HANKUN
汉坤律师事务所
Han Kun Law Offices

汉坤专递

2022 年第 9 期（总第 185 期）

新法评述

1、简评《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》

2、申报要求落地 — 国家网信办发布《数据出境安全评估申报指南（第一版）》

新法评述

1、简评《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》

作者：段志超丨蔡克蒙丨金今

一、概述

2022 年 9 月 14 日，国家互联网信息办公室发布《关于修改〈中华人民共和国网络安全法〉的决定（征求意见稿）》（**“《征求意见稿》”**）。《征求意见稿》主要加重了《网络安全法》项下违法行为的法律责任，对违反网络运行安全义务、违反网络信息安全义务、违反关键信息基础设施安全保护义务及违反个人信息保护义务的罚则在体系上进行整合统一，并与《个人信息保护法》（**“《个保法》”**）、《数据安全法》等新法衔接协调。我们将在下文对《征求意见稿》体现的修订要点予以梳理、总结。

二、加重违反网络运行安全义务的法律责任

《征求意见稿》对未履行网络安全等级保护制度要求的安全保护义务、未制定实施网络安全事件应急预案、未对产品服务提供持续安全维护等违反网络运行安全一般规定的法律责任进行了整合统一，并补充了违反《网络安全法》第二十三条“网络关键设备和网络安全专用产品强制性认证检测要求”的罚则。而尤其值得关注的是，此次修订对统一后的法律责任在整体上进行加重。《征求意见稿》呼应《个保法》第六十六条的规定，将罚款上限抬高至五千万元或者上一年度营业额的百分之五，对直接责任人员的罚款上限也抬高至一百万元，同时增加了对其禁止任职的规定。

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
《网络安全法》第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（四）采取数据分类、重要数据备份和加密等措施；（五）法律、行政法规规定的其他义务。	**【未履行网络运行安全义务的法律责任】** 由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。	**【违反网络安全保护义务的法律责任】** 由有关主管部门责令改正，给予警告、通报批评；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节特别严重的，由省级以上有关主管部门责令改正，处

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
《网络安全法》第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。		**一百万元以上五千万元以下或者上一年度营业额百分之五以下罚款**，并可以责令停止相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处**十万元以上一百万元以下罚款**，并可以**决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作**。
《网络安全法》第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。	**【关键信息基础设施运营者未履行网络运行安全义务的法律责任】** 由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。	
《网络安全法》第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；（二）定期对从业人员进行网络安全教育、技术培训和技能考核；（三）对重要系统和数据库进行容灾备份；（四）制定网络安全事件应急预案，并定期进行演练；（五）法律、行政法规规定的其他义务。		
《网络安全法》第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。		
《网络安全法》第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。		
《网络安全法》第二十二条第一款、第二款 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网	**【未履行网络产品和服务安全义务的法律责任】** 由有关主管部门责令改正，给予	

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。 网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。	警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。	
~~《网络安全法》第四十八条第一款 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。~~		
《网络安全法》第二十四条第一款 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。	**【违反用户身份管理规定的法律责任】** 由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	
《网络安全法》第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。	**【违法开展网络安全服务活动的法律责任】** 由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。	
《网络安全法》第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格	未规定罚则	

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。		
《网络安全法》第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。	**【拒绝支持协助维护国家安全及侦查犯罪的法律责任】** 由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款。	
《网络安全法》第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。	**【实施危害网络安全行为的法律责任】** 尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。 单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。	**【导致危害网络运行安全后果的法律责任】** 尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。 单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。 违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。
《网络安全法》第四十六条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不	**【利用网络从事与违法犯罪相关的活动的法律责任】** 尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重	

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。	的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。 单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。	

三、侵犯个人信息权利法律责任衔接《个保法》

《个保法》于 2021 年 11 月 1 日生效，在此之前对侵犯个人信息权利进行的处罚主要以《网络安全法》为依据。《个保法》生效之后，《网络安全法》中与个人信息保护相关的罚则内容需与《个保法》协调一致，以避免出现适用上的矛盾冲突。《征求意见稿》将侵犯个人信息权利的罚则改为指向《个保法》及其他法律、行政法规的转致性条款，一方面在体系上衔接新法，另一方面相比于原有罚则，在实质上加重了网络运营者侵犯个人信息权利的法律责任。

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
《网络安全法》第二十二条第三款 网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。	**【侵犯个人信息权利的法律责任】** 由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。	**【侵犯个人信息权利的法律责任】** **依照有关法律、行政法规的规定处罚。**
《网络安全法》第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。 网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。		
《网络安全法》第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识		

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
别特定个人且不能复原的除外。 网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。		
《网络安全法》第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。		
《网络安全法》第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。	**【侵犯个人信息权利的法律责任】** 尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。	

四、加重关键信息基础设施安全保护法律责任

对于违反关键信息基础设施采购国家安全审查规定的法律责任，《征求意见稿》同样将罚金上限抬高至上一年度营业额的百分之五。对于违反关键信息基础设施数据境内存储和对外提供规定的法律责任，《征求意见稿》引入转致性条款，指向《数据安全法》第四十六条及《个保法》第六十六条，相比原有罚则均规定了更重的法律责任。

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
《网络安全法》第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。	**【违反关键信息基础设施采购国家安全审查规定的法律责任】** 由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	**【违反关键信息基础设施采购国家安全审查规定的法律责任】** 由有关主管部门责令停止使用，处采购金额一倍以上十倍以下或者**上一年度营业额百分之五以下罚款**，对直接负责的主管人员和其他直接责任人员处一万元以上十万

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
		元以下罚款。
《网络安全法》第三十七条 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。	**【违反关键信息基础设施数据境内存储和对外提供规定的法律责任】** 由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	**【违反关键信息基础设施数据境内存储和对外提供规定的法律责任】** **依照有关法律、行政法规的规定处罚**。

五、完善网络信息安全法律责任体系

《征求意见稿》对违反用户信息治理、安全管理、建立网络信息安全投诉举报制度等网络信息安全义务的法律责任进行了整合，统一将处罚上限调整至五千万元或上一年度营业额的百分之五，同时添加了对于直接责任人员的从业禁止规定。

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
《网络安全法》第四十八条第一款 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。	**【设置恶意程序的法律责任】** 由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。	**【违反网络信息安全保护义务的法律责任】** 由有关主管部门责令改正，给予警告、通报批评，没收违法所得；拒不改正或者情节严重的，处一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处**一百万元以上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
《网络安全法》第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。	**【未履行信息安全管理义务的法律责任】** 由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	
《网络安全法》第四十八条第二款 电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措		

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
施，保存有关记录，并向有关主管部门报告。		务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处**十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。**
《网络安全法》第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。 网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。	**【网络运营者阻碍执法的法律责任】** 由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款。	
《网络安全法》第十二条第二款 任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。	**【发布传输违法信息的法律责任】** 依照有关法律、行政法规的规定处罚。	**【发布传输违法信息的法律责任】** 依照有关法律、行政法规的规定处罚。 法律、行政法规没有规定的，由有关主管部门责令改正，给予警告、通报批评，没收违法所得；拒不改正或者情节严重的，处**一百万元以下罚款**，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 情节特别严重的，由省级以上有关主管部门责令改正，没收违法所得，处**一百万元以上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、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员**处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的**

关联条文	原《网络安全法》罚则	《征求意见稿》罚则
		董事、监事、高级管理人员或者从事网络安全管理和网络运营关键岗位的工作。

六、结语

《征求意见稿》的核心在于加重《网络安全法》项下的违法责任，将罚款上限与个人责任均拉齐至与《个保法》一致，体现了国家对于维护网络安全的强势态度。此次修订尚处于征求意见阶段，距离正式生效仍有一段时间，从事网络运营的相关主体应积极履行网络运行安全、网络信息安全、个人信息保护义务，并对立法动态予以持续关注。

2、申报要求落地 — 国家网信办发布《数据出境安全评估申报指南（第一版）》

作者：段志超丨蔡克蒙丨徐紫寰丨张子谦

2022 年 8 月 31 日，国家互联网信息办公室（“**网信办**”）发布了《数据出境安全评估申报指南（第一版）》（“**《申报指南》**”）。《申报指南》进一步细化和落实了《数据出境安全评估办法》（“**《评估办法》**”）中有关数据出境安全评估（“**安全评估**”）的相关规定，并进一步阐明了安全评估的适用范围、申报方式及流程、申报材料，公开了申报咨询的联系方式，并提供了包括《数据出境安全评估申报书》、《数据出境风险自评估报告（模板）》在内的文件模板，为数据处理者规范、有序申报数据出境安全评估提供了指导和帮助。

在*往期文章*中，我们已经对《评估办法》的要点做出介绍，本文将在此基础上，简析《申报指南》中明确的新要求，并提示安全评估申报中需要重点关注的事项。

一、重申安全评估的适用范围

对于必须申报安全评估的情形，《申报指南》重申了《评估办法》第 4 条的规定[1]，并在此基础上进一步明确了数据出境行为的判断标准：

- 数据处理者将在境内运营中收集和产生的数据传输、存储至境外；
- 数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以**查询、调取、下载、导出**；
- **国家网信办规定的其他数据出境行为**。

与 2022 年 7 月 7 日网信办有关负责人在《评估办法》答记者问[2]中的介绍相比，《申报指南》将第二种出境场景中“境外的机构、组织或者个人可以访问或者调用”更新为“境外的机构、组织或者个人可以查询、调取、下载、导出”，进一步细化说明了远程访问的具体表现形式。

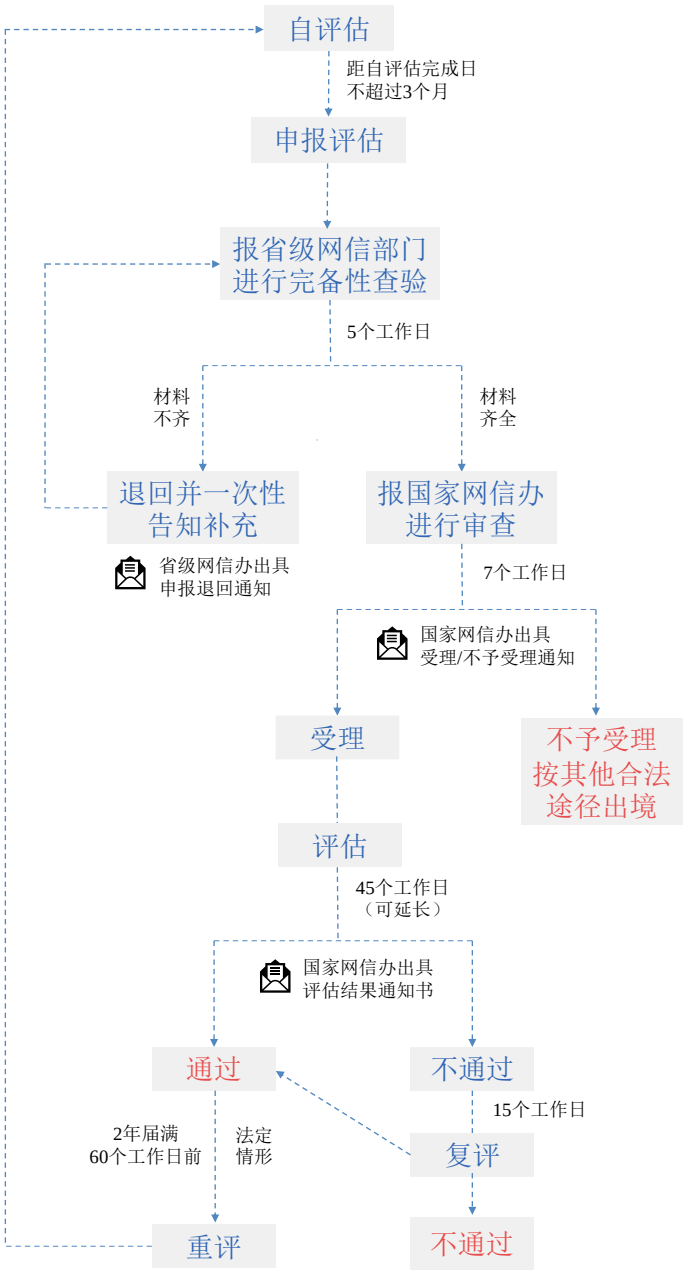
值得关注的是，《申报指南》新增了“国家网信办规定的其他数据出境行为”这一兜底性条款，为监管机构日后应对复杂的数据出境场景预留出解释空间。然而，对于此前备受关注的境外直接收集场景，即境外主体直接从境内个人信息主体处收集其个人信息，《申报指南》并没有直接做出规定，建议相关企业持续密切关注监管动态，及时采取相应的合规措施。

二、细化申报方式及流程

《申报指南》在《评估办法》第 7 条和第 11-13 条的基础上，对申报方式和流程做出了更明确和具体的规定，相关流程图和要点如下：

[1] 《评估办法》第 4 条：“数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：（一）数据处理者向境外提供重要数据；（二）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；（三）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者向境外提供个人信息；（四）国家网信部门规定的其他需要申报数据出境安全评估的情形。”

[2] 2022 年 7 月 7 日，《数据出境安全评估办法》答记者问，具体内容请见：http://www.cac.gov.cn/2022-07/07/c_1658811536800962.htm（最后访问时间：2022 年 9 月 1 日）。



（一）自评估须在申报之日前 3 个月内完成

在《申报指南》提供的申报材料模板中，《承诺书》和《数据出境风险自评估报告（模板）》明确要求自评估工作应当在安全评估申报之日前 3 个月内完成，且至申报之日未发生重大变化。

（二）申报方式明确为线下

根据《申报指南》，数据处理者申报安全评估应当向所在地省级网信办送达书面申报材料并附带材料电子版。其中，材料电子版需通过光盘方式提交。

（三）申报流程中包含三个“通知”

在《评估办法》的基础上，《申报指南》明确指出在三个申报重要节点，数据处理者可能收到的通知文件，包括：

- 未通过完备性查验时：由省级网信办向数据处理者出具申报退回通知；
- 受理审查结束时：由国家网信办书面通知数据处理者是否受理；
- 安全评估结束时：由国家网信办向数据处理者出具评估结果通知书。对于无异议的数据处理者，其应按照数据出境安全管理相关法律法规和评估结果通知书的有关要求，规范相关数据出境活动；对于有异议的数据处理者，收到评估结果通知书将成为《评估办法》第 13 条规定的 15 个工作日异议期的起算标志。

此外，对于正式启动安全评估后的评估期限，《评估办法》第 12 条将其规定为 45 个工作日，情况复杂或者需要补充、更正材料的情况下安全评估还可能被进一步延长。但考虑到《评估办法》规定必须申报安全评估的门槛较低，且 6 个月的整改宽限期时间有限，可以预见短期内申报安全评估的案件量会比较大，不排除监管机构在开展安全评估时对于一部分行业相对不敏感、数据出境行为必要性高、出境数据字段相对不敏感的案件不进行实质审查，从而在相对较短的时间内允许相关数据出境。

（四）申报咨询窗口开放

《申报指南》公布了安全评估申报咨询的联系方式，为企业于实践中解决申报问题提供了明确的渠道：

- 电子邮箱：sjcj@cac.gov.cn；
- 联系电话：010-55627135。

截至本文发布之日，北京市网信办已经开通数据出境安全评估申报咨询电话（010-67676912），后续各省级网信办可能将陆续发布申报咨询的联系方式，建议企业持续关注监管机构的公示信息。

三、明确申报材料具体要求

与《评估办法》第 6 条相比，《申报指南》进一步细化了数据处理者申报安全评估时应当提交的申报材料，并同时提供了相应模板，具体包括：

- 统一社会信用代码证件影印件；
- 法定代表人身份证件影印件；
- 经办人身份证件影印件；
- 经办人授权委托书；
- 数据出境安全评估申报书，其中包括承诺书、数据出境安全评估申报表；
- 与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件影印件；
- 数据出境风险自评估报告；
- 其他相关证明材料。

对于前述材料，有以下值得关注的要点：

（一）首次提出安全评估申报的“经办人”要求

《申报指南》首次明确了安全评估申报过程中的“经办人”角色要求。根据《申报指南》附件中的《经办人授权委托书》、《数据出境安全评估申报书（模板）》，“经办人”应由数据处理者单位的员工担任，并经数据处理者授权。“经办人”的职责为代表数据处理者开展安全评估申报工作，包括填写数据出境安全评估申报书等。

（二）数据发送方与接收方均应配有数据安全负责人员和相关管理机构

根据《申报指南》附件中的《数据出境安全评估申报书（模板）》，申报安全评估时，数据处理者应当在申报表中填写其数据安全负责人和管理机构的信息，以及境外接收方数据安全责任人和管理机构情况。

对于数据处理者的数据安全负责人和管理机构要求，《数据安全法》第 27 条和《个人信息保护法》第 52 条、《关键信息基础设施安全条例》第 14 条此前已分别对重要数据处理者、个人信息处理者、关键信息基础设施运营者做出规定，此外《信息安全技术 个人信息安全规范》（GB/T35273-2020）进一步明确了判断是否需要设立个人信息保护负责人和个人信息保护工作机构的标准[3]。《申报指南》在前述法律和国家标准的基础上，将设立数据安全负责人和管理机构的合规义务扩展至所有申报安全评估的数据处理者。换言之，即使拟申报安全评估的数据处理者处理个人信息未达前述标准，申报安全评估前仍需配有数据安全负责人和管理机构。

此外值得关注的是，申报安全评估时还需填写境外接收方数据安全责任人和管理机构情况。企业因采购境外数据处理服务而涉及安全评估申报的，应在供应商选用环节重视其数据安全保护人员和组织配备情况，并考虑在相关采购合同中要求供应商确保设有相关责任人和管理机构，以满足安全评估要求。

（三）重要数据和个人信息出境可以一并申报

《申报指南》附件中数据出境安全评估申报表“09 拟出境数据情况”栏中可以同时填写重要数据和个人信息出境情况，且《数据出境安全评估申报书（模板）》的“拟出境数据情况”部分不再明确区分重要数据和个人信息，这似表明同一数据出境场景下、向同一境外接收方提供重要数据和个人信息可以合并申报。然而，对于跨国企业关注的同一出境场景下、向集团内不同境外接收方提供数据的情形，《申报指南》并未做明确说明，有待于监管后续在实践中予以明晰。

（四）明确《评估办法》中的“法律文件”概念

《评估办法》第 8 条[4]将“数据处理者与境外接收方拟订立的法律文件”列为安全评估的重点评估内容之一，但未对“法律文件”这一概念做出明确定义。《申报指南》对此明确将其解释为“数据出境

[3] 《数据安全法》第 27 条：“重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。”《个人信息保护法》第 52 条：“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应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。”《关键信息基础设施安全条例》第 14 条：“运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。”《信息安全技术 个人信息安全规范》（GB/T35273-2020）11.1 规定：“满足以下条件之一的组织，应设立专职的个人信息保护负责人和个人信息保护工作机构，负责个人信息安全工作：（1）主要业务涉及个人信息处理，且从业人员规模大于 200 人；（2）处理超过 100 万人的个人信息，或预计在 12 个月内处理超过 100 万人的个人信息；（3）处理超过 10 万人的个人敏感信息的。”

[4] 《评估办法》第 8 条：“数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务……”

相关合同或者其他具有法律效力的文件”。

《申报指南》要求数据处理者在数据出境安全评估申报表中，按照《评估办法》第 9 条[5]对法律文件的规定，逐一填写必备内容的对应条款。鉴于安全评估对法律文件的严格要求，建议企业在准备相关合同时参考或使用网信办发布的个人信息出境标准合同模板，或确保在其他法律文件（如接收方的单方承诺函或境内外所在各方集团数据安全管理制度或政策）中严格按照《评估办法》的要求设置相关条款，以符合安全评估要求。

此外，《申报指南》明确说明法律文件应以中文版本为准，若仅有非中文版本，须同步提交准确的中文译本。

（五）关注数据处理者遵守中国法律、行政法规、部门规章情况

根据《申报指南》，申报安全评估时，数据处理者应在数据出境安全评估申报表中填写“遵守中国法律、行政法规、部门规章情况”。具体而言，数据处理者应介绍简述近 2 年在业务经营活动中受到行政处罚和有关主管监管部门调查及整改情况，重点说明数据和网络安全方面相关情况。

四、发布数据出境风险自评估报告模板

根据《评估办法》第 5 条[6]，数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估。同时根据第 6 条的规定，向主管部门申报数据出境安全评估时需提交数据出境风险自评估报告（“**自评估报告**”）。因此，申报企业所提交的自评估报告将成为监管机构在开展安全评估时重要的评估对象。本次《申报指南》附件 4 为拟申报安全评估并开展风险自评估的企业提供了自评估报告模板，并在其中对企业应当提供的事实材料以及开展的评估维度予以明确，为拟申报企业的风险自评估工作提供了重要参考。

（一）自评估报告的提交要求

数据处理者在向省级网信办申报数据出境安全评估时需一并提交填写完整且内容真实的自评估报告。应当注意的是，《评估指南》要求，如果企业在开展自评估工作时有第三方机构参与，则需要在自评估报告中说明第三方机构的基本情况及参与评估的情况，并在相关内容页上加盖第三方机构公章。根据《评估指南》的整体要求，我们理解“第三方机构的基本情况”可能包括第三方机构名称、性质、主营业务情况、注册地与办公地等。“参与评估的情况”则可能包括第三方机构在企业自评估活动中参与的工作以及发挥的作用。

---

[5] 《评估办法》第 9 条：“数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，至少包括以下内容：（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。”

[6] 《评估办法》第 5 条：“数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；（二）出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；（六）其他可能影响数据出境安全的事项。”

（二）自评估报告的整体内容及新增要求

自评估报告的整体分为自评估工作简述、出境活动整体情况、拟出境活动的风险评估情况、出境活动风险自评估结论四部分。

自评估报告第一部分主要简述自评估工作的开展情况，包括起止时间、组织情况、实施过程、实施方式等。我们理解，若存在第三方机构参与自评估工作，也可以在此部分一并披露。第二部分主要侧重于对数据处理者业务和数据出境事实情况进行梳理，包括数据处理者基本情况、数据出境设计业务和信息系统情况、拟出境数据情况、数据处理者数据安全保障能力情况、境外接收方情况、法律文件约定数据安全保护责任义务情况，以及数据处理者认为需要说明的其他情况，其中“法律文件约定数据安全保护责任义务情况”延续了《评估办法》第 9 条关于数据安全保护责任义务的要求。值得注意的是，自评估报告第二部分（即出境活动整体情况）对数据出境事实梳理的范围进行了扩张，具体而言新增的内容包括：

- 除数据出境活动所涉及的事实外，还需填写数据处理者除公开工商信息外的其他基本情况，包括股权结构和实际控制人信息、组织架构信息、数据安全管理机构信息、整体业务与数据情况、境内外投资情况；
- 需全面梳理出境活动可能涉及的设施的基本情况，包括数据出境涉及业务的数据资产情况、境内外信息系统情况、境内外数据中心（包含云服务）情况、数据出境链路情况（如链路提供商、链路数量与带宽等）；
- 要求披露数据出境后向境外其他接收方提供的情况；
- 在数据处理者安全保障能力方面，自评估报告在《信息安全技术 数据出境安全评估指南（征求意见稿）》的基础上进一步要求数据处理者说明其内部数据分类分级以及风险评估制度建设情况，以及遵守数据和网络安全相关法律法规的情况；
- 在境外接收方情况方面，新增对“境外接收方处理数据的全流程过程描述”的要求，即需说明在境外接收方从境内收集数据后使用、存储、对外提供、删除数据的全生命周期过程。

自评估报告第三部分基本重申了《评估办法》第 5 条关于数据出境风险评估维度的要求，为数据处理者在第二部分事实梳理基础上进行风险评估提供依据，同时其新增对“评估发现的问题和风险隐患以及相应采取的整改措施及整改效果”进行重点说明的要求，因此数据处理者除对拟出境活动进行风险评估外，还需披露其为降低风险而采取的整改措施及整改效果。

五、我们的观点

《评估办法》的生效意味着企业数据出境活动合规整改正式进入倒计时，《申报指南》的出台为拟申报数据出境安全评估的企业提供了具体指引。基于《评估办法》和《申报指南》，企业可考虑从如下方面开展数据出境合规工作，以降低风险：

- 梳理数据处理活动中涉及的数据出境场景以及相应事实情况，判断是否落入需申报安全评估的范畴，并相应选择数据出境策略（如完全本地化存储数据或按照规定准备数据出境安全评估的申报工作）；
- 以《申报指南》自评估报告模板第二部分为基础尽快开展自评估工作，并于自评估期间对发现的风

险及时采取整改措施，以便在《评估办法》的 6 个月宽限期内顺利完成安全评估；

- 按照《申报指南》的要求准备相关申报材料（包括统一社会信用代码证件影印件、法定代表人身份证件影印件、经办人身份证件影印件、经办人授权委托书、数据出境安全评估申报书，其中包括承诺书、数据出境安全评估申报表、与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件影印件、数据出境风险自评估报告、其他相关证明材料）并向省级网信部门递交材料；
- 建立关于数据出境评估的合规内部制度，持续对数据出境情况进行监测，并在发生需要重新申报安全评估的情形时更新相关材料内容重新申报评估。

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

海口　朱俊　律师：

电话：　+86 898 3665 5000

Email：　jun.zhu@hankunlaw.com

武汉　马姣　律师：

电话：　+86 27 5937 6200

Email：　jiao.ma@hankunlaw.com

香港　陈达飞　律师：

电话：　+852 2820 5616

Email：　dafei.chen@hankunlaw.com