观韬中茂律师事务所 Guantao Law Firm

WeBank 微众银行

金融科技 微洞察

FISCO金链盟

# 2020 中国金融数据跨境流动监管政策报告

2020/09

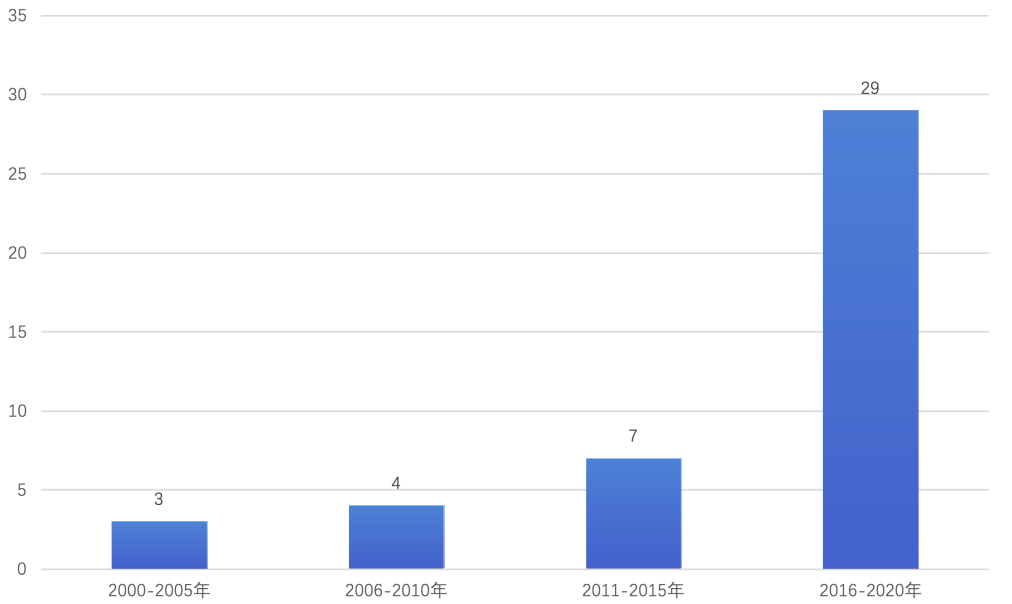
# 前言 PREFACE

## 备受关注的金融数据跨境流动

随着改革开放的不断深入，中国经济与世界经济之间的联系越来越密切，尤其是2001年中国加入世界贸易组织后，中国融入经济全球化的步伐加快，中国企业与居民与世界各个国家与地区的贸易与交往日趋频繁，其从事跨境经济活动所产生的数据往往是跨越国界的。金融是经济的血脉，越来越多的跨境贸易等经济活动随之也带来了对跨境金融的强烈需求。而提供金融服务的金融机构，一方面在提供金融服务时，期望能够获得客户的各类相关数据为其获取客户、经营决策提供支持，另一方面，出于合规管理的需要，也需要数据履行相关的义务。同时，洗钱等金融犯罪活动也由于科技的发展以及金融服务业的全球化而变得日益复杂化，各国监管机构之间也很自然的在数据交换方面有着强烈的诉求。因此，从业务、合规、监管三方面看，金融数据跨境流动必不可少。

另外，金融数据的跨境流动在带来便利的同时，也潜藏着一系列风险。金融数据与个人隐私及企业合法权益、公共权益乃至国家安全紧密相关，数据的跨境流动也必然意味着风险的复杂化、扩大化及不可控倾向。

为了应对上述数据跨境需求与风险控制之间的矛盾，保护金融数据安全，实现风险可控，在金融数据的跨境流动方面，我国立法者及金融监管部门多年来进行了大量的积极探索，近年更是愈加频繁，2015年至2020年关于与金融数据跨境流动有关的文件数量是2000年至2015年所出台文件数量总和的两倍还多（如下图）。从这些规范性文件中，我们梳理出了两条监管思路，**一是金融行业监管部门的数据跨境规制体系，二是《网络安全法》的数据跨境规制体系。**

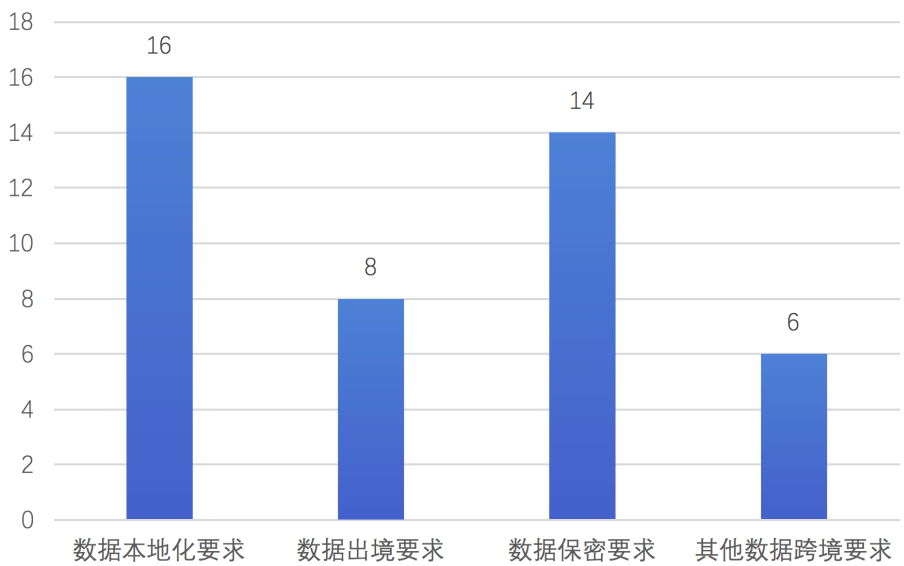



图表 1:数据跨境传输有关规范性文件数量

# 目录 CONTENTS

# 金融行业监管部门数据跨境规制体系

**根据我们对金融行业监管部门数据跨境流动方面的规范性文件的检索和分析，我们将金融行业的监管分为四个层次，分别为：数据本地化的要求、数据出境的要求、数据保密要求以及其他数据跨境要求。**下文将进行纵向、横向的交叉分析和要点提示，以期能为金融机构从业者提供内部数据治理及数据全球化部署这一“必修课”提供参考和帮助。




图表 2：不同类别的规范性文件数量

# 纵向分析

## 监管层次1:数据本地化的要求

### 1.1数据本地化要求条文梳理

监管层次 1：数据本地化规制

| 序号 | 规范性文件 | 相关条文 | 主体+客体 |
| --- | --- | --- | --- |
| 1 | 《电子银行业务管理办法》<br>银监会<br>2006.1.26 发布 | 第十条 金融机构开办以互联网为媒介的网上银行业务、手机银行业务等电子银行业务，除应具备第九条所列条件外，还应具备以下条件：……（四） 中资银行业金融机构的电子银行业务运营系统和业务处理服务器设置在中华人民共和国境内。（五） 外资金融机构的电子银行业务运营系统和业务处理服务器可以设置在中华人民共和国境内或境外。设置在境外时，应在中华人民共和国境内设置可以记录和保存业务交易数据的设施设备，能够满足金融监管部门现场检查的要求，在出现法律纠纷时，能够满足中国司法机构调查取证的要求。 | 中资银行业金融机构+电子银行业务运营系统和业务处理服务器；<br>外资金融机构+从设置在境外的电子银行业务运营系统和业务处理服务器+在境内设置记录和保存业务交易数据的设施设备 |
| 2 | 《金融机构反洗钱规定》<br>中国人民银行<br>2006.11.14 发布 | 第九条 金融机构应当按照规定建立和实施客户身份识别制度。……（四） 保证与其有代理关系或者类似业务关系的境外金融机构进行有效的客户身份识别，并可从该境外金融机构获得所需的客户身份信息。 | 金融机构+从有代理关系或类似关系的境外金融机构+获取客户身份信息 |
| 3 | 《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》<br>中国人民银行<br>2011.1.21 发布 | 六、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。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。 | 银行业金融机构+个人金融信息 |
| 4 | 《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》<br>中国人民银行上海分行<br>2011.5.12 发布 | 五、关于银行将业务系统置于境外的问题<br>境内法人银行储存、处理和分析客户个人金融信息的业务系统不应置于境外；境内不具有法人资格的分行，依靠境外总行、境外其他分行或境外关联公司的相关系统，在中国境外储存、处理和分析客户个人金融信息，应当满足以下条件：（一）取得客户书面授权或同意；（二）其境外总行或关联公司应有相应的保障措施，能够确保客户个人金融信息安全，并由总行以法人名义承担相应的法律责任。 | 境内法人银行+储存、处理和分析客户个人金融信息的业务系统 |
| 5 | 《保险公司财会工作规范》<br>中国保险监督管理委员会（已变更）<br>2012.7.1 发布 | 第八十二条 保险公司财务信息系统中的业务、财务数据应当在中国境内存储,并进行异地备份。 | 保险公司财务系统+业务数据/财务数据 |

| | | | |
|---|---|---|---|
| 6 | 《关于调整证券资格会计师事务所申请条件的通知》<br>财政部、中国证券监督管理委员会<br>2012.1.21 发布 | 第六条增加第十款：证券资格会计师事务所应当充分利用信息技术支持业务工作和管理活动。存储业务工作、客户资料的数据服务器和信息技术应用服务器应当架设在中国境内，对服务器的访问以及相关数据调用应当保存清晰完整的日志 | 证券资格会计师事务所+存储业务工作、客户资料的数据服务器和信息技术应用服务器 |
| 7 | 《征信业管理条例》<br>国务院<br>2013.1.21 发布 | 第二十四条 征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。<br>征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定。 | 征信机构+境内采集的信息 |
| 8 | 《非银行支付机构网络支付业务管理办法》<br>中国人民银行<br>2015.12.28 发布 | 第二十六条 支付机构应当在境内拥有安全、规范的网络支付业务处理系统及其备份系统，制定突发事件应急预案，保障系统安全性和业务连续性。<br>支付机构为境内交易提供服务的，应当通过境内业务处理系统完成交易处理，并在境内完成资金结算。 | 支付机构+网络支付业务处理系统、备份系统 |
| 9 | 《网络借贷信息中介机构业务活动管理暂行办法》<br>银监会、工信部、公安部、网信办<br>2016.8.17 发布 | 第二十七条 第三款 在中国境内收集的出借人与借款人信息的储存、处理和分析应当在中国境内进行。除法律法规另有规定外，网络借贷信息中介机构不得向境外提供境内出借人和借款人信息。 | 网络借贷信息中介机构+境内收集的出借人信息/借款人信息 |
| 10 | 《中国银行业监督管理委员会中资商业银行行政许可事项实施办法》<br>银保监会<br>2018.8.17 修订 | 第九十八条 开办以互联网为媒介的网上银行业务、手机银行业务等电子银行业务，除应具备第九十七条所列条件外，还应具备以下条件：……（四）电子银行业务运营系统和业务处理服务器设置在中华人民共和国境内。 | 中资银行的电子银行+业务运营系统和业务处理服务器 |
| 11 | 《外商投资期货公司管理办法》<br>证监会<br>2018.8.24 发布 | 第十五条 外商投资期货公司交易、结算、风险控制等信息系统的核心服务器以及记录、存储客户信息的数据设备，应当设置在中国境内。<br>在符合法律、行政法规和中国证监会有关规定的前提下，外商投资期货公司可以利用境外股东的资源和技术，提升信息系统的效率和安全水平。 | 外商投资期货公司+核心服务器/记录存储客户信息的数据设备 |
| 12 | 《中国银保监会外资银行行政许可事项实施办法》<br>银保监会<br>2019.12.26 发布 | 第一百二十条 外商独资银行、中外合资银行申请开办信用卡发卡业务，除应当具备本办法第一百一十九条规定的条件外，还应当具备下列条件：……（二）具备办理信用卡业务的专业系统。在中国境内建有发卡业务主机、信用卡业务申请管理系统、信用评估管理系统、信用卡账户管理系统、信用卡交易授权系统、信用卡交易监测和伪冒交易预警系统、信用卡客户服务中心系统、催收业务管理系统等专业化运营基础设施，相关设施通过了必要的安全检测和业务测试，能够保障客户资料和业务数据的完整性和安全性。<br>第一百二十一条 外商独资银行、中外合资银行申请开办信用卡收单业务，除应当具备本办法第一百一十九条规定的条件外，还应当具备下 | 外商独资银行、中外合资银行+信用卡发卡业务专业系统<br>外商独资银行、中外合资银行+信用卡收单业务专业系统 |

| | | | |
|---|---|---|---|
| | | 列条件：……（二）具备办理收单业务的专业系统。在中国境内建有收单业务主机、特约商户申请管理系统、特约商户信用评估管理系统、特约商户结算账户管理系统、账务管理系统、收单交易监测和伪冒交易预警系统、交易授权系统等专业化运营基础设施，相关设施通过了必要的安全检测和业务测试，能够保障客户资料和业务数据的完整性和安全性； | |
| 13 | 《中国银保监会外资银行行政许可事项实施办法》<br>银保监会<br>2019.12.26 发布 | 第九十四条外商独资银行、中外合资银行申请解散，应当向银保监会或者所在地银保监局提交下列申请资料（一式两份），同时抄送所在地银保监分局（一份）：……（五）……客户身份资料和业务档案移交在中国境内依法设立的档案保管机构的相关说明；<br>第九十八条 外商独资银行、中外合资银行申请关闭分行或者分行级专营机构，外国银行申请关闭分行，应当具备下列条件：……（三）具有有效的资产处置、债务清偿、人员安置及客户身份资料和业务档案在中国境内保存的方案。 | 外商独资银行、中外合资银行+解散时+客户身份资料和业务档案在中国境内保存<br><br>外商独资银行、中外合资银行、外国银行+关闭分行时+客户身份资料和业务档案在中国境内保存 |
| 14 | 《信用评级业管理暂行办法》<br>中国人民银行、发改委、财政部、证监会<br>2019.11.26 发布 | 第三十条第二款 信用评级机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。信用评级机构向境外组织或者个人提供信息，应当遵守法律法规以及信用评级行业主管部门和业务管理部门的有关规定。 | 信用评级机构+境内采集的信息 |
| 15 | 《个人金融信息（数据）保护试行办法（初稿）》 | 第二十条 (个人金融信息跨境流动的要求)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。除法律、法规、规章及有关主管部门另有规定外，金融机构不得向境外提供境内个人金融信息。境内金融机构为处理跨境业务向境外机构（含总公司、母公司或者分公司、子公司以及其他为完成该业务所必需的关联机构）提供境内收集的个人金融信息的，应当事先取得信息主体的明示同意，并依法开展个人金融信息出境安全评估。未经评估或者经评估存在显著风险隐患的，境内金融机构不得向境外机构提供个人金融信息。<br>境内金融机构向境外机构提供境内收集的个人金融信息的，应当与境外机构签订协议明确对方的职责和义务。个人金融信息出境后，境内金融机构应当建立个人金融信息出境记录并且至少保存 5 年，并通过现场核查等必要措施，监督境外机构有效履行保护个人金融信息安全的职责和义务，持续保障个人金融信息安全。 | 金融机构+境内收集的个人金融信息 |
| 16 | 《JR/T0171-2020 个人金融信息保护技术规范》<br>中国人民银行<br>2020.2.13 发布 | 7.1.3 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，具体要求如下：<br>• 应符合国家法律法规及行业主管部门有关规定； | 持牌金融机构、涉及个人金融信息处理的相关机构+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 |

| | | | |
|---|---|---|---|
| | | • 应获得个人金融信息主体明示同意；<br>• 应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；<br>• 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。 | |

**1.2数据本地化要求要点提示**

**1.2.1数据本地化可以理解为对数据信息的境内存储要求，**通过要求相关数据信息在某国家或区域范围内进行存储，来实现对特定数据信息相对独立自主的占用、处理、管理效果。

**1.2.2数据本地化的要求并非近年才有。**通过上表我们可以看到，2006年银监会在《电子银行行业务管理办法》中，已就中资银行的相关运营系统和服务器做出了设置在境内的要求。除金融数据以外，我们还检索到1982年《关于对外合作开采海洋石油资源资料管理的规定》中要求“运往国外的原始资料，在复制或使用完毕后，应及时运回中国境内保存”。也即，在数据信息的跨境流动还未像当下如此便捷和频繁的时期，国家已对特定数据信息做出了本地化的要求。

**1.2.3数据本地化不仅针对数据信息还针对数据信息的载体。**比如，上表中《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》中的数据本地化客体是“个人金融信息”，但《电子银行业务管理办法》、央行上海分行《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》、《中国银行业监督管理委员会中资商业银行行政许可事项实施办法》、《非银行支付机构网络支付业务管理办法》等文件都对相关金融机构或第三方支付机构的运营系统/业务处理系统/存储数据设备这类数据信息的载体做出设置在境内的要求。

**1.2.4数据本地化存储的方式一般包括境内物理服务器或云服务器。**在“数据上云”越来越普遍的当下，我们也应关注到如果使用云服务存储数据信息应当如何应对数据本地化的要求。尽管目前我们还未检索到对“境内存储”的存储方式作出明确规定的金融行业监管规范性文件，但从2018年8月《国务院办公厅关于加强政府网站域名管理的通知》中提出的，对于“自行建设运维的政府网站服务器不得放在境外；租用网络虚拟空间的，所租用的空间应当位于服务商的境内节点”我们可以分析出，如果相关数据信息有境内存储要求，且企业选择云服务器进行存储的情况下，应当注重选择服务商境内节点所提供的云服务。

## 监管层次2:数据出境要求

### 2.1数据出境要求条文梳理

监管层次 2：数据出境要求

| 序号 | 规范性文件 | 相关条文 | 主体+客体 |
| --- | --- | --- | --- |
| 1 | 《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》<br>中国人民银行<br>2011.1.21 发布 | 六、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。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。 | 银行业金融机构+个人金融信息 |
| 2 | 《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》<br>中国人民银行上海分行<br>2011.5.12 发布 | 四、关于银行业金融机构向境外提供个人金融信息的问题<br>《 通知 》 第六条规定： “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。” 为客户办理业务所必需，且经客户书面授权或同意，境内银行业金融机构向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规。银行业金融机构应当保证其境外总行、母行或分行、子行为所获得的个人金融信息保密。 | 银行业金融机构+个人金融信息 |
| 3 | 《个人金融信息（数据）保护试行办法（初稿）》 | 第二十条 (个人金融信息跨境流动的要求)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。除法律、法规、规章及有关主管部门另有规定外，金融机构不得向境外提供境内个人金融信息。境内金融机构为处理跨境业务向境外机构（含总公司、母公司或者分公司、子公司以及其他为完成该业务所必需的关联机构）提供境内收集的个人金融信息的，应当事先取得信息主体的明示同意，并依法开展个人金融信息出境安全评估。未经评估或者经评估存在显著风险隐患的，境内金融机构不得向境外机构提供个人金融信息。<br>境内金融机构向境外机构提供境内收集的个人金融信息的，应当与境外机构签订协议明确对方的职责和义务。个人金融信息出境后，境内金融机构应当建立个人金融信息出境记录并且至少保存 5 年，并通过现场核查等必要措施，监督境外机构有效履行保护个人金融信息安全的职责和义务，持续保障个人金融信息安全。 | 金融机构+境内收集的个人金融信息 |
| 4 | 《JR/T0171-2020 个人金融信息保护技术规范》<br>中国人民银行<br>2020.2.13 发布 | 7.1.3 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，具体要求如下：<br>• 应符合国家法律法规及行业主管部门有关规 | 持牌金融机构、涉及个人金融信息处理的相关机构+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 |

| | | | |
|---|---|---|---|
| | | • 应获得个人金融信息主体明示同意；<br>• 应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；<br>• 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。 | |
| 5 | 《银行业金融机构反洗钱和反恐怖融资管理办法》<br>银保监会<br>2019.1.29 发布 | 第二十八条 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，非依法律、行政法规规定，银行业金融机构不得向境外提供。<br>银行业金融机构对于涉及跨境信息提供的相关问题应当及时向银行业监督管理机构报告，并按照法律法规要求采取相应措施。 | 银行业金融机构+因反洗钱/反恐怖融资义务获取的客户身份资料和交易信息 |
| 6 | 《证券法》<br>全国人大常委<br>2019.12.18 修订 | 第一百七十七条第二款 境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料。 | 任何单位和个人+证券业务活动有关的文件和资料 |
| 7 | 《征信业管理条例》<br>国务院<br>2013.1.21 发布 | 第二十四条 征信机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。<br>征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院征信业监督管理部门的有关规定。 | 征信机构+境内采集的信息 |
| 8 | 《信用评级业管理暂行办法》<br>中国人民银行、发改委、财政部、证监会<br>2019.11.26 发布 | 第三十条第二款 信用评级机构在中国境内采集的信息的整理、保存和加工，应当在中国境内进行。信用评级机构向境外组织或者个人提供信息，应当遵守法律法规以及信用评级行业主管部门和业务管理部门的有关规定。 | 信用评级机构+信息 |

### 2.2数据出境要求要点提示

**2.2.1对于个人金融信息出境的要求逐步明确。**对比上表中规范性文件对于个人金融信息出境的限制要求，我们可以看到如下图中的变化。一方面对于个人金融信息出境的限制不再一刀切，将金融机构跨境开展业务的需要纳入跨境传输监管的考量因素之中；另一方面，出境的条件要求逐渐增多，以严格把控个人金融信息跨境传输可能出现的风险。

除法律法规及中国人民银行另有规定+不得提供

↓

业务需要+授权同意+向总/分/母/子行+境外机构保密义务

↓

业务需要+明示同意+向必要关联机构+符合监管规定+开展安全评估+境外机构数据安全保护能力达标+签订协议/现场核查等措施确保对境外机构的保密、删除、案件协查义务

**2.2.2数据信息的范围可解释空间较大，需要从业机构审慎把握。**数据出境要求主要涉及的数据信息类型包括个人金融信息、企业和个人信用信息、证券业务活动有关的文件或资料、因反洗钱/反恐怖融资义务获取的客户身份资料和交易信息，其中前三类信息的范围规定都较为宽泛，留有较大的解释空间。如，对个人金融信息的范围限定上，相关文件都有类似“金融机构在与个人建立业务关系过程中获取、保存的其他个人信息”、“ 及其他反映特定个人某些情况的信息”的“兜底条款”；同样的，企业和个人的信用信息范围在《征信业管理条例》中并未有明确规定，但根据《个人信用信息基础数据库管理暂行办法》，个人信息包括“个人基本信息、个人信贷交易信息以及反映个人信用状况的其他信息”。

**2.2.3关注金融行业标准《JR/T0171-2020个人金融信息保护技术规范》（以下简称“《规范》”）。**《规范》是今年2月13日由央行发布的推荐性行业标准，是对金融行业有关主体在个人金融信息安全管理和安全技术方面的指导建议。虽然《规范》在效力上属于推荐性行业标准，并无强制执行力，但是金融行业监管部门很可能将《规范》作为参考依据，在具体的执法行动或监督检查中适用。对于“个人金融信息”的出境而言，《规范》第7.1.3条的要求严苛，并且“开展安全评估”的具体流程以及“境外机构的数据安全保护能力达标”的具体要求还有待明确，但足以体现央行对于个人金融信息出境方面的监管的精细化和审慎，应当引起金融机构的足够关注。此外，根据《规范》第7.1.3条的提示，金融机构也应关注国家、行业有关部门制定办法与标准以开展“个人金融信息出境安全评估”。

**2.2.4关注消费者金融信息跨境传输规定的变化。**央行在今年9月15日发布的《中国人民银行金融消费者权益保护实施办法》中，不仅没有保留2019年12月改文件征求意见稿中关于我国消费者金融信息境内存储和跨境传输的规定，同时也删去了2016年版本中关于个人金融信息境内存储和跨境传输的规定，如下表。我们分析，央行删除跨境传输规定，不代表此后个人（消费者）

金融信息的跨境传输不再受到相关监管，而是可能为国家、行业有关部门制定的个人信息、个人金融信息跨境传输的规定预留立法空间：首先，未来央行可能在正式出台的《个人金融信息（数据）保护试行办法》或类似文件中规定个人金融信息跨境传输的规制要求。其次，银行业金融机构很可能被列为关键信息基础设施运营者，因此在个人信息跨境传输上可受制于《网络安全法》及配套法律法规的规定。最后，《个人信息保护法》的出台，也可能对个人信息的保护和跨境传输做出进一步的规定。

| 序号 | 规范性文件 | 相关条文 | 结构：主体+客体 |
| --- | --- | --- | --- |
| 1 | 《中国人民银行金融消费者权益保护实施办法》<br>中国人民银行<br>（银发〔2016〕314号文印发）<br>2016.12.14 发布<br>（已失效） | 第三十三条 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。除法律法规及中国人民银行另有规定外，金融机构不得向境外提供境内个人金融信息。<br>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，并通过签订协议、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。 | 银行业金融机构、其他金融机构、非银行支付机构+境内收集的个人金融信息 |
| 2 | 《中国人民银行金融消费者权益保护实施办法（征求意见稿）》<br>中国人民银行<br>2019.12.27 发布 | 第三十四条 在中国境内收集的消费者金融信息的存储、处理和分析应当在中国境内进行。因业务需要，确需向境外提供消费者金融信息的，应当同时符合以下条件：<br>（一）为处理跨境业务所必需；<br>（二）经金融消费者书面授权；<br>（三）信息接收方为完成该业务所必需的关联机构（含总公司、母公司或者分公司、子公司等）；<br>（四）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消费者金融信息保密；<br>（五）符合法律法规和其他相关监管部门的规定。 | 银行业金融机构、非银行支付机构+境内收集的消费者金融信息 |
| 3 | 《中国人民银行金融消费者权益保护实施办法》<br>中国人民银行<br>中国人民银行令〔2020〕第5号<br>2020年9月15日发布 | （2020年9月15日发布的《中国人民银行金融消费者权益保护实施办法》，已删除2016年版本中关于个人/消费者金融信息跨境传输的有关规定。） | |

## 监管层次3：数据保密要求

### 3.1数据保密要求条文梳理

监管层次 3：数据保密要求

| 序号 | 规范性文件 | 相关条文 | 结构：主体+客体 |
|---|---|---|---|
| 1 | 《个人存款账户实名制规定》<br>国务院<br>2000.3.20 发布 | 第八条 金融机构及其工作人员负有为个人存款账户的情况保守秘密的责任。<br>金融机构不得向任何单位或者个人提供有关个人存款账户的情况，并有权拒绝任何单位或者个人查询、冻结、扣划个人在金融机构的款项；但是，法律另有规定的除外。 | 金融机构+个人存款账户的情况 |
| 2 | 《人民币银行结算账户管理办法》<br>中国人民银行<br>2003.4.10 发布 | 第九条 银行应依法为存款人的银行结算账户信息保密。对单位银行结算账户的存款和有关资料，除国家法律、行政法规另有规定外，银行有权拒绝任何单位或个人查询。对个人银行结算账户的存款和有关资料，除国家法律另有规定外，银行有权拒绝任何单位或个人查询。 | 银行+存款人的银行结算账户信息 |
| 3 | 《个人信用信息基础数据库管理暂行办法》<br>中国人民银行<br>2005.8.18 发布 | 第五条 中国人民银行、商业银行及其工作人员应当为在工作中知悉的个人信用信息保密。 | 商业银行+个人信用信息 |
| 4 | 《反洗钱法》<br>全国人大常委<br>2006.10.31 发布 | 第五条第一款 对依法履行反洗钱职责或者义务获得的客户身份资料和交易信息，应当予以保密；非依法律规定，不得向任何单位和个人提供。 | 金融机构、特定非金融机构+因反洗钱获取的客户身份资料和交易信息 |
| 5 | 《金融机构反洗钱规定》<br>中国人民银行<br>2006.11.14 发布 | 第十五条 金融机构及其工作人员对依法履行反洗钱义务获得的客户身份资料和交易信息应当予以保密；非依法律规定，不得向任何单位和个人提供。<br>金融机构及其工作人员应当对报告可疑交易、配合中国人民银行调查可疑交易活动等有关反洗钱工作信息予以保密，不得违反规定向客户和其他人员提供。 | 金融机构、特定非金融机构+因反洗钱/反恐怖融资获知的客户身份资料、交易信息和反洗钱和反恐怖融资工作信息 |
| 6 | 《中国人民银行关于证券期货业和保险业金融机构严格执行反洗钱规定防范洗钱风险的通知》<br>中国人民银行<br>2007.1.30 | 二(五) 证券期货业和保险业金融机构应当履行的其他反洗钱义务包括：按照反洗钱预防、监控制度的要求，开展对本机构反洗钱工作人员反洗钱培训和对客户的反洗钱宣传工作；对依法履行反洗钱义务获得的客户身份资料和交易信息，应当予以保密；依法配合人民银行进行反洗钱调查等。 | 证券公司、期货经纪公司、基金管理公司、保险公司、保险资产管理公司+因反洗钱/反恐怖融资获知的客户身份资料、交易信息 |
| 7 | 《支付机构反洗钱和反恐怖融资管理办法》<br>中国人民银行<br>2012.3.5 发布 | 第九条 支付机构及其工作人员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应当予以保密；非依法律规定，不得向任何单位和个人提供。<br>支付机构及其工作人员应当对报告可疑交易、配合中国人民银行及其分支机构调查可疑交易活动等有关反洗钱和反恐怖融资工作信息予以保密，不得违反规定向客户和其他人员提供。 | 取得支付业务许可证的非金融机构（支付机构）+因反洗钱/反恐怖融资获知的客户身份资料、交易信息和反洗钱和反恐怖融资工作信息 |
| 8 | 《非银行支付机构网络支付业务管理办法》<br>中国人民银行<br>2015.12.28 发布 | 第二十条 支付机构应当依照中国人民银行有关客户信息保护的规定，制定有效的客户信息保护措施和风险控制机制，履行客户信息保护责任。……支付机构应当以“最小化”原则采集、使用、存储和传输客户信息，并告知客户相关信息的使用目的和范围。支付机构不得向其他机构或个人提供客户信息，法律法规另有规定，以及 | 支付机构+客户信息 |

| | | | |
|---|---|---|---|
| | | 经客户本人逐项确认并授权的除外。 | |
| 9 | 《中国人民银行金融消费者权益保护实施办法》<br>中国人民银行<br>2020.9.15 发布 | 第三十四条第二款银行、支付机构及其工作人员应当对消费者金融信息严格保密，不得泄露或者非法向他人提供。 | 银行业金融机构、非银行支付机构+消费者金融信息 |
| 10 | 《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》<br>中国人民银行、银保监会、证监会<br>2018.10.10 发布 | 第九条 从业机构及其员工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应当予以保密。非依法律规定，不得向任何单位和个人提供。<br>从业机构及其员工应当对报告可疑交易、配合中国人民银行及其分支机构开展反洗钱调查等有关反洗钱和反恐怖融资工作信息予以保密，不得违反规定向任何单位和个人提供。 | 互联网金融从业机构+因反洗钱/反恐怖融资获知的客户身份资料、交易信息和反洗钱和反恐怖融资工作信息 |
| 11 | 《银行业金融机构反洗钱和反恐怖融资管理办法》<br>银保监会<br>2019.1.29 发布 | 第二十二条 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，银行业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。 | 银行业金融机构+因反洗钱/反恐怖融资获得的客户身份资料和交易信息 |
| 12 | 《证券法》<br>全国人大常委<br>2019.12.18 修订 | 第四十一条 证券交易场所、证券公司、证券登记结算机构、证券服务机构及其工作人员应当依法为投资者的信息保密，不得非法买卖、提供或者公开投资者的信息。<br>证券交易场所、证券公司、证券登记结算机构、证券服务机构及其工作人员不得泄露所知悉的商业秘密。 | 证券交易场所/证券公司/证券登记结算机构/证券服务机构+投资者的信息 |
| 13 | 《信用评级业管理暂行办法》<br>中国人民银行、发改委、财政部、证监会<br>2019.11.26 发布 | 第三十条第一款 信用评级机构应当建立信用评级业务信息保密制度。对于在开展信用评级业务、处理信用评级数据库系统过程中知悉的国家秘密、商业秘密和个人隐私，信用评级机构及其从业人员应当依法履行保密义务。 | 信用评级机构+开展评级过程中知悉的国家秘密、商业秘密、个人隐私 |
| 14 | 《网络借贷信息中介机构业务活动管理暂行办法》<br>银监会、工信部、公安部、网信办<br>2016.8.17 发布 | 第二十七条第一款、第二款 网络借贷信息中介机构应当加强出借人与借款人信息管理，确保出借人与借款人信息采集、处理及使用的合法性和安全性。<br>网络借贷信息中介机构及其资金存管机构、其他各类外包服务机构等应当为业务开展过程中收集的出借人与借款人信息保密，未经出借人与借款人同意，不得将出借人与借款人提供的信息用于所提供服务之外的目的。 | 网络借贷信息中介机构/资金存管机构/其他各类外包服务机构+境内收集的出借人信息/借款人信息 |

### 3.2数据保密要求要点提示

**2.2.1对于个人金融信息出境的要求逐步明确。**对比上表中规范性文件对于个人金融信息出境的限制要求，我们可以看到如下图中的变化。一方面对于个人金融信息出境的限制不再一刀切，将金融机构跨境开展业务的需要纳入跨境传输监管的考量因素之中；另一方面，出境的条件要求逐渐增多，以严格把控个人金融信息跨境传输可能出现的风险。

**3.2.1相关主体在进行数据跨境传输时不能忽视对传统数据保密合规义务的履行。**保密义务的内涵为“除法律法规另有规定外，不得向任何单位或者个人提供”此类数据信息。严格来看，这种金融行业数据保密的要求制约着数据跨境传输至其他主体的情形。此外，“法律法规的另有规定”也一般指的是公权力介入要求提供相关数据信息的情形。

**3.2.2数据保密是金融机构较为传统的合规要求。**在21世纪初，金融行业数据跨境流动还未像现在如此频繁以及受到重视的时候，监管就要求金融机构就负有为存款账户信息、因反洗钱/反恐怖融资获知的客户身份资料、交易信息、个人信用信息等数据信息进行保密的义务。

**3.2.3数据保密要求的义务主体扩大。**虽然我国金融科技发展起源可追溯至上世纪90年代，但从上表我们可以看到，在2000年至2010年间，数据保密义务的主体主要为传统持牌金融机构，如银行、信托投资公司、证券公司、期货经纪公司、保险公司等。即使，2006年《反洗钱法》规定“特定非金融机构”也应当对“因反洗钱获取的客户身份资料和交易信息”履行保密义务，但并未明确“特定非金融机构”有哪些，并且在第35条中明确“应当履行反洗钱义务的特定非金融机构的范围、其履行反洗钱义务和对其监督管理的具体办法，由国务院反洗钱行政主管部门会同国务院有关部门制定。”在2003年以后，电子商务在我国开始兴起，非银行支付机构登上舞台。在接下来的十年间，互联网技术与金融行业进一步加速融合，蓬勃发展。为应对高速发展过程中不断涌现的问题，在2010年至今，监管部门针对非银行支付机构、互联网金融从业机构以及信用评级机构，制定了对客户身份和交易信息、消费者金融信息、个人隐私信息、网络借贷中出借人和借款人信息等数据信息的保密要求，“特定非金融机构”的范围逐步清晰。其实，不限于数据保密的要求，由于互联网金融以及金融科技的迅猛发展，“特定非金融机构”掌握的数据量激增和数据重要程度提升，针对“特定非金融机构”，在对数据信息的跨境传输上的其他要求（如数据本地化要求、数据出境的要求）上，也日渐向传统持牌金融机构靠拢。

## 监管层次4:其他数据跨境活动要求

### 4.1条文梳理

监管层次 4：其他数据跨境活动要求

| 序号 | 规范性文件 | 相关条文 | 主体+义务 |
| --- | --- | --- | --- |
| 1 | 《金融机构反洗钱规定》<br>中国人民银行<br>2006.11.14 发布 | 第五条 中国人民银行依法履行下列反洗钱监督管理职责：……（六） 按照有关法律、行政法规的规定，与境外反洗钱机构交换与反洗钱有关的信息和资料。<br>第六条 中国人民银行设立中国反洗钱监测分析中心，依法履行下列职责：……（五） 经中国人民银行批准，与境外有关机构交换信息、资料。 | 中国人民银行、中国反洗钱监测分析中心依法与境外机构交换反洗钱有关信息和资料 |
| 2 | 《银行业金融机构反洗钱和反恐怖融资管理办法》<br>银保监会<br>2019.1.29 发布 | 第三十一条 国务院银行业监督管理机构依法履行下列反洗钱和反恐怖融资监督管理职责：……（九）指导银行业金融机构应对境外协助执行案件、跨境信息提供等相关工作。 | 银行业监督管理机构指导金融机构应对反洗钱和反恐怖融下境外协助执行、跨境信息提供 |
| 3 | 《证券法》<br>全国人大常委<br>2019.12.18 修订 | 第一百七十七条第二款 境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料。<br><br>第一百七十七条第一款 国务院证券监督管理机构可以和其他国家或者地区的证券监督管理机构建立监督管理合作机制，实施跨境监督管理。 | 证券监督管理机构与境外证券监督管理机构开展合作，实施跨境监督管理。 |
| 4 | 《金融机构反洗钱规定》<br>中国人民银行<br>2006.11.14 发布 | 第十四条 金融机构及其工作人员应当依法协助、配合司法机关和行政执法机关打击洗钱活动。<br>金融机构的境外分支机构应当遵循驻在国家或者地区反洗钱方面的法律规定，协助配合驻在国家或者地区反洗钱机构的工作。 | 金融机构的境外分支机构+配合驻在国/地区监管工作 |
| 5 | 《银行业金融机构反洗钱和反恐怖融资管理办法》<br>银保监会<br>2019.1.29 发布 | 第二十六条第一款 银行业金融机构应当做好境外洗钱和恐怖融资风险管控和合规经营工作。境外分支机构和附属机构要加强与境外监管当局的沟通，严格遵守境外反洗钱和反恐怖融资法律法规及相关监管要求。 | 银行业金融机构境外分支机构+配合境外监管要求 |
| 6 | 《支付机构反洗钱和反恐怖融资管理办法》<br>中国人民银行<br>2012.3.5 发布 | 第七条 支付机构应要求其境外分支机构和附属机构在驻在国家（地区）法律规定允许的范围内，执行本办法有关客户身份识别、客户身份资料和交易记录保存工作的要求，驻在国家（地区）有更严格要求的，遵守其规定。如果本办法的要求比驻在国家（地区）的相关规定更为严格，但驻在国家（地区）法律禁止或者限制境外分支机构和附属机构实施本办法，支付机构应向中国人民银行报告。 | 7! 取得支付业务许可证的非金融机构（支付机构）+ 在驻在国/地区法律允许范围内执行《支付机构反洗钱和反恐怖融资管理办法》 |

### 4.2要点分析

**4.2.1由监管部门直接负责的数据信息跨境传输。**上表中的前三个文件列举了三种情形下的数据跨境传输将由相关监管部门进行负责，金融机构在其中如有数据信息跨境传输行为，需要接受监管部门的监督指导或批准：一是向境外反洗钱机构提供信息和资料；二是应对境外协助执行的反洗钱或反恐怖融资案件；三是向境外提供证券业务活动有关的文件和资料。

**4.2.2境外分支机构的数据信息提供义务。**通过上表中的后三个文件我们可以看到，境外分支机构在开展业务的过程中，为开展业务以及履行反洗钱/反恐怖融资义务，将进行客户身份识别、客户身份资料和交易记录保存等工作。在此过程中，可能存在两种形式向境外监管部门提供数据信息，一是由境外分支机构直接提供相关数据信息；二是，境外分支机构将相关数据信息传输至境内总行/总部保存的，可能需要由总行/总部向提供相关数据信息。由于第二种形式，与“由监管部门直接负责的数据信息跨境传输”的情形存在重合，建议金融机构同样在相关监管部门的监督和指导下进行。

## 横向分析

在对上述四个监管层次的要求进行横向对比分析后，我们认为需要关注以下方面：

**1.数据本地化要求与数据出境要求**

我们认为，数据本地化要求和数据出境要求都是监管部门通过行政方式干预数据跨境流动的限制性手段，但是两者的侧重点不同。综合比对数据本地化要求和数据出境要求我们可以看到，存在三种组合形式（如下表）：一是可以在境外存储，但境内也应存储；二是仅要求在境内存储，但未限制跨境传输；三是要求境内存储，同时限制/禁止跨境传输。

| | |
|---|---|
| **组合 1：**<br>可以在境外存储，但境内也应存储 | 《电子银行业务管理办法》银监会 2006.1.26 发布<br>第十条（五） 外资金融机构的电子银行业务运营系统和业务处理服务器可以设置在中华人民共和国境内或境外。设置在境外时，应在中华人民共和国境内设置可以记录和保存业务交易数据的设施设备，能够满足金融监管部门现场检查的要求，在出现法律纠纷时，能够满足中国司法机构调查取证的要求。 |
| **组合 2：**<br>仅要求在境内存储，但未限制跨境传输 | 《保险公司财会工作规范》中国保险监督管理委员会（已变更）2012.7.1<br>第八十二条 保险公司财务信息系统中的业务、财务数据应当在中国境内存储,并进行异地备份。 |
| **组合 3：**<br>要求境内存储，同时限制/禁止跨境传输 | 《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》2011.1.21 发布<br>六、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。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。 |

**2. 对传统数据保密要求的突破效果**

同时，我们也关注到一些规范性文件关于数据跨境传输的规定，实质上产生了对传统数据保密要求的突破效果。例如下表中，2000年国务院发布的规定中对个人存款账户数据做出保密的要求；2011年1月央行的文件中要求“银行业金融机构不得向境外提供境内个人金融信息”，且根据该文件，个人金融信息包含了个人账户信息。**但2011年5月央行上海分行的文件对前述两个文件都做出了突破，允许母行与子行之间在满足一定条件下跨境传输个人金融信息。**法律意义上，母行和子行是不同法人主体，也即，子行向母行（或母行向子行）传输数据信息，可以理解为保密主体向其他单位传输数据信息，是突破了保密要求的。但央行上海分行的文件提出，对于母行与子行之间在满足“业务必需+客户同意+确保保密”的条件下，跨境提供境内个人金融信息可不视为违规。此后，央行在2020年发布的《JR/T0171-2020 个人金融信息保护技术规范》，在确认上海分行的该种数据跨境传输条件框架下，又添加了签订协议、现场核查等要求，在一定程度上“抵消”了传统的数据保密合规要求对数字化时代下数据需要在业务关联度较高的不同法人主体间跨境传递的“负面影响”。

| 序号 | 规范性文件 | 涉及的数据信息 | 要求 |
|---|---|---|---|
| 1 | 《个人存款账户实名制规定》<br>国务院<br>2000.3.20 发布 | 个人存款账户信息 | 金融机构及其工作人员负有为个人存款账户的情况保守秘密的责任。<br>金融机构不得向任何单位或者个人提供有关个人存款账户的情况，并有权拒绝任何单位或者个人查询、冻结、扣划个人在金融机构的款项；但是，法律另有规定的除外。 |
| 2 | 《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》<br>中国人民银行<br>2011.1.21 发布 | 个人金融信息：个人身份信息、个人财产信息、个人账户信息、个人信息用信息、个人金融交易信息、衍生信息、业务过程中获取 | 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。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。 |

| | | | |
|---|---|---|---|
| 3 | 《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》<br>中国人民银行上海分行<br>2011.5.12 发布 | 或保存的其他个人信息。 | 为客户办理业务所必需，且经客户书面授权或同意，境内银行业金融机构向境外总行、母行或分行、子行提供境内个人金融信息的，可不认为违规。银行业金融机构应当保证其境外总行、母行或分行、子行为所获得的个人金融信息保密。 |
| 4 | 《JR/T0171-2020 个人金融信息保护技术规范》<br>中国人民银行<br>2020.2.13 发布 | 个人金融信息：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。<br>注 1 :本标准中的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。 | 7.1.3 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，具体要求如下：<br>• 应符合国家法律法规及行业主管部门有关规定；<br>• 应获得个人金融信息主体明示同意；<br>• 应依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；<br>• 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。 |

# 《网络安全法》数据跨境规制体系

《网络安全法》(以下简称“网安法”)数据跨境规制体系主要是以其第三十七条为中心展开的——“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,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;法律、行政法规另有规定的,依照其规定。”

为便于研究,我们将该条拆分为如下表中的结构,并在下文中对在业务过程中困扰企业较多的**1)主体——关键信息基础设施运营者,2)客体——个人信息/重要数据**以及**3)要求——安全评估**这三项要素作出分析。

| | 数据本地化 | 数据出境 |
|---|---|---|
| 主体 | 关键信息基础设施运营者 | |
| 客体 | 个人信息/重要数据 | |
| 条件 | 境内运营中收集和产生 | 境内运营中收集和产生+因业务需要 |
| 要求 | 境内存储 | 安全评估 |
| 例外 | 法律、行政法规另有规定,依照其规定 | |

## 主体:关键信息基础设施运营者(CIIO)

根据网安法第31条至39条,“关键信息基础设施的运营者”(以下简称“CIIO”)在个人信息和重要数据的跨境流动上受到较多限制,以及较一般网络运营者,CIIO对于所持有的关键信息基础设施(以下简称“CII”)负有更多的安全保护义务,因此对于网络运营者来说,明晰自身是否运营CII意义重大。

我们将与CII有关的重要文件或监管部门重要行动脉络进行了梳理，如下表：

| | |
|---|---|
| 2003 年 8 月 | 国家信息化领导小组关于加强信息安全保障工作的意见提出 “要重点保护基础信息网络和和关系国家安全、经济命脉、社会稳定等方面的重要信息系统” |
| 2014 年 2 月 | 中央网络安全和信息化领导小组第一次会议中，习近平提出建设网络强国，做好网络安全和信息化工作，并提出进行关键信息基础设施保护立法工作 |
| 2016 年 7 月 | 中央网络安全和信息化领导小组批准，开展首次全国范围的关键信息基础设施网络安全检查工作 |
| 2016 年 11 月 | 《网络安全法》公布，第三章 网络运行安全 第二节 关键信息基础设施的运行安全：<br>• 第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。<br>• 第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。 |
| 2017 年 7 月 | 国家网信办《关键信息基础设施安全保护条例（征求意见稿）》：<br>• 第十八条 下列单位运行、管理的网络设施和信息系统,一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益的,应当纳入关键信息基础设施保护范围:(一)政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位;(二)电信网、广播电视网、互联网等信息网络,以及提供云计算、大数据和其他大型公共信息网络服务的单位;(三)国防科工、大型装备、化工、食品药品等行业领域科研生产单位;(四)广播电台、电视台、通讯社等新闻单位;(五)其他重点单位。<br>• 第十九条 国家网信部门会同国务院电信主管部门、公安部门等部门制定关键信息基础设施识别指南。国家行业主管或监管部门按照关键信息基础设施识别指南,组织识别本行业、本领域的关键信息基础设施,并按程序报送识别结果。关键信息基础设施识别认定过程中,应当充分发挥有关专家作用,提高关键信息基础设施识别认定的准确性、合理性和科学性。 |
| 2017 年 8 月 | 两部国家标准征求意见稿公布<br>•《信息安全技术 关键信息基础设施安全保障评价指标体系（征求意见稿）》<br>•《信息安全技术 关键信息基础设施安全检查评估指南（征求意见稿）》 |
| 2018 年 6 月 | 两部国家标准征求意见稿公布：<br>•《信息安全技术 关键信息基础设施网络安全保护要求（征求意见稿）》<br>•《信息安全技术 关键信息基础设施安全控制措施（征求意见稿）》 |
| 2019 年 2 月 | 中国人民银行发布《中国人民银行职能配置、内设机构、人员编制规定》，提出中国人民银行的内设机构科技司负责 “拟订金融业信息化发展规划，承担金融标准化组织管理协调工作。指导协调金融业网络安全和信息化建设以及金融业关键信息基础设施建设。编制并推动落实金融科技发展规划，拟订金融科技监管基本规则，指导协调金融科技应用。承担中国人民银行科技管理、信息化规划和建设等工作。”<br>全国信安标委秘书处就在北京组织召开了国家标准《信息安全技术 关键信息基础设施网络安全保护基本要求（报批稿）》的试点工作启动会。本次试点工作在电信、广电、能源、交通、金融、卫生健康等重点行业和领域选取了 12 家单位作为标准应用试点单位。中国电子技术标准化研究院、中国信息安全测评中心、国家信息技术安全研究中心、国家计算机应急技术处理协调中心、公安部第三研究所、公安部第一研究所、国家工业信息安全发展研究中心、中国互联网络信息中心等 8 家标准编制单位作为第三方测评机构。 |

| | |
|---|---|
| 2019 年 12 月 | 国家网信办等十部委发布《网络安全审查办法》。国家网信办相关负责人就《网络安全审查办法》答记者问中表示：根据中央网络安全和信息化委员会《关于关键信息基础设施安全保护工作有关事项的通知》精神，电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等行业领域的重要网络和信息系统运营者在采购网络产品和服务时，应当按照《网络安全审查办法》要求考虑申报网络安全审查。<br>• 第二十条：本办法中关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者。 |
| 2020 年 6 月 | 国务院办公厅《国务院 2020 年立法工作计划》：国务院 2020 年拟制定、修订的行政法规包括《关键信息基础设施安全保护条例》，由网信办、工信部、公安部起草。 |
| 2020 年 7 月 | 公安部发布《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，指出：<br>公安机关指导监督关键信息基础设施安全保护工作。在落实网络安全等级保护制度基础上，突出保护重点，强化保护措施，切实维护关键信息基础设施安全。根据党中央和公安部有关规定，公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的主管、监管部门（以下统称保护工作部门）应制定本行业、本领域关键信息基础设施认定规则并报公安部备案。保护工作部门根据认定规则负责组织认定本行业、本领域关键信息基础设施，及时将认定结果通知相关设施运营者并报公安部。 |
| 2020 年 8 月 | 信安标委公布了两项关于关键信息基础设施的国标文件征求意见稿：<br>•《信息安全技术 关键信息基础设施边界确定方法（征求意见稿）》<br>•《信息安全技术 关键信息基础设施安全防护能力评价方法（征求意见稿）》 |

根据我们对上表中的CII有关动态及规范性文件的研究和分析，我们认为金融机构从业人员需要关注以下要点：

**1.金融机构所运行、管理的网络设施和信息系统一直作为关键信息基础设施监管涉及的重要对象**

从上表我们可以看到，“金融”一直作为重要行业和领域被屡次提及，国家标准《信息安全技术 关键信息基础设施网络安全保护基本要求（报批稿）》试点工作所选取的12家单位亦包含了金融机构。

**2.将可能由央行科技司具体负责金融业的关键信息基础设施识别认定工作**

根据网安法第32条以及今年7月公安部发布《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，我们基本可以明确，将由公安部指导和监督关键信息基础设施的安全保护工作；重要行业和领域的主管、监管部门负责制定本行业、本领域CII认定规则并报公安部备案；主管、监管部门根据CII认定规则识别本行业、本领域的CII，并将认定结果报给公安部并通知CIIO。另根据央行在2019年2月发布的《中国人民银行职能配置、内设机构、人员编制规定》，科技司将负责金融业的CII建设工作。综合来看，金融行业领域内，很可能由央行科技司主要负责金融行业内CII的个认定规则制定与认定工作，并将规则与认定结果报公安部。

**3.《关键信息基础设施安全保护条例》预计今年将会出台**

根据国务院办公厅今年6月份发布的《国务院2020年立法工作计划》，国务院2020年拟制定、修订的行政法规包括《关键信息基础设施安全保护条例》，由网信办、工信部、公安部起草。

**4.关注《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（以下简称“《关保等保指导意见》”）**

根据结合有关文件的解读，我们认为需要明确《关保等保指导意见》传达出的如下信息：

**4.1关键信息基础设施的保护（以下简称“关保”）是在“等保2.0”基础之上实行的重点保护**

根据网安法第31条对于关键信息基础设施“在网络安全等级保护制度的基础上，实行重点保护”，以及《关保等保指导意见》工作目标中提出的“在贯彻落实网络安全等级保护制度的基础上，关键信息基础设施涉及的关键岗位人员管理、供应链安全、数据安全、应急处置等重点安全保护措施得到有效落实，关键信息基础设施安全防护能力明显增强”，我们看出，如果说等保是面向网络运营者的普遍义务，那么关保则是针对CIIO的特殊义务；同样的，等保面向的一般的网络设施和信息系统，关保则是面向承载着重要行业和领域的关键业务的网络设施和信息系统。

**4.2等保与关保的异同点**

另外根据我们对涉及等保有关国家标准与关保有关国家标准的对比梳理，我们认为有以下异同点，可以帮助大家理解等保与关保的关系，以及认识关保：

**4.2.1关保和等保的对象都是网络设施和信息系统，区别在于：**等保面向的一般的网络设施和信息系统，包括：基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）、工业控制系统和采用移动互联技术的系统等；关保则是面向承载着重要行业和领域的关键业务的网络设施和信息系统，《关保和等保指导意见》还特别提出“基础网络、大型专网、核心业务系统、云平台、大数据平台、物联网、工业控制系统、智能制造系统、新型互联网、新兴通讯设施等”应作为重点保护对象纳入CII范围。

**4.2.2义务主体上，等保2.0体系下，网络安全等级保护义务是基础的、普遍适用的，但关保针对重要行业领域。**

义务要求上，关保的要求显然较等保要求更高。

**4.2.3关保和等保范围都将按照认定规则和一定流程、程序来进行识别认定，区别在于：**等保的

认定规则由《GB/T 28448-2019 信息安全技术网络安全等级保护测评要求》等国家标准明确，但关保的认定规则需要由相应行业、领域的主管或监管部门制定，是否公开还不明确。

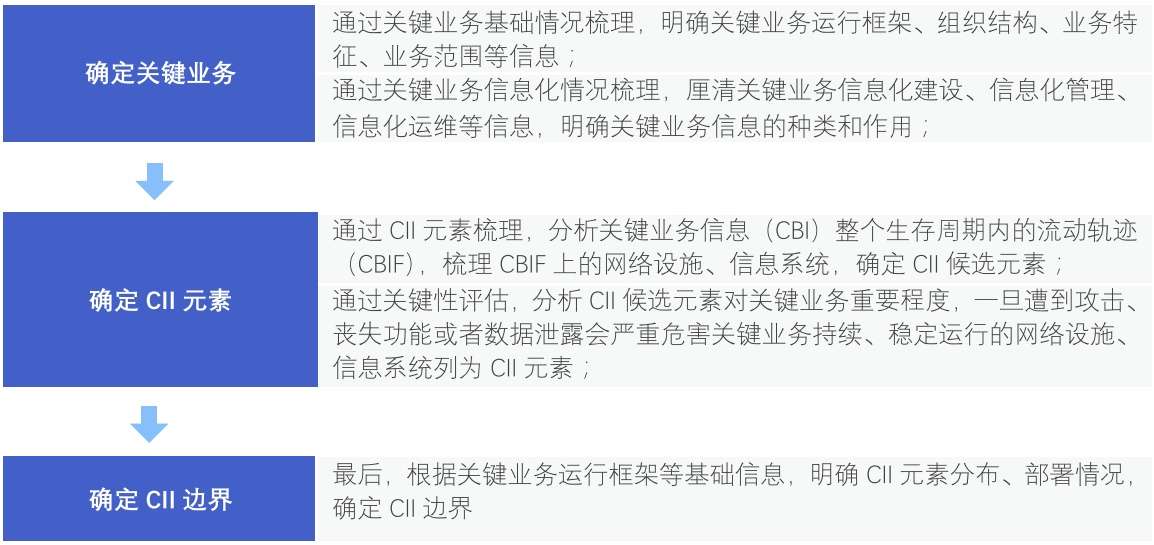
**4.2.4关保和等保范围都将由专门机构来识别认定，区别在于：**等保的测评认定可由公安部认可的测评服务单位提供，但关保的认定将由相应行业、领域的主管或监管部门负责。

**4.2.5等保和关保的指导监督工作都由公安机关负责，区别在于：**等保二级以上的网络运营者只需要至县级以上公安机关备案；但关保的备案是由相应行业领域的主管或监管部门报公安部备案。

**4.2.6保密要求上，我们认为，一般对于通过等保测评认定的评级结果没有保密要求；**但是鉴于CII与国家安全、国计民生、公共利益极为相关，因此，某网络设施和信息系统是否被认定为关键信息基础设施这一信息很可能是保密的。

**5.关注《信息安全技术 关键信息基础设施边界确定方法（征求意见稿）》（以下简称“《边界确定方法》”）**

前不久发布的《边界确定方法》为我们展现了CII边界确定的方法（如下图）。此外，根据该文件，我们也需要关注到，1）由“行业主管部门认定的关键业务”是确定CII边界的前提，以及2）由于关键业务是发展变化的，相应的CII边界也应作出及时调整。



## 客体:个人信息/重要数据

根据网安法第31条至39条,“关键信息基础设施的运营者”(以下简称“CIIO”)在个人信息和重要数据的跨境流动上受到较多限制,以及较一般网络运营者,CIIO对于所持有的关键信息基础设施(以下简称“ CII”)负有更多的安全保护义务,因此对于网络运营者来说,明晰自身是否运营CII意义重大。

### 1.个人信息

关于个人信息的定义和范围,网安法、《GB/T 35273-2020信息安全技术 个人信息安全规范》(以下简称“《个人信息规范》”)都给了较为明确定义,特别是《个人信息规范》,提供了判定某项信息是否属于个人信息的两条参考路径:“一是识别,即从信息到个人,由信息本身的特殊性识别出特定自然人,个人信息应有助于识别出特定个人。二是关联,即从个人到信息,如已知特定自然人,由该特定自然人在其活动中产生的信息(如个人位置信息、个人通话记录、个人浏览记录等)即为个人信息。符合上述两种情形之一的信息,均应判定为个人信息。”此外,《个人信息规范》的附录A给出了个人信息的举例,其中与金融行业较为相关是“个人财产信息”,包括“银行账户、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等,以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息”。

此外,根据我们为金融机构提供数据合规服务的经验,对于《个人信息规范》已列举出的个人信息类型,需要按照关于个人信息保护的有关规定进行收集使用等处理行为,这一点并无太多争议,但对于一些还未明确列举是否是个人信息,比如带有预测成分的个人用户画像,其属性判定就需要依照前述“两条参考路径”以及监管动向进行具体判定。

### 2.重要数据

我们对“重要数据”有关的重要文件梳理如下表:

| | |
|---|---|
| 2017 年 4 月 | 网信办《个人信息和重要数据出境安全评估办法（征求意见稿）》关于重要数据定义：<br>重要数据，是指与国家安全、经济发展，以及社会公共利益密切相关的数据，具体范围参照国家有关标准和重要数据识别指南。 |
| 2017 年 8 月 | 信安标委发布国家标准《信息安全技术 数据出境安全评估指南（征求意见稿）》。<br>◆ 该文件指出，重要数据是指，相关组织、机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：<br>a) 危害国家安全、国防利益，破坏国际关系；<br>b) 损害国家财产、社会公共利益和个人合法利益；<br>c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；<br>d) 影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；<br>e) 干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；<br>f) 危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；<br>g) 影响或危害国家经济秩序和金融安全；<br>h) 可分析出国家秘密或敏感信息；<br>i) 影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。<br>根据上述定义和行业（领域）主管部门相关规定，指南提出了各行业(领域)重要数据的范围。各行业（领域）主管部门应结合实际，明确本行业（领域）重要数据定义、范围或判定依据；并根据行业（领域）发展变化，及时更新或替换本指南中相关内容。<br>◆ 该文件对金融行业重要数据的范围列举如下：<br>A.19 金融<br>主管部门：人民银行。<br>重要数据包括但不限于：<br>A.19.1 金融机构安全信息<br>A.19.2 自然人、法人和其他组织金融信息<br>A.19.3 中央银行、金融监管部门、外汇管理部门工作中产生的不涉及国家秘密的工作秘密。 |
| 2019 年 5 月 | 网信办发布《数据安全管理办法（征求意见稿）》，关于重要数据的定义：<br>重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。 |
| 2020 年 4 月 | 金标委编制的《金融数据安全 数据安全分级指南（送审稿）》发布。 |
| 2020 年 7 月 | 全国人大常委发布《数据安全法（草案）》<br>第十九条 国家根据数据在经济社会发展中的重要程度,以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用,对国家安全、公共利益或者公民、组织合法权益造成的危害程度,对数据实行分级分类保护。 各地区、各部门应当按照国家有关规定,确定本地区、本部门、本行业重要数据保护目录,对列入目录的数据进行重点保护。<br>第二十五条 开展数据活动应当依照法律、行政法规的规定和国家标准的强制性要求,建立健全全流程数据安全管理制度,组织开展数据安全教育培训,采取相应的技术措施和其他必要措施,保障数据安全。重要数据的处理者应当设立数据安全负责人和管理机构,落实数据安全保护责任。<br>第二十八条 重要数据的处理者应当按照规定对其数据活动定期开展风险评估,并向有关主管部门报送风险评估报告。 风险评估报告应当包括本组织掌握的重要数据的种类、数量,收集、存储、加工、使用数据的情况,面临的数据安全风险及其应对措施等。 |
| 2020 年 7 月 | 公安部发布《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，指出：<br>加强重要数据和个人信息保护。(关键信息基础设施）运营者应建立并落实重要数据和个人信息安全保护制度，对关键信息基础设施中的重要网络和数据库进行容灾备份，采取身份鉴别、访问控制、密码保护、安全审计、安全隔离、可信验证等关键技术措施， |

| | |
|---|---|
| | 实保护重要数据全生命周期安全。运营者在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，因业务需要，确需向境外提供的，应当遵守有关规定并进行安全评估。 |
| 2020 年 8 月 | 信安标委发布关于征集《信息安全技术 重要数据识别指南》国家标准的参编单位通知。 |
| 2020 年 8 月 | 信安标委发布《信息安全技术 网络数据处理安全规范（征求意见稿）》，该文件对重要数据做出定义，并对网络运营者关于重要数据的识别、传输和存储、访问控制与审计、向他人提供、删除与匿名化处理提出具体要求。此外提出，“网络运营者向境外提供个人信息或者重要数据的，应遵循国家相关规定和相关标准的要求。"<br>3.6 重要数据<br>一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据，包括未公开的政府信息，数量达到一定规模的基因、地理、矿产信息等，原则上不包括个人信息、企业内部经营管理信息等。 |

根据我们对上表中“重要数据”有关内容的研究和分析，我们认为金融机构从业人员需要关注以下要点：

**2.1关注《金融数据安全 数据安全分级指南（送审稿）》（以下简称“《分级指南》”）**

《分级指南》对于金融行业从业者在进行数据分级以及数据治理较具有参考价值，其结合影响对象、影响程度因素，将金融数据分为1至5级，其中有关重要数据的内容摘录如下表。从中我们认为可以解读出如下几个要点：

**2.1.1重要数据的占比小。**按照《分级指南》对金融数据的分级，重要数据属于其第5级数据，我们认为其在金融机构数据中的占比非常小。

**2.1.2金融业重要数据一旦遭到破坏的影响对象为国家安全和公众权益。**对于国家安全，影响轻微即可能属于重要数据，对于公众权益，需要造成非常严重的影响才可能属于重要数据。按照此种影响对象和影响程度的考量，破坏仅对个人权益或企业权益造成影响的数据，不足以被认定为重要数据。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。

**2.1.3汇聚后的个人数据可能构成重要数据。**《分级指南》附录C对于“海量信息汇聚得到的衍生特征数据”这一重要数据包含的内容描述为：汇聚后覆盖多省市的金融消费者真实交易信息。

**2.1.4重要数据与关键信息基础设施的关系。**根据《分级指南》附录C的表述，我们可归结出两条关系：1）一旦被破坏，将危害关键信息基础设施，属于重要数据；2）关键信息基础设施的网络安全缺陷信息（网络设备、服务器、信息系统等有关漏洞信息）属于重要数据。

| 最低安全级别参考 | 数据定级要素 | | 数据一般特征 |
|---|---|---|---|
| | 影响对象 | 影响程度 | |
| 5 级 | 国家安全 | 非常严重/严重/中等/轻微 | • 重要数据，通常主要用于金融行业大型或特大型机构、金融交易过程中重要核心节点类机构中的关键业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用；<br>• 数据安全性遭到破坏后，影响国家安全，或对公众权益造成非常严重的影响。 |
| 5 级 | 公众权益 | 非常严重 | |

附录 C
重要数据是指我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：
——危害国家安全、国防利益，破坏国际关系；
——损害国家财产、社会公共利益和个人合法利益；
——影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；
——影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；
——干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；
——危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；
——影响或危害国家经济秩序和金融安全；
——可分析出国家秘密或敏感信息；
——影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。
重要数据的内容可包括宏观特征数据、海量信息汇聚得到的衍生特征数据、行业监管机构决策和执法过程中的数据，以及关键信息基础设施网络安全缺陷信息等，如：
——宏观特征：可反映不可更改或长时间保持稳定的经济特征、社会特征的数据；
——海量信息汇聚得到的衍生特征数据：汇聚后覆盖多省市的金融消费者真实交易信息；
——行业监管机构决策和执法过程中的数据：行政机关、执法机关在履职或执法过程中收集和产生的不涉及国家秘密且未公开的受控数据；
——关键信息基础设施网络安全缺陷信息：网络设备、服务器、信息系统等有关漏洞信息。
重要数据一般不包括企业生产经营和内部管理信息、个人信息等。
其中，金融业重要数据通常能够反映与金融机构或政府财政职能范围内的职责、交易或其他方面的相关信息，此类信息包括但不限于金融机构持有的客户信息，如：银行业、保险业及证券期货业各金融机构、非银行支付机构以及为上述机构提供清算服务的特许清算机构在经营过程中收集或产生的数据；金融业机构网络与信息系统规划建设、运行维护、安全保障等数据；中央银行、金融监管部门、外汇管理部门工作中产生的不涉及国家秘密的工作秘密等。

### 2.2对于泄露仅影响到个人权益和企业权益的，一般不认为是重要数据

根据监管部门最新的文件，重要数据一旦泄露，其影响对象是国家安全或公共利益。实际上，监管部门关于重要数据的认定范围经历了一个“窄-宽-窄”的过程（如下表），其中2017年8月网信办采取的标准过于宽泛，目前监管部门已不再采取该种标准。

| 变化 | 文件 | 影响对象 |
| --- | --- | --- |
| 窄 | 2017 年 4 月，网信办《个人信息和重要数据出境安全评估办法（征求意见稿）》 | 国家安全、经济发展，社会公共利益 |
| 宽 | 2017 年 8 月，信安标委发布国家标准《信息安全技术 数据出境安全评估指南（征求意见稿）》 | 国家安全、经济发展，公共利益，个人合法权益，国际关系，司法执法活动，政府行政行为等 |
| 窄 | 2019 年 5 月，网信办发布《数据安全管理办法（征求意见稿）》 | 国家安全、经济安全、社会稳定、公共健康和安全 |
| | 2020 年 8 月信安标委发布《信息安全技术 网络数据处理安全规范（征求意见稿）》 | 国家安全、公共安全、经济安全和社会稳定 |

**2.3关注《数据安全法（草案）》释放的信号**

根据《数据安全法（草案）》第19条、第25条和第28条，我们认为需要关注如下内容：

2.3.1重要数据是在数据分级分类基础上进行的重点保护。

2.3.2不同地区、不同部门、不同行业将分别制定重要数据保护目录。

2.3.3将有配套的关于数据安全的法律、行政法规的规定和国家标准的强制性要求。

2.3.4重要数据的处理者注意需要设立数据安全负责人和管理机构，落实数据安全保护责任。

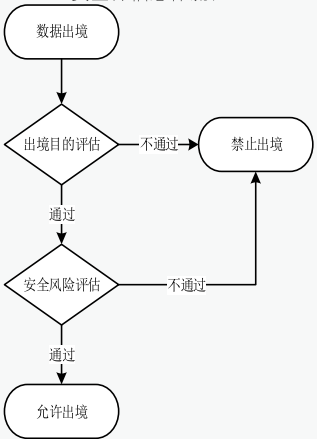
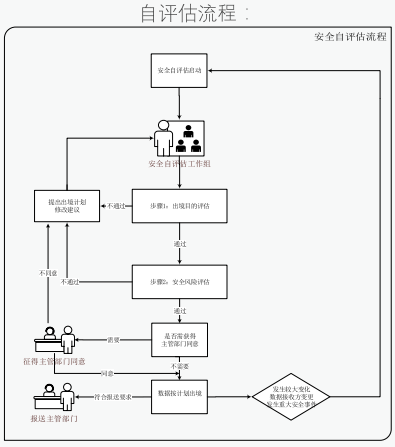
2.3.5重要数据的处理者应当定期开展有关重要数据的风险评估。

**2.4《信息安全技术 重要数据识别指南》关于重要数据的分类标准很可能将不再沿用行业分类的方式**

根据中国信通院安全研究所数据安全研究部副主任陈湉所撰《对《数据安全法》的理解和认识|重要数据如何保护》，我们了解到拟定的《信息安全技术 重要数据识别指南》“简化了重要数据定义、明确提出了重要数据的主要分布；不再延用行业分类的方式，而是从数据的作用、受破坏后可能带来的影响等角度，将重要数据分为国民经济运行类、安保类、自然资源与环境类、健康类、敏感技术类、用户类及政府工作秘密类。”

## 要求：安全评估

我们对数据出境安全评估的有关内容梳理如下表：

| | |
|---|---|
| 2016 年 11 月<br>《网络安全法》 | “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。” |
| 2017 年 4 月<br>网信办《个人信息和重要数据出境安全评估办法（征求意见稿）》 | 第二条 网络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。因业务需要，确需向境外提供的，应当按照本办法进行安全评估。<br>第六条 行业主管或监管部门负责本行业数据出境安全评估工作，定期组织开展本行业数据出境安全检查。<br>第七条 网络运营者应在数据出境前，自行组织对数据出境进行安全评估，并对评估结果负责。<br>第八条 数据出境安全评估应重点评估以下内容：<br>（一）数据出境的必要性；<br>（二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；<br>（三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；<br>（四）数据接收方的安全保护措施、能力和水平，以及所在国家和地区的网络安全环境等；<br>（五）数据出境及再转移后被泄露、毁损、篡改、滥用等风险；<br>（六）数据出境及出境数据汇聚可能对国家安全、社会公共利益、个人合法利益带来的风险；<br>（七）其他需要评估的重要事项。<br>第十条 行业主管或监管部门组织的安全评估，应当于六十个工作日内完成，及时向网络运营者反馈安全评估情况，并报国家网信部门。 |
| 2017 年 8 月<br>信安标委《信息安全技术 数据出境安全评估指南（征求意见稿）》 | 安全评估总体流程：<br>  <br><br>自评估流程：<br>  <br> |

根据上表，关于数据出境的安全评估，2017年出台《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下简称“《2017出境评估办法》”）及其配套的国家标准《信息安全技术 数据出境安全评估指南（征求意见稿）》（以下简称“《2017出境评估指南》”）采取的是“网络运营者自评估+行业主管或监管部门安全评估”的模式，这可作为行业从业者可预期的数据出境的评估模式参考。**但鉴于《2017出境评估办法》和《2017出境评估指南》至今未再修订，其关于重要数据、需要进行数据出境评估的主体范围认定上已与目前监管思路和文件产生较大出入，因此该两份文件关于安全评估的义务主体层面的内容还需谨慎对待。**

## 《网络安全法》数据跨境规制体系小结

根据对网安法监管体系下数据出境的分析我们可以看出，首先，在主体上，关键信息基础设施及其运营者的认定存在一个过程，尽管金融机构被认定为CIIO的可能性较大，但并不意味着其持有的所有网络设施和信息系统都将被认定为CII，且今年公安部的指导监督下CII的识别认定工作应当会较之前有较大进展；其次，在客体层面，关于个人信息的范围认定趋于明确；关于重要数据的范围认定上还需等待相关文件出台，但其影响对象应当为“国家安全”和“公众权益”这一方向逐渐明确，也即意味着“重要数据”并不会在一个企业的数据比例中占比非常大。再次，对于数据出境评估所需要依据安全评估办法，还有待相关文件出台。

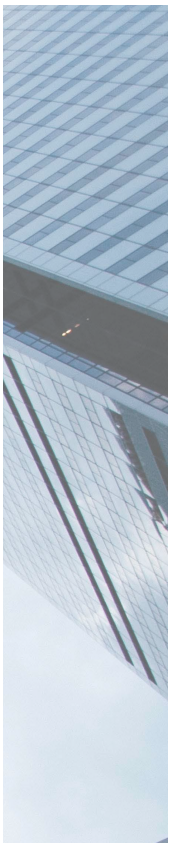
# 结语

通过对“金融行业监管部门数据跨境规制”和“《网络安全法》数据跨境规制”两个监管体系有关规范性文件的梳理和要点提示我们可以看到：

**金融行业监管这条线下，数据跨境流动监管要求主要是控制与“人”有关的数据信息及业务运营或处理系统，主要处理的是金融行业有关主体因跨境开展业务产生的数据跨境传输需求与将控制金融数据跨境传输所带来的风险之间的矛盾，**监管要求散布于多部文件之中较为庞杂，但相对明确，便于金融行业从业者把握。其中特别需要提示的是，应当密切关注央行《个人金融信息（数据）保护试行办法》或类似文件的出台，将很有可能涉及个人金融信息的出境规制。

**网安法监管这条线下，数据跨境流动监管要求主要是控制CIIO的个人信息和重要数据，主要处理的是不限于金融行业在内的重要领域、行业的数据跨境传输需求与控制数据跨境传输给国家安全、社会公共利益所带来的风险之间的矛盾，**涉及的规范性文件不多，但具体要求还都有待关保工作的开展和有关文件的出台来进一步的明确。

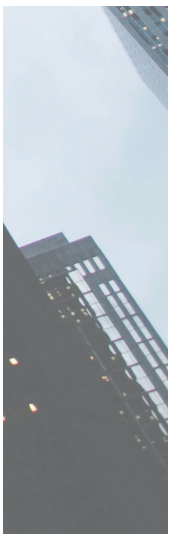
此外，我们也发现了这两条线之间的连接点，也是殊途同归之处，都在于“数据出境安全评估制度”。根据网安法第37条，CIIO的个人信息和重要数据出境将有赖于“国家网信部门会同国务院有关部门制定的办法进行安全评估。根据金融行业标准《JR/T0171-2020个人金融信息保护技术规范》，金融机构应依据



国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估。但截至目前安全评估的依据和流程都还不清晰。

对于金融行业从业者来说，两条线各有侧重、互为补充，虽然法定义务有待细化和统一，但脉络已经显现，两条线都需要保持关注。

最后，从跨境数据流动的监管政策体系变化能看到，我国监管机构的立场与时俱进，根据技术发展和金融业务的实际需求而不断调整。从一开始“一刀切”地限制数据出境，后来逐渐有条件地允许合规流动，到现在形成一套较为完整的体系来规范引导，体现了创新监管、分层监管、精准监管的演进历程。由此，监管政策一方面服务好了跨境金融的市场需求，另一方面也满足了跨境监管合作的要求。未来，金融跨境数据的流动一定会持续完善，我们将继续保持密切关注。



## 参考文章


1.上海市法学会江翔宇课题组《金融数据跨境流动立法与监管的比较研究报告》

2.马兰《金融数据跨境流动规制的核心问题和中国因应》，载《国际法研究》2020年第3期

3.袁立志 冯坚坚《银行业金融数据出境的监管框架与脉络》

4.李伟《我国金融数据跨境流动规则建设的思考与建议》

# 附录

## 相关规范性文件

1.《个人存款账户实名制规定》国务院2000.3.20发布

2.《人民币银行结算账户管理办法》中国人民银行2003.4.10发布

3.《个人信用信息基础数据库管理暂行办法》中国人民银行2005.8.18发布

4.《电子银行业务管理办法》中国银行业监督管理委员会2006.1.26发布

5.《反洗钱法》全国人民代表大会常务委员会2006.10.31发布

6.《金融机构反洗钱规定》中国人民银行2006.11.14发布

7.《中国人民银行关于证券期货业和保险业金融机构严格执行反洗钱规定防范洗钱风险的通知》中国人民银行2007.1.30发布

8.《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》中国人民银行2011.1.21发布

9.《关于银行业金融机构做好个人金融信息保护工作有关问题的通知》中国人民银行上海分行2011.5.12发布

10.《关于调整证券资格会计师事务所申请条件的通知》财政部、中国证券监督管理委员会2012.1.21发布

11.《支付机构反洗钱和反恐怖融资管理办法》中国人民银行2012.3.5发布

12.《保险公司财会工作规范》中国保险监督管理委员会2012.7.1发布

13.《征信业管理条例》国务院2013.1.21发布

14.《非银行支付机构网络支付业务管理办法》中国人民银行2015.12.28发布

15.《网络借贷信息中介机构业务活动管理暂行办法》中国银行业监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室2016.8.17发布

16.《网络安全法》全国人民代表大会常务委员会2016.11.7发布

17.《个人信息和重要数据出境安全评估办法（征求意见稿）》国家互联网信息办公室2017.4.11发布

18.《关键信息基础设施安全保护条例（征求意见稿）》国家互联网信息办公室2017.7.10发布

19.《信息安全技术 关键信息基础设施安全保障评价指标体系（征求意见稿）》全国信息安全标准化技术委员会2017.8.30发布

20.《信息安全技术 关键信息基础设施安全检查评估指南（征求意见稿）》全国信息安全标准化技术委员会2017.8.30发布

21.《信息安全技术 数据出境安全评估指南（征求意见稿）》全国信息安全标准化技术委员会2017.8.30发布

22.《信息安全技术 关键信息基础设施网络安全保护要求（征求意见稿）》全国信息安全标准化技术委员会2018.6.11发布

23.《信息安全技术 关键信息基础设施安全控制措施（征求意见稿）》全国信息安全标准化技术委员会2018.6.11发布

24.《中国银行业监督管理委员会中资商业银行行政许可事项实施办法》中国银行保险业监督管理委员会2018.8.17修订

25.《外商投资期货公司管理办法》中国证券监督管理委员会2018.8.24发布

26.《互联网金融从业机构反洗钱和反恐怖融资管理办法（试行）》中国人民银行、中国银行保险业监督管理委员会、中国证券监督管理委员会2018.10.10发布

27.《银行业金融机构反洗钱和反恐怖融资管理办法》中国银行保险业监督管理委员会2019.1.29发布

28.《中国人民银行职能配置、内设机构、人员编制规定》中国人民银行2019.2.2发布

29.《数据安全管理办法（征求意见稿）》国家互联网信息办公室2019.5.28发布

30.《信用评级业管理暂行办法》中国人民银行、国家发展和改革委员会、财政部、中国证券监督管理委员会2019.11.26发布

31.《中国中国银行保险业监督管理委员会外资银行行政许可事项实施办法》中国银行保险业监督管理委员会2019.12.26发布

32.《信息安全技术 关键信息基础设施网络安全保护基本要求（报批稿）》全国信息安全标准化技术委员会发布

33.《信用评级业管理暂行办法》中国人民银行、国家发展和改革委员会、财政部、中国证券监督管理委员会2019.11.26发布

34.《证券法》全国人民代表大会常务委员会2019.12.18修订

35.《个人金融信息（数据）保护试行办法（初稿）》

36.《JR/T0171-2020个人金融信息保护技术规范》中国人民银行2020.2.13发布

37.《GB/T 35273-2020信息安全技术 个人信息安全规范》国家标准管理委员会2020.3.6发布

38.《网络安全审查办法》国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局2020.4.13发布

39.《金融数据安全 数据安全分级指南（送审稿）》金融标准化技术委员会2020.4.13发布

40.《国务院2020年立法工作计划》国务院办公厅2020.6.26发布

41.《数据安全法（草案）》全国人民代表大会常务委员会2020.7.3发布

42.《信息安全技术 关键信息基础设施边界确定方法（征求意见稿）》全国信息安全标准化技术委员会2020.8.10发布

43.《信息安全技术 关键信息基础设施安全防护能力评价方法（征求意见稿）》全国信息安全标准化技术委员会2020.8.10发布

44.《信息安全技术 网络数据处理安全规范（征求意见稿）》全国信息安全标准化技术委员会2020.8.28发布

45.《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2020.9.15发布

# 关于我们 ABOUT US

## 观韬中茂律师事务所

观韬中茂律师事务所成立于1994年2月，是总部设于中国北京的专业化、综合性大型律师事务所。经过与创设于上世纪五十年代的香港王泽长·周淑娴·周永健律师行，以及创建于上世纪九十年代的上海市中茂律师事务所、上海市申达律师事务所的合并，观韬中茂现拥有800余名律师、200余位合伙人，在法律服务、专业建设和律师团队等方面已成为中国优秀律师事务所之一。

王渝伟律师数据合规团队是观韬中茂律师事务所专注网络安全、数据隐私合规法律服务的专业团队，在大数据、人工智能、互联网、金融科技、云计算、物联网等领域拥有为头部企业提供涉及复杂技术与商业场景项目提供全面数据合规服务的丰富经验和卓越能力。

## 金融科技·微洞察

“金融科技·微洞察”是微众银行运营的金融科技研究品牌，聚焦国内外金融科技领域的技术发展、标准制定及产业应用，把握当下金融科技热点话题与政策动向，洞察未来领先的金融形态和商业模式。

微众银行作为国内首家互联网银行，自2014年成立之初即将“科技、普惠、连接”作为银行的三大发展愿景，将积极运用科技创新探索普惠金融新模式、新业态作为银行重要的发展方向，致力于为普罗大众、微小企业提供差异化、有特色、优质便捷的金融服务。自立行至今，微众银行在金融科技“ABCD”（人工智能、区块链、云计算、大数据）等四大领域积极探索，2017年即已成为国内首家获评“国家级高新技术企业”的商业银行，截至2019年末共申请国家及国际专利数超过1000余件，拥有自身所有重要业务和技术系统的知识产权，有效实现了银行业信息化安全可控的战略目标。

## 金链盟

深圳市金融区块链发展促进会（简称“金链盟”）成立于2016年5月，由微众银行、腾讯、深圳市金融科技协会、深证通等二十余家金融机构和科技企业共同发起，2019年11月正式注册为社会团体法人。至今，金链盟成员已涵

括银行、证券、基金、保险、地方股权交易所、科技公司等六大类行业的150余家单位，成为国内最大的区块链组织和最具国际影响力的区块链联盟之一。

金链盟开源工作组于2017年推出了安全可控、稳定易用、高性能的金融级区块链底层平台——FISCO BCOS（Be Credible, Open & Secure）。该平台获得了2018年度深圳金融科技创新专项奖一等奖，并于2019年入选成为国家级区块链服务网络（BSN）中的首个国产联盟链底层平台。目前，FISCO BCOS开源生态圈已汇聚了上万名个人开发者、超1000家机构与企业，在政务、金融、公益、版权、供应链、教育等不同领域已有80余个落地应用，发展成为最大最活跃的国产开源联盟链生态圈。

## 免责声明

## 联合出品

观韬中茂律师事务所 Guantao Law Firm　WeBank 微众银行　金融科技 微洞察　FISCO 金链盟

## 报告出品人

王渝伟　姚辉亚

## 报告作者

陈坤　徐磊

## 美术编辑

邓少雁

## 联络邮箱

wangyw@guantao.com　weinsights@webank.com

观韬中茂律师事务所

金融科技·微洞察