。

（三）支付结算业务的合规审查义务进一步加重，相关业务风控流程需对照完善

《数安条例（征）》第 8 条以及第 41 条要求任何组织和个人不得为存在“违法违规开展数据处理活动的主体”以及“提供用于穿透、绕过数据跨境安全网关的程序、工具、线路（我们理解即‘翻墙’软件）的主体”提供支付结算服务，否则可能面临 50 万元以下的罚款或吊销相关业务许可证的罚则。

就此，银行业金融机构以及非银行支付机构等具备对外提供支付结算服务资质的机构应进一步增强对用户及商户数据处理合规情况及业务类型的管控，制定适当的审查机制及文本约束机制以避免向前述违反《数安条例（征）》的主体提供支付结算服务。

（四）“贷款导流”、“联合贷”、“基金保险导流”等业务的算法策略、流量分发的规则更加严格，未来将面临大额处罚

《数安条例（征）》第 43 条要求互联网平台运营者应当建立与数据相关的平台规则、隐私政策和算法策略披露制度，特别是第 46 条明确列举了几种禁止行为，包括“在平台规则、算法、技术、流量分配等方面设置不合理的限制和障碍，限制平台上的中小企业公平获取平台产生的行业、市场数据等，阻碍市场创新”。违反前述规定且拒不改正的可能面临“处上一年度销售额 1%以上 5%以下的罚款”。

由于《数安条例（征）》对于“互联网平台运营者”的概念界定范围相对宽泛，如果金融机构存在通过运营 APP 或小程序进行线上展业的模式，则同样有可能被认定为“互联网平台运营者”，并进而受限于对于流量分发的限制以及算法策略的披露要求。若《数安条例（征）》根据现行版本生效，则包括“贷款导流”、“联合贷”、“基金保险导流”在内的各类以“流量分发”作为核心逻辑的金融业务可能会面临被要求对其生态体系进行开放的压力。

（五）数据分类分级管理工作或将更快落地，委托处理或受限于监管部门前置同意

《数安条例（征）》再次强调了“数据分类分级保护制度”的建立，并明确行业主管机关将组织市场主体进行重要数据的识别工作，市场主体完成相关工作后，需在 15 个工作日内向网信部门完成备案。在此基础上，《数安条例（征）》还进一步要求处理重要数据的系统均需要满足“三级等保”和“关键信息基础设施”的安全保护要求。

其次，《数安条例（征）》强化了重要数据处理者的安全评估义务，要求其开展数据安全年度评估，并针对共享、交易、委托处理、向境外提供等特定环节开展数据安全评估。此外，《数安条例（征）》还进一步要求企业在进行重要数据的共享、交易、委托处理时，需经主管部门或网信办同意。

前述有关数据安全的要求进一步大幅提升了金融机构在数据治理以及数据安全领域的合规压力，特别是其中提及的“重要数据委托处理需经主管部门或网信办同意”的要求，对于“重要数据”的认定仍未给出确切的标准，将可能导致在金融业务开展过程中普遍存在的风控辅助、数据分析、客服外包、委外催收等各个业务环节受限于监管部门的前置同意，其无论是对于金融机构而言抑或对于监管部门而言都将意味着极为繁琐而繁重的工作量。考虑到其合理性以及必要性尚存一定的争议，其能否在正式生效的法规中得以保留有待进一步观察。

（六）数据跨境监管范围进一步扩大，细节规则仍有待进一步明确

在数据跨境安全管理方面，《数安条例（征）》将监管范围扩大到了全部类型的数据，即并未参照此前的相关立法将有关数据跨境的监管限于“个人信息”和“重要数据”，并统一要求数据的出境活动均需要至少满足“网信安全评估”、“个保认证”、“签署标准合同”等合规要求中的一项。

但与此同时，《数安条例（征）》也进一步明确了“个人信息处理者为履行合同所必需”而实施的个人信息出境可以豁免前述要求，一定程度上简化了“跨境贸易”、“跨境支付”等业务中可能涉及到的个人信息出境活动的合规流程要求。但对于“单独同意”要求的适用，《数安条例（征）》并未明确承认其可基于“个人信息处理者为履行合同所必需”而被豁免，但从《个保法》的体系解释角度以及从业务合理性的角度出发，我们仍倾向于认为“个人信息处理者为履行合同所必需”仍是可以豁免出境环节的“单独同意”的情形之一。

（七）有关个人信息保护的合规要求大幅度强化和调整，企业的合规压力进一步提升

1. **关于合法性基础：**《数安条例（征）》第 19 条规定基于用户同意处理个人信息的，也应当满足“提供服务所必需”或“履行法定义务所必需”的要求，这在一定程度上改变了《个保法》第 13 条设定的并行多元合法性基础（“履行合同所必需”、“履行法定义务所必需”不需取得个人同意）的模式，对于全市场范围内截止目前已经开展的个保法合规整改工作或将带来较大的困扰。

2. **关于委托处理：**《数安条例（征）》第 12、32、33 条针对“重要数据的委托处理”进行了细化规定，要求取得用户的单独同意，每年开展数据安全评估，并事先取得主管部门同意。前述规则也在较大程度上颠覆了此前相关立法中对于数据委托处理活动的合规要求。如严格按照《数安条例（征）》的要求执行，无论是对于金融机构而言亦或是主管部门而言都会造成较为繁重的合规负担，相关要求最终是否会落地执行也有待进一步观察。

3. **关于隐私政策：**《数安条例（征）》第 20 条对于个人信息处理规则（即隐私政策）的内容要求予以明确，相关市场主体可能需要对照该等内容要求进一步查漏补缺。此外，第 43 条还规定对于平台规则、隐私政策制定或者对用户权益有重大影响的修订，应当事先公开征求意见。如果相关主体被

认定为日活用户超过 1 亿的大型互联网平台（理论上金融机构的线上 APP 也有可能落入该项），还应当将前述平台规则、隐私政策等提交评估，并经主管部门同意。

4. **关于个人同意方式：**《数安条例（征）》第 21、25、49 条等对于个人同意的要求予以明确，如按照服务类型分别申请同意，敏感个人信息取得单独同意（即“数据处理者在开展具体数据处理活动时，对每项个人信息取得个人同意，不包括一次性针对多项个人信息、多种处理活动的同意”）、不得将生物特征作为唯一身份认证方式强制用户同意、收集个人信息用户个性化推荐应取得单独同意等。

5. **关于权利响应机制：**《数安条例（征）》第 23、24 条等对于用户权利的响应机制也进行了规定，要求向用户提供便捷的结构化查询机制、在 15 个工作日内反馈、规定了用户“信息可携带权”的响应范围等。但就可携带权而言，目前规定的是“基于同意或者订立、履行合同所必需而收集的个人信息”都应当响应用户的信息转移请求，我们理解该等范围界定存在一定的不明确之处，如“何为履行合同所必需”（需要与隐私政策的披露挂钩）、“通过第三方间接收集的信息是否应当转移”等，仍有待澄清。

二、应对思路与建议

整体而言，当前版本的《数安条例（征）》涵盖内容广泛，但其中仍有一定数量条款的确切含义有待进一步厘清和明确，如第 19 条对于“个人信息处理合法性基础的叠加适用”、第 33 条对于“特定数据处理活动（如委托处理）的主管部门前置同意”等均存在较大的落地难度。

就现阶段而言，我们认为金融行业的从业主体可以优先考虑针对其中有待进一步明确的内容准备相应的修订意见并反馈监管部门（意见反馈截止时间为 2021 年 12 月 13 日），或考虑就此类疑难条款的适用与监管部门沟通其具体理解。

而针对《数安条例（征）》下提及的内容相对清晰合理的合规要求，则可考虑预先进行相关的业务流程及内部合规工作的优化调整。如针对《数安条例（征）》中提及的重要数据识别、第三方的数据安全责任义务、数据安全相关自评估等工作，预先建设相关的工作流程，以便在新规生效后及时响应合规要求。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

权威

电话： +86 21 6080 0946
Email： wei.quan@hankunlaw.com