汉坤法律评述

2020 年 10 月 14 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

央行发布金融数据安全分级指南

作者：杨铁成 | 葛音 | 郑婷 | 乔梦晶

2020 年 9 月 23 日，中国人民银行（“**央行**”）发布了《金融数据安全 数据安全分级指南（JR/T 0197-2020）》（“**《金融数据分级指南》**”）。在《中华人民共和国网络安全法》（“**《网络安全法》**”）以及其它现行数据保护监管规定的基础上，《金融数据分级指南》对金融业机构的数据分级工作提出了更为系统化和具体化的要求。本文将从企业合规角度解读《金融数据分级指南》要点，并重点关注《金融数据分级指南》在现行法规及标准基础上提出的新要求。

一、“数据分类分级”的背景和原则——*发布《金融数据分级指南》的目的是什么？*

“数据分类分级”一直是网络安全和数据保护领域的重要监管原则之一。2016 年，《网络安全法》对网络运营者提出了一系列安全保护义务，其中涵盖了数据分类分级要求。根据《网络安全法》第 21 条的规定，企业作为网络运营者，应当采取数据分类以及其它安全保护措施，以防止数据被泄露、窃取或篡改。此外，2020 年 7 月 3 日，全国人大常委会发布了《中华人民共和国数据安全法（草案）》，提出了在国家层面建立全面的数据保护体系，并在其中明确了对数据实行分级分类保护的要求。

另外，监管机构还发布了一系列征求意见稿，明确了数据分类分级的合规要求，例如：《网络安全等级保护条例（征求意见稿）》、《数据安全管理办法（征求意见稿）》、《关键信息基础设施安全保护条例（征求意见稿）》、《信息安全技术 数据安全分类分级实施指南（草案）》等。与此同时，监管机构针对工业等不同行业也制定了各自领域的数据分类分级指南。

在金融领域，“数据分类分级”也是金融监管机构的监管重点之一。2018 年 9 月，中国证券监督管理委员会发布了《证券期货业数据分类分级指引（JR/T 0158-2018）》（“**《证券期货业数据分类分级指引》**”），在金融领域首次提出数据分类分级的要求。但是，《证券期货业数据分类分级指引》的适用范围仅涵盖证券公司、期货公司和基金管理公司。

2020 年 2 月 13 日，央行与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）》（“**《个人金融信息规范》**”）。《个人金融信息规范》延续了“数据分级分类”的监管思路，将个人金融信息按照其敏感程度分为 C3、C2 和 C1 三类。我们在此前发布的汉坤法律评述中对《个人金融信息规范》进行了详细解析，参见*《个人金融信息保护技术规范》重点解析*。

随着金融技术和数字经济的发展，金融数据呈现出巨大的社会和商业价值，同时其复杂程度也日益加深。在此背景下，央行发布了《金融数据分级指南》，旨在为金融机构的数据分级工作提供详细可行的指引，有助于金融机构更进一步明确数据保护对象，合理分配数据安全保护的资源和成本，并进一步建立完善金融数据生命周期管理框架。

二、“金融业机构”范围的变化——*《金融数据分级指南》的适用范围是什么？*

《金融数据分级指南》将其适用范围界定为从事《国民经济行业分类（GB/T 4754-2017）》中所述金融业的相关机构（统称“**金融业机构**”）。

《证券期货业数据分类分级指引》仅适用于证券公司、期货公司及基金管理公司。与之相比，《金融数据分级指南》的适用范围则扩大至其它类型的金融机构，例如商业银行、保险公司以及信托公司等。《金融数据分级指南》也适用于私募基金管理人（包括 PFM、QDLP 和 QDIE 等机构）、第三方支付公司、征信机构等。此外，由于行业间关联性以及监管机构对于适用范围的解释可能存在一定灵活性，《金融数据分级指南》有可能间接影响到从事数据安全评估的机构，例如第三方数据评估机构等。

值得注意的是，尽管《金融数据分级指南》和《个人金融信息规范》从字面内容上看都适用于“金融业机构”，但上述两项标准在“金融业机构”的定义上存在一定区别。根据《个人金融信息规范》，“金融业机构”包括“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”，这就意味着《个人金融信息规范》不仅直接适用于广义的持牌金融机构，包括银行业金融机构、证券公司、基金管理公司、保险公司，同时也直接适用于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、征信机构等。此外，虽然 PFM/QDLP 等私募基金管理人不属于严格意义上的“持牌金融机构”，但如果其在提供金融服务的过程中处理了任何客户的个人信息，也应被视作“涉及个人金融信息处理的相关机构”，从而应当遵守《个人金融信息规范》。

我们在下表中对《个人金融信息规范》、《证券期货业数据分类分级指引》及《金融数据分级指南》对不同类型机构的适用情况进行了总结：

<table>
<tr><th>机构类型</th><th>《个人金融信息规范》</th><th>《证券期货业数据分类分级指引》</th><th>《金融数据分级指南》</th></tr>
<tr><td>持牌的证券期货业机构
（即证券公司、期货公司以及基金管理公司）</td><td rowspan="5">√
（适用于相关机构所处理的“个人金融信息”）</td><td>√</td><td>可选择适用
（数据分级工作可参照《证券期货业数据分类分级指引》执行）</td></tr>
<tr><td>其它持牌金融机构
（包括商业银行、保险公司以及信托公司等）</td><td rowspan="4">×</td><td rowspan="4">√
（适用于相关机构的“金融数据”）</td></tr>
<tr><td>私募基金管理人
（包括 PFM、QDLP 和 QDIE 等机构）</td></tr>
<tr><td>第三方支付公司</td></tr>
<tr><td>征信机构</td></tr>
</table>

需要指出的是，本次发布的《金融数据分级指南》是金融行业推荐性标准，而非强制性标准。尽管《金融数据分级指南》作为推荐性标准不具有强制约束力，在具体适用上保留了一定空间，但推荐性标准在实践中可被此后发布的强制性规定所引用或涵盖。另外，我们不排除金融监管机构在开展监督检查或执法活动时可能将其作为重要参考，将《金融数据分级指南》视为金融业机构在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照《金融数据分级指南》中的相关标准与要求，以在最大程度上规避与金融数据分级相关的任何法律或合规风险。

三、“金融数据”的范围——*数据安全定级包含哪些金融数据？*

《金融数据分级指南》注重对金融业机构在开展业务活动、提供金融服务以及日常经营管理时采集或生成的“电子数据”进行分级。《金融数据分级指南》所涉及的金融数据包括但不限于以下四类：

第一类：向客户提供金融产品或服务的过程中直接（或间接）采集的电子数据；

第二类：金融业机构信息系统内生成和/或存储的电子数据，包括业务数据、交易信息、经营管理数据等；

第三类：金融业机构内部办公网络中产生、交换、归档的电子数据，如机构内部日常事务处理信息、内部通知、电子邮件信息等；以及

第四类：金融业机构原纸质文件经过扫描或其它电子化手段形成的电子数据。

值得注意的是，涉及国家秘密的数据不适用于《金融数据分级指南》，而应依据有关机关制定的有关保守国家秘密的法律法规处理，例如《中华人民共和国保守国家秘密法》、《中华人民共和国保守国家秘密法实施条例》、《国家秘密定密管理暂行规定》等。

四、金融数据分级保护的标准——*如何对金融数据进行定级？*

与《证券期货业数据分类分级指引》类似，《金融数据分级指南》建立了多级数据分类体系，以“影响对象”和“影响程度”为主要定级要素。根据《金融数据分级指南》，金融业机构应通过评估数据安全性遭受破坏后的“影响对象”和“影响程度”，将金融数据按重要性由高到低分为 5 级、4 级、3 级、2 级和 1 级。

其中，“影响对象”包括国家安全、公众权益、个人隐私、企业合法权益等。“影响程度”分为“严重损害”、“一般损害”、“轻微损害”和“无损害”。金融业机构在进行数据分级时可参照下表：

最低安全级别参考	数据定级要素		数据一般特征与示例
	影响对象	影响程度	
5	国家安全	严重损害/一般损害/轻微损害	■ 金融业机构的“重要数据”； ■ 用于金融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的关键业务；以及 ■ 针对特定人员公开，且仅为必须知悉的对
	公众权益	严重损害	

最低安全级别参考	数据定级要素		数据一般特征与示例
	影响对象	影响程度	
			象访问或使用。
4	公众权益	一般损害	■ 用于金融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的重要业务； ■ 针对特定人员公开，且仅为必须知悉的对象访问或使用；以及 ■ **个人金融信息中的 C3 类信息**。
	个人隐私	严重损害	
	企业合法权益	严重损害	
3	公众权益	轻微损害	■ 用于金融业机构关键或重要业务； ■ 针对特定人员公开，且仅为必须知悉的对象访问或使用；以及 ■ **个人金融信息中的 C2 类信息**。
	个人隐私	一般损害	
	企业合法权益	一般损害	
2	个人隐私	轻微损害	■ 用于金融业机构一般业务； ■ 针对受限对象公开，通常用于内部管理；以及 ■ **个人金融信息中的 C1 类信息**。
	企业合法权益	轻微损害	
1	国家安全	无损害	■ 可被公开或被公众获知；以及 ■ 个人金融信息主体主动公开的信息。
	公众权益	无损害	
	个人隐私	无损害	
	企业合法权益	无损害	

值得注意的是，《金融数据分级指南》附录 A（《*数据定级规则参考表*》）进一步全面总结了数据样例及其相对应的数据安全级别。《金融数据分级指南》中也进一步描述了详细的评估标准。

五、金融数据定级流程——*金融业机构如何进行数据定级？*

根据《金融数据分级指南》中规定的定级流程，金融业机构应自行在机构内部判定和批准数据安全分级。《金融数据分级指南》规定了数据安全定级的内部流程，包括以下五个步骤：

第 1 步（数据资产梳理）
■ 对电子数据进行盘点、梳理与分类 ■ 形成统一的数据资产清单
↓
第 2 步（数据安全定级准备）
■ 明确数据定级颗粒度 ■ 识别数据安全定级关键要素
↓

第 3 步（数据安全级别判定）
■ 数据安全级别评定 ■ 根据定级形成不同安全级别的数据清单
↓
第 4 步（数据安全级别审核）
■ 审核数据安全评定过程及结果
↓
第 5 步（数据安全级别批准）
■ 由数据安全管理最高决策组织对数据安全级别评定结果进行批准

根据《金融数据分级指南》，金融业机构应确定其数据安全管理最高决策组织，例如，在机构内设立数据安全管理委员会等。此外，金融业机构应明确组织架构，清晰划分相关部门以及人员的角色和职责。目前，数据安全级别评定结果无需监管部门批准。

六、数据保护要求——*金融业机构应承担何种金融数据保护义务？*

根据《金融数据分级指南》，金融业机构应将其金融数据按重要性由高到低分为 5 级、4 级、3 级、2 级和 1 级。《个人金融信息规范》将个人金融信息按照其敏感程度分为 C3、C2 和 C1 类信息。尽管《金融数据分级指南》并未直接对金融业机构规定数据保护要求，但值得注意的是，《金融数据分级指南》明确了其与《个人金融信息规范》的关联性，即：

1. 《个人金融信息规范》中的 C3 类信息应与《金融数据分级指南》中的 4 级数据相对应；
2. C2 类信息应与 3 级数据对应；以及
3. C1 类信息应与 2 级数据对应。

鉴于此，金融业机构在将数据按照 1 级至 5 级进行判定时，应参照遵守《个人金融信息规范》中相应的数据保护要求，如：

1. 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 类信息应采取加密等技术措施，防止被未经授权第三方获取；
2. 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；
3. 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；
4. 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）；
5. 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
6. 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。

七、展望——*我们对监管趋势有何预期？*

相较于现行法律法规而言，《金融数据分级指南》更具实用性，对金融业机构的合规实践有着重要的指导作用，为金融业数据保护规范化和数据生命周期管理奠定了基础。我们预期央行等金融监管机构可能在未来就此制定和发布详细的实施细则。

此外，尽管《金融数据分级指南》填补了金融数据分级分类管理方面的空白，标志着数据保护规则的进一步完善，但《金融数据分级指南》仍为金融监管部门后续的规则制定保留了一定的空间。例如，虽然金融业机构应将其金融数据分为 5 级、4 级、3 级、2 级和 1 级，但《金融数据分级指南》并没有对每一级金融数据提出数据保护要求，相关要求可能会在后续出台的监管规则或国家/行业标准中得到进一步明确。

随着数据生命周期管理和个人信息保护监管框架的不断发展，我们也将持续关注相关监管要求的更新，并及时与各位读者分享我们的观点。

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：

杨铁成

Tel: +86 10 8516 4286
Email: tiecheng.yang@hankunlaw.com

葛音

Tel: +86 21 6080 0966
Email: yin.ge@hankunlaw.com