HANKUN
汉坤律师事务所
Han Kun Law Offices

汉坤专递

2020 年第 10 期（总第 162 期）

新法评述

1、央行发布金融数据安全分级指南

2、《个人信息保护法（草案）》浅析

新法评述

1、央行发布金融数据安全分级指南

作者：杨铁成丨葛音丨郑婷丨乔梦晶

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：

<table>
<tr><th rowspan="2">最低安全级别参考</th><th colspan="2">数据定级要素</th><th rowspan="2">数据一般特征与示例</th></tr>
<tr><th>影响对象</th><th>影响程度</th></tr>
<tr><td rowspan="2">5</td><td>国家安全</td><td>严重损害/一般损害/轻微损害</td><td rowspan="2">■ 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象访问或使用。</td></tr>
<tr><td>公众权益</td><td>严重损害</td></tr>
<tr><td rowspan="3">4</td><td>公众权益</td><td>一般损害</td><td rowspan="3">■ 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</td></tr>
<tr><td>个人隐私</td><td>严重损害</td></tr>
<tr><td>企业合法权益</td><td>严重损害</td></tr>
</table>

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	
			■ 个人金融信息中的 C3 类信息。
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。

2、《个人信息保护法（草案）》浅析

作者：段志超丨蔡克蒙丨胡敏喆

2020 年 10 月 21 日，全国人大常委会正式全文发布经常委会一审审议的《个人信息保护法（草案）》[1]（**“草案”**）。我国首部个人信息保护专项立法正式亮相。

草案在顺应加强个人信息保护趋势的同时，在具体内容上体现了鲜明的特点，意图全面系统地建设具有中国特色的个人信息保护基本制度。一方面，其继承和发展了《民法典》、《网络安全法》勾勒出的个人信息保护框架，丰富了相关内容，保持了立法的延续性。另一方面，其在个人信息定义、域外效力、处罚力度（罚金可能高达五千万或年度营业额 5%）以及个人信息处理的法律基础等方面，又开放性地借鉴了包括 GDPR 在内的域外主流数据立法，在现有法律法规的基础上实现了突破。此外，立法机关显然听取了互联网、人工智能、数字化营销等大数据行业的具体需求，在诸如个人数据跨境制度设计、数据处理的合法基础以及个人权利适用限制等方面较此前若干相关法规草案进行了更针对性且更具可操作性的设计，为促进数据的有效流转和开发提供了保障。

一、识别+关联：扩展的个人信息定义

草案第四条将个人信息界定为“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”。这一定义在《网络安全法》《民法典》以“识别”为核心界定个人信息的基础上，进一步加入了“关联”标准。

- “识别”强调“从信息到人”。这里的“识别”并不要求可以确定某一个体的自然身份，而只要通过特定信息在特定群体中确定某一个体即可视为“识别”。例如企业仅掌握设备识别号码，而不掌握手机号码、姓名、身份证号等实名信息，无法确定用户真实身份，但由于设备识别号码具有唯一性，可在用户群体中确定唯一个体，因此仍属于个人信息。
- 与已识别或者可识别的自然人“有关”的各种信息，体现了新增的“关联”标准。关联强调“人到信息”，即与已知特定个体有关的信息。例如体现其活动或爱好等的信息，这些信息可能不具有唯一性或识别性，但仍应视为个人信息。

在比较法视野中，欧盟通用数据保护条例（GDPR）等域外立法[2]多采纳“识别+关联标准”界定个人信息，我国《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》、《个人信息安全规范》等在实践中常用的操作性规范亦多纳入“关联”标准。草案吸取了这些有益经验，将“关联”标准正式纳入法律层面，将有助于更为全面、充分地保护个人信息。

草案个人信息定义的另一亮点是将“匿名化”后的信息排除出个人信息的范畴。草案区分了“匿名化”，指“个人信息经过处理无法识别特定自然人且不能复原的过程”和“去标识化”，指“个人信息经过

[1] http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80808175265dd401754405c03f154c。

[2] GDPR 第 2 条：“Personal data means any information relating to an identified or identifiable natural person (‘data subject’)”。近期立法中，泰国规定，“Personal Data” means any information relating to a Person, which enables the identification of a Person, whether directly or indirectly, but does not include the information of deceased Persons；印度规定，“Personal Data” means “any information that relates to a natural person which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person”。

处理，使其在不借助额外信息的情况下无法识别特定自然人的过程”。前者通常是统计意义上的信息，已经丧失了个体“颗粒度”；后者通常是对标识符进行删除和变换。然而，具体某项经处理的信息是否能够达到匿名化的程度，进而不再受到草案的保护，还是仅仅属于去标识化信息，仍应遵守草案的要求，需结合相关国家标准在个案中进行判断。

二、域外效力：跨境场景下的长臂管辖

此前，《网络安全法》等法律法规主要将适用范围限定在境内网络运营者。但在实践中，许多境外运营者未在境内设立运营主体，但通过跨境服务直接收集中国境内自然人的个人信息，在此情况下是否仍需遵守中国个人信息保护相关法律法规常存在争议。

草案第三条则弥补了上述缺陷，第三条第二款规定“以向境内自然人提供产品或者服务为目的，或者为分析、评估境内自然人的行为等发生在我国境外的处理我国境内自然人个人信息的活动，也适用本法”。该条的规定与 GDPR 第 3 条第 2 款所规定的域外适用所确立的“指向（targeting）”与“监控（monitoring）”标准颇为类似。参考 GDPR 相关的解释及我国发布的《信息安全技术 数据出境安全评估指南（征求意见稿）》，境外运营者如使用中文、以人民币作为结算货币、向中国境内配送物流、向中国境内用户开展定向营销或推广，或对中国境内自然人进行画像分析均可能落入草案第三条第二款规定的适用范围。

草案第五十二条进一步规定了境外个人信息处理者应在境内设立专门机构或者指定代表，专门负责个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。草案尚未明确机构或代表的具体要求或需要承担的法律责任。此外，草案还规定，境外组织、个人损害中国公民个人信息权益或中国国家安全的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

三、个人信息处理者和受托方：委托处理关系下尚待明晰的边界

与《民法典》相似，草案并未像欧盟 GDPR 一样区分个人信息控制者和处理者，而是统一使用“个人信息处理者”这一概念，将其界定为“自主决定处理目的、处理方式等个人信息处理事项的组织、个人。”

草案尽管不存在“控制者与处理者”的区分，但仍然对个人信息的“委托处理关系”做出了专门的规定，主要包括：

- 委托方应当与受托方约定委托处理的目的、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托方的个人信息处理活动进行监督；
- 受托方应当按照约定处理个人信息，不得超出约定的处理目的、处理方式等处理个人信息，并应当在合同履行完毕或者委托关系解除后，将个人信息返还个人信息处理者或者予以删除；
- 未经个人信息处理者同意，受托方不得转委托他人处理个人信息。

从表面上看，草案中“个人信息处理者”的定义与 GDPR 项下的“控制者”的概念较为接近，而受托方与 GDPR 项下的“处理者”类似，但能否将这两组概念等同仍存在疑问。例如第五十条规定的安全保证义务、第五十五条的个人信息泄露补救措施、第六十条的约谈、第六十五条的损害赔偿责任等规定，如将适用范围单纯限制在决定“处理目的、处理方式”的个人信息处理者（类似于 GDPR 项下的“控制者”），而不包含受托处理个人信息的“处理者”，似会导致保护不周之嫌。另外，在许多通常可以被理解为“委托处理”的关系中，受托一方在许多情况下也会对“处理目的、处理方式”具有较大的决定权，此时受托方应被

视为共同处理者还是受托方可能仍需在个案中进行分析和判断。

四、个人信息处理法律基础：“同意”不再是唯一路径

《网络安全法》将信息主体“同意”作为个人信息处理的唯一合法性基础。这一规定在当时的背景下无疑有助于彰显个人的主体地位，限制对个人信息的窃取、贩卖或隐秘收集等明显侵犯个人信息的行为。但是，随着国内个人信息保护实践的发展，无差别地要求企业获得用户同意已经难以满足日益复杂多样的个人信息处理场景，容易导致“同意”在实践中流于形式。《民法典》虽首次在立法层面规定了“同意的例外”，但范围仅包括处理已经公开的信息以及维护公共利益或者自然人合法权益。《个人信息安全规范》等国家标准规定了更多的无需获得同意的例外情形，并通过区分基本业务功能与扩展业务功能提出了差异化的同意要求，对破解“强迫同意”、“捆绑同意”提供了有益的指引。但由于标准的效力层级较低，无法突破上位法要求，因此企业在合规实践中面临着诸多不确定性。

为了解决上述现实问题，草案首次在信息主体同意之外增加了其他个人信息处理的合法基础，包括：

- 为订立或者履行个人作为一方当事人的合同所必需；
- 为履行法定职责或者法定义务所必需；
- 为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；
- 为公共利益实施新闻报道、舆论监督等行为在合理的范围内处理个人信息；以及
- 法律、行政法规规定的其他情形等。

我们认为，草案规定的更加丰富的个人信息处理法律基础，能够为个人信息处理者提供更加多样的选择，有助于解决同意僵化、滥用及在特定场景下不具有可操作性等问题，使同意更加真实、有效和有针对性，提升信息主体对其个人信息的控制力。

五、“告知—同意”：基于场景的差异化要求和信息主体的选择权

增加其他个人信息处理的法律基础并不意味着同意不再重要。相反，草案在汲取《App 违法违规收集使用个人信息行为认定方法》、《个人信息安全规范》等法规规范和监管实践经验的基础上，细化了“告知-同意”的要求，保障信息主体可以在充分知情的情况下对同意特定个人信息处理活动作出有效选择。草案在“告知-同意”方面的主要规定如下：

- **告知内容：**告知内容主要包括个人信息处理者的身份和联系方式；个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；个人行使本法规定权利的方式和程序等；
- **告知的例外：**（1）法律、行政法规规定的保密情形，或者（2）紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的情形，可以不向个人进行告知。但在后一种情况下应当在紧急情况消除后予以告知；
- **知情同意：**处理个人信息应当在事先充分告知的前提下取得个人同意，如果法律、行政法规规定应当取得个人单独同意或者书面同意的，从其规定；
- **二次利用重新取得同意：**处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意；

- **不得强制同意**：不得以个人不同意处理其个人信息或者撤回其对个人信息处理的同意为由，拒绝提供产品或者服务；
- **撤回同意**：基于个人同意而进行的个人信息处理活动，个人有权撤回同意；
- **合并分立**：因合并、分立等原因需要转移个人信息的，需要向个人告知接收方的身份、联系方式。接收方变更原先的处理目的或处理方式，应当重新告知并获得用户同意；
- **向第三方提供**：向第三方提供个人信息的，应当向个人告知第三方的身份、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；
- **处理已经公开的信息**：应当符合个人信息被公开时的用途，超出与该用途相关的合理范围的，应当重新获得同意。在公开用途的判断上，个人信息处理者承担合理、谨慎的处理义务。

六、敏感个人信息处理：非必要不可为

草案首次在法律层面提出了“个人敏感信息”的概念，即“一旦泄露或者非法使用，可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息，包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息”。草案设专节对敏感个人信息的处理活动提出了更高的保护要求：

- 个人信息处理者处理敏感个人信息，应当具有特定的目的和充分的必要性；
- 处理敏感个人信息，除一般告知事项外，还应当向个人告知处理敏感个人信息的特殊目的、必要性以及对个人的影响；
- 基于个人同意处理敏感个人信息的，个人信息处理者应当取得个人的单独同意；
- 法律、行政法规规定处理敏感个人信息应当取得相关行政许可或者作出更严格限制的，从其规定；
- 个人信息处理者应当在处理敏感个人信息前进行风险评估，并对处理情况进行记录。

此外，针对公共场所图像这类可能涉及个人行踪、生物特征信息等个人敏感信息，且在实践中经常被滥用的信息，草案规定在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。收集的个人图像、个人身份特征信息只能用于维护公共安全的目的，不得公开或者向他人提供收集的个人信息。

七、个人权利：知情和控制

草案将信息主体权利单独成章，以彰显其重要性。草案规定，在个人信息处理活动中，个人享有知情权、决定权、限制权、拒绝权、查询权、复制权、更正权、删除权、解释权、自动化决策反对权。这部分的亮点主要包括：

- 草案首次提出限制权和拒绝权，有权限制或者拒绝他人对其个人信息进行处理，但法律、行政法规另有规定的除外；
- 草案细化了删除权的适用条件，包括：（1）约定的保存期限已届满或者处理目的已实现；（2）个人信息处理者停止提供产品或者服务；（3）个人撤回同意；（4）个人信息处理者违反法律、行政法规或者违反约定处理个人信息；（5）法律、行政法规规定的其他情形。但是，法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者应当停止处理个人信息；

- 草案首次提出了解释权，即个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

针对实践中争议极大的个性化推荐、“大数据杀熟”等基于画像的商业营销，草案明确“自动化决策”是指利用个人信息对个人的行为习惯、兴趣爱好或者经济、健康、信用状况等，通过计算机程序自动分析、评估并进行决策的活动。草案对“自动化决策”活动作出了如下规定：

- 利用个人信息进行自动化决策，应当保证决策的透明度和处理结果的公平合理；
- 个人认为自动化决策对其权益造成重大影响的，有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定；
- 通过自动化决策方式进行商业营销、信息推送，应当同时提供不针对个人特征的选项。

当前实践中，大多数企业尚未建立完备的个人信息权利实现机制，因此草案的相关规定如付诸实施无疑将对企业个人信息保护提出巨大挑战。然而，草案对大多数个人信息权利的行使条件、时限、能否收费、实现方式等未作具体规定，仍有待监管机关在实践中通过解释和执法活动加以明确。

八、数据跨境合规：差异化考量下的多元路径

草案中最受跨国企业关注的当属个人信息的跨境流动制度。对此，草案依据个人信息出境对国家安全可能带来的不同风险，作出了差异化的制度安排。

- 对于关键信息基础设施运营者，草案沿用了《网络安全法》的规定，要求关键信息基础设施运营者确需向境外提供个人信息的，应当通过国家网信部门组织的安全评估；
- 处理个人信息达到国家网信部门规定数量的个人信息处理者，与关键信息基础设施运营者等同处理，同样需要在个人信息出境前通过国家网信部门组织的安全评估。类似要求此前公布的《个人信息和重要数据出境安全评估办法》等法规征求意见稿即有体现，应该说并不意外；
- 其他一般情况下，个人信息处理者因业务等需要而向境外提供个人信息的，可以选择不同的出境机制，包括（1）通过国家网信部门组织的安全评估；（2）经专业机构进行个人信息保护认证；（3）与境外接收方订立合同，约定双方的权利和义务，并监督其个人信息处理活动达到本法规定的个人信息保护标准；或（4）法律、行政法规或者国家网信部门规定的其他条件。相比于《个人信息出境安全评估办法（征求意见稿）》等征求意见稿要求所有运营者事先向监管部门申请安全评估的要求，草案的规定提供了更为便利和多样的选择；
- 草案明确，在“国际司法协助或行政执法协助”中需要向境外传输个人信息时，需要依法申请有关主管部门批准，对一些国家根据国内法强行调取域外数据做出了回应，彰显了捍卫国家主权的立场。

总体而言，我们认为对于一般的个人信息出境，相较于统一要求事先评估，草案提出的多元化个人信息出境机制与国际主流更为接轨，有助于在保护国家安全和个人信息安全的前提下，降低个人信息出境成本，推动数据有序流转与利用，预期将会得到业界的肯定与欢迎。

九、公权力适用：规范和节制

草案首次明确了国家机关处理个人信息的基本要求，设立专节对国家机关处理个人信息提出了如下要求：

- **职责必要性：**国家机关为履行法定职责处理个人信息的，应当依照法律或者行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度；
- **告知同意及其例外：**原则上，国家机关处理个人信息也应当履行告知同意的法律要求；但法律、行政法规规定应当保密，或者告知、取得同意将妨碍国家机关履行法定职责的除外；
- **禁止公开或对外提供：**除法律、行政法规另有规定或者取得个人同意外，国家机关不得公开或者向他人提供其处理的个人信息；
- **数据本地化：**针对国家机关处理的个人信息，草案明确要求国家机关应当将相关个人信息存储在我国境内。确需向境外提供的，应当进行风险评估并可以要求有关部门提供支持与协助。

草案的上述规定有助于遏制公权力机关过度收集、滥用个人信息的行为，规范国家机关处理公民个人信息的权限和程序，在当前许多公权力机关以防疫名义过度收集个人信息的背景下尤显重要。我们期待未来在更为具体的法律法规中，细化国家机关处理个人信息的具体规则，保障公民的合法权益。

十、处罚和救济：高额罚金和公益诉讼

草案大幅度提高了对违法行为的处罚力度，规定企业违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施的，履行个人信息保护职责的部门可能责令企业改正违法行为，没收违法所得，给予警告。企业拒不改正的，可能被处以一百万元以下的罚款，情节严重的，还有可能面临五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。同时，直接负责的主管人员和其他直接责任人员也可能面临一万元以上一百万元以下的罚款。

此外，针对实践中个人在侵犯个人信息诉讼中获赔过低，缺乏诉讼动力的情况，草案规定个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、履行个人信息保护职责的部门和国家网信部门确定的组织可以依法向人民法院提起诉讼。这一规定为检察机关、消费者权益保护组织等提起个人信息公益诉讼提供了明确的依据。

十一、总结与展望

总体而言，我们认为草案充分地借鉴了当前各国各地区个人信息保护立法的先进经验，吸收了近几年来我国个人信息保护执法活动中的有益成果，有效回应了实践中个人信息保护面临的重点和难点问题，平衡了个人信息保护、个人信息的利用与流转、国家安全和社会公众利益等多方面利益。草案的出台将为个人信息权益保护和数字经济发展提供有力保障。

对于国内企业而言，虽然近年来不少国内企业个人信息保护合规水平显著提高，但相较草案而言，企业在分场景落实告知同意要求、信息主体权利保护、个人信息保护风险评估、个人信息跨境流转等方面仍普遍存在较大的差距。

对于跨国公司而言，虽然不少企业已建立了较为完备的 GDPR 等域外法合规机制，但这些机制在国内落地程度有限，且即使落地亦无法全面满足草案在上述方面的特殊要求。对此，我们建议企业应抓住草案公布后至正式生效前的窗口期，借此机会全面对照梳理既有的个人信息保护工作现状，系统排查合规风险，及时调整合规方案，弥补差距和短板，尽快提升公司的个人信息保护水平，降低面临行政处罚、民事赔偿乃至刑事处罚的风险。

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