THE US-CHINA BUSINESS COUNCIL
美 中 贸 易 全 国 委 员 会

美中贸易全国委员会关于《网络数据安全管理条例（征求意见稿）》的反馈意见

2021 年 12 月 13 日

美中贸易全国委员会（下称“我委员会”）谨代表 260 余家会员企业,感谢有此机会就《网络数据安全管理条例（征求意见稿）》（下称“意见稿”）提出意见。意见稿是《中华人民共和国数据安全法》《中华人民共和国网络安全法》和《中华人民共和国个人信息保护法》的重要施行办法。我委员会充分肯定意见稿在澄清法规、解释要求方面的重要性。设立强有力的网络安全和隐私保护标准，澄清现有法规内容，出台与现行法规相适应的新规，都是有利于减轻企业合规负担的积极举措。

但是，本意见稿中的部分内容已经远超出上述三部现行法律《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》的范围，可能导致非预期后果。这种不一致性集中体现在三个方面：扩大了重要数据的定义，混同个人隐私和网络安全，模糊了中国当前几大网络安全制度之间的差异。

管辖范围扩大，与现行法律的要求不一致：当前意见稿第三十五条对于跨境数据传输安全评估的要求与《个人信息保护法》中的要求重复，还将审查对象扩大到了所有数据，这种监管范围的扩大将会对数据流动造成比较大的影响。而且，意见稿在定义和审查方法上也与《个人信息保护法》中的规定不同。我委员会建议缩小第三十五条的适用范畴，比如规定“出境安全评估、认证、订立标准合同”适用于重要数据、或者由关键信息基础设施运营者处理的数据。我们还建议比照欧盟标准合同条款（SCC），东盟跨境数据流动示范合同条款（MCCs），或其他国际上广泛采用的合同，制定一个中国标准合同的模板。

针对重要数据订立的条文现在适用于所有数据：依据当前意见稿，任何与重要数据有关的数据都可能面临安全评估。这意味着，不论企业采取怎样的隐私或数据安全措施，总是可能会面临重复监管。比如，如果企业雇员参与的项目恰好涉及重要数据，除非设置豁免条例，那么这些雇员的人力资源数据或被解读为涉及国家利益的“重要数据”。

监管主体权限较大，过度监管风险增加：当前意见稿赋予了监管部门较大权限，这意味着企业即便因小的过失或疏忽面临安全评估，也需要向监管部门提供访问其私营领域数据的权限。这种监管方式忽视了企业对消费者负有的法律和合同规定的责任。

应增设合理的过渡期，配合法律施行：鉴于网络安全和数据管理方面的合规负担较重，企业需要投入大量资源和时间，为了确保有充足时间厘清这些标准，我委员会建议在所有重要数据目录颁布后，设立 18 至 24 个月的宽限期。

应参照国际标准，考虑法律影响：我委员会高度认可中国政府在《数字经济伙伴关系协定》（DEPA）和《全面与进步跨太平洋伙伴关系协定》（CPTPP）框架下主动采取的措施。考虑到中国正在积极参与国际标准的制定过程，我委员会强烈建议中国尽可能多认可、多采纳国际标准，包括遵循数据跨境自由流动、禁止规定数据存储本地化等。在国际标准的基础上制定法律是开放、包容、透明的充分体现，这样既能确保中国国内标准的全面性，又能持续促进经济增长。

厘清个人信息和重要数据，分别监管：虽然在本意见稿和其他法规中，超过一定数量的个人信息会都被直接当作重要数据，但是从本质和风险来看，个人信息与重要数据仍存在区别。因此，不同数据类型应该对应不同的隐私保护标准。将这两个术语混为一谈的法规将会给企业增加不必要的合规成本，亦不能满足消费者需求。

推动商业群体建设，建设互信伙伴关系：我委员会支持政府积极展开可信的数据监管实践，比如根据风险建立分类分级的数据保护制度。为了使分类达到最佳效果，监管部门和商业群体应基于其行业和领域，采取以风险管控为本的解决方法，充分发挥自我裁定权，对各自数据进行分类分级。此外，鉴于二者的分类分级目的不同，我们建议区分政府数据和商业数据。对于商业数据分类而言，企业应有权带头对所有权下的数据设定适当的分级分类标准。

关于各条文的具体意见可以参考下表。我委员会感谢有此机会提交意见，以下是针对相关条款提出的具体建议。联系人：闫羽；010-65920727;邮箱 yyan@uschina.org

条款号	条款内容	意见	建议
2	**第二条** 在中华人民共和国境内利用网络开展数据处理活动，以及网络数据安全的监督管理，适用本条例。 自然人因个人或者家庭事务开展数据处理活动，不适用本条例。	本条原本的规定仅针对域外数据处理适用，现范围扩大至中国境内“重要数据”的处理。这与《中华人民共和国个人信息保护法》规定不符，缺乏法律依据。	建议根据《个人信息保护法》，将本条适用范围改回“个人信息”，严格参照《个人信息保护法》划定适用情形。我们提出了以下建议： 1. 删去第（三）款； 2. 仅在危害国家安全，公众利益，侵害公民权利的时可以适用于域外； 3. 解释本条法律不适用于脱机（比如人工处理数据或在离线处理数据时）数据处理的含义； 4. 豁免因个人或者家庭事务开展内部数据处理活动的行为； 5. 明确第（二）款中的“分析”和“安全评估”。
5	**第五条** 国家建立数据分类分级保护制度。按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。 国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。各地区、各部门应当按照国家数据分类分级要求，对本地区、本部门以及相关行业、领域的数据进行分类分级管理。		建议将本条第一句话改为：“第五条 国家为政府数据建立数据分类分级保护制度。” 建议行业主管部门和地方政府合作洽谈，共同完成数据分级分类工作。本条关于“一般数据”的内容与《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》不符，缺乏法律依据，建议删除。 如保留，为避免误解、保持一致性，建议采用国家标准中“普通数据”的概念替换“一般数据”。

6	**第六条** 数据处理者对所处理数据的安全负责，履行数据安全保护义务，接受政府和社会监督，承担社会责任。数据处理者应当按照有关法律、行政法规的规定和国家标准的强制性要求，建立完善数据安全管理制度和技术保护机制。	强制要求应以法规形式明确列出。国家标准只能作为建议，不能在规章中作为要求企业强制执行的标准。应该保留企业自由裁量权，根据自身情况来确定最佳方式，而国家标准仅作为参考、或者部分采纳的最佳实践。 此外，本条的使用范围应限于重要数据或核心数据的处理者，不包括个人信息处理者。	建议将本条修改为： “第六条 重要数据和核心数据处理者对所处理数据的安全负责，履行数据安全保护义务，接受政府和社会监督，承担社会责任。数据处理者应当按照有关法律、行政法规的规定和国家标准的强制性要求，建立完善数据安全管理制度和技术保护机制。”
7	**第七条** 国家推动公共数据开放、共享，促进数据开发利用，并依法对公共数据实施监督管理。国家建立健全数据交易管理制度，明确数据交易机构设立、运行标准，规范数据流通交易行为，确保数据依法有序流通。	建议明确公共数据的构成和产出者。 是否允许企业随意处理集中、匿名化、拟匿名化的公共数据？	
8	**第八条** 任何个人和组织开展数据处理活动应当遵守法律、行政法规，尊重社会公德和伦理，不得从事以下活动： …. 任何个人和组织知道或者应当知道他人从事前款活动的，不得为其提供技术支持、工具、程序和广告推广、支付结算等服务。	服务提供方不应该为本条中服务使用者的违法行为负责。 大部分跨国企业已经设定保护商业机密和消费者隐私的内部章程，包括明确排除非法数据处理行为的责任与义务合同。	建议补充，如果服务提供商通过中断或终止服务和支持来对付消费者，应提供证明非法行为存在的法律证据，或监管部门下达的指令。 因此建议直接删除整条，因为本条列举的民事或刑事违法行为都已经被现有法律规章涵盖。
9	**第九条** 数据处理者应当采取备份、加密、访问控制等必要措施，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，应对数据安全事件，防范针对和利用数据的违法犯罪活动，维护数据的完整性、保密性、可用性。 数据处理者应当按照网络安全等级保护的要求，加强数据处理系统、	网络安全等级保护制度（MLPS）和《关键信息基础设施安全保护条例》订立了等级保护和关键信息基础设施安全保护的基本原则和流程。因此，在建设等级分类保护制度、规范关键信息基础设施时，也应该考虑上述内容。 应该删除“处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求”这种缺乏法律依据的规定。	清晰的系统范围定义是有必要的，以避免不必要的误解。 对于处理重要数据的系统要求满足等级保护三级或以上是有必要的，但是对于非关键信息基础运营者，要同时再满足关键信息基础设施安全保护要求，会给企业增加不必要的工作量和运营成本。

	数据传输网络、数据存储环境等安全防护，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，处理核心数据的系统依照有关规定从严保护。 数据处理者应当使用密码对重要数据和核心数据进行保护。	处理重要数据的数据处理者不一定是关键信息基础运营者。因此对于非关键信息基础运营者对其处理重要数据的系统完成等级保护三级后，是否有必要还要满足关键信息基础设施安全保护要求？ 需要进一步说明“密码”技术。此处的密码是侧重于单纯的密码还是包含其他密码技术？	因此，建议只有关键信息基础运营者需要另外满足关键信息基础设施安全保护要求。鉴于保护重要数据和核心数据的方法和技术非常多，建议保护形式不局限于单纯的密码，而接受除密码外的其他技术（比如：访问控制，加密等） 建议将本条清晰断句，修改为： “第九条 数据处理者应当采取备份、加密、访问控制等必要措施，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，应对数据安全事件，防范针对和利用数据的违法犯罪活动，维护数据的完整性、保密性、可用性。 数据处理者应当按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护。 处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求。处理核心数据的系统依照有关规定从严保护。 数据处理者应当对重要数据和核心数据进行加密保护。”
10	**第十条** 数据处理者发现其使用或者提供的网络产品和服务存在安全缺陷、漏洞，或者威胁国家安全、危害公共利益等风险时，应当立即采取补救措施。	意见稿应该基于风险管控的原则，允许企业自主选择合适的补救措施。	建议将本条修改为： “第十条 数据处理者发现其使用或者提供的网络产品和服务存在安全缺陷、漏洞，或者威胁国家安全、危害公共利益等风险时，应当立即采取适

			当补救措施。”
11	**第十一条** 数据处理者应当建立数据安全应急处置机制，发生数据安全事件时及时启动应急响应机制，采取措施防止危害扩大，消除安全隐患。.... （一）在发生安全事件的八小时内向设区的市级网信部门和有关主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等； （二）在事件处置完毕后五个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。	该条所设置的告知/报告时限过于严苛，考虑到数据安全事件常发性、往往需要一定的知悉和了解时间，并且通常还涉及复杂的技术问题，建议安全事件中适当提升告知/报告的门槛，明确合规动作的优先序并延长时限要求。如因时限过短导致不具备可操作，出现普遍性的违法或将采取补救措施和报告义务本末倒置，并不利于维护数据安全和信息主体权益。企业处理安全事件过程中应该将排查风险和消除危害后果作为第一要务，优先集中资源采取适当的补救措施，其次才是告知和报告义务。	建议将本条修改为： 第十一条 “发生重要数据或者十万人以上个人信息泄露、毁损、丢失等数据安全事件时，数据处理者还应当履行以下义务： （一）在发生安全事件的七十二小时内向设区的市级网信部门和有关主管部门报告事件基本信息，包括涉及的数据数量、类型、可能的影响、已经或拟采取的处置措施等； （二）在事件处置完毕后三十个工作日内向设区的市级网信部门和有关主管部门报告包括事件原因、危害后果、责任处理、改进措施等情况的调查评估报告。”
12	**第十二条** 数据处理者向第三方提供个人信息，或者共享、交易、委托处理重要数据的，应当遵守以下规定： （三）留存个人同意记录及提供个人信息的日志记录，共享、交易、委托处理重要数据的审批记录、日志记录至少五年。	《个人信息保护法》第四十七条中要求“处理目的已实现、无法实现或者为实现处理目的不再必要”时需要删除个人信息数据，而此条款中要求相关记录要至少保存5年。 如果企业需要在每次变更或新增数据处理者之前取得用户同意，用户会面临消息轰炸。这种情况下，用户不得不从“同意”和干扰中做出选择。因为用户会因为没有给与“同意”就终止了服务感到困惑、不满。此外，留存同意记录的期限也过长。 强制规定留存期限会导致无用数据堆积，且第二十二条中明显已经要求数据在不需要的情况下应删除。	建议将本条按照个人信息和重要数据一分为二。建议将“第三方”改为“其他数据处理者”，与《个人信息保护法》保持一致。 建议和《个人信息保护法》统一，清晰界定需要存储的数据的范围和年限，以帮助数据处理者正确地、合规地处理数据，避免不必要的误解。

13	**第十三条** 数据处理者开展以下活动，应当按照国家有关规定，申报网络安全审查： ….. 大型互联网平台运营者在境外设立总部或者运营中心、研发中心，应当向国家网信部门和主管部门报告。	该标准过于宽泛，实践中经营者难以自行判断业务是否属于需要申报网络安全审查的交易。 网络安全审查是否指的是《数据安全法》中的“国家安全审查”？如是，建议替换本意见稿中的说法，因为本意见稿是《数据安全法》的配套施行法律。	由于个人可能承担的风险已经显著降低，建议本条豁免匿名化与拟匿名化的个人信息。 另外，建议明确申报门槛。
14	**第十四条** 数据处理者发生合并、重组、分立等情况的，数据接收方应当继续履行数据安全保护义务，涉及重要数据和一百万人以上个人信息的，应当向设区的市级主管部门报告；数据处理者发生解散、被宣告破产等情况的，应当向设区的市级主管部门报告，按照相关要求移交或删除数据，主管部门不明确的，应当向设区的市级网信部门报告。	考虑到目前互联网产业的产业规模以及数据在各个产业中的广泛运用，一百万的门槛过低，将导致大量数据处理者在惯常的交易活动中均负有报告义务，并且该报告义务在法律意义上和程序意义上均不明确，将会给交易带来不确定性。例如，交易方无法在交易谈判过程中和交易合同文本中准确预估该报告义务对交易可能产生的影响。过低的门槛和不确定的流程不仅会导致不成比例地挤占监管资源，而且会严重影响商业交易效率，进而制约经济发展。另外在企业解散或破产情况下额外施加报告义务与《个人信息保护法下》规定和精神不符。后者仅要求告知个人信息主体。	建议删除本条。 如保留，建议对该条做如下修改： 1. 提高申报门槛到 1 亿人； 2. 明确该报告义务的具体程序和法律后果包括处理时限； 3. 删除“数据处理者发生解散、被宣告破产等情况的……应当向设区的市级网信部门报告”。
15	**第十五条** 数据处理者从其他途径获取的数据，应当按照本条例的规定履行数据安全保护义务。	《个人信息保护法》已对数据处理者处理数据（包括数据收集）的合法性基础进行了列举，此处“其他途径”的内涵不明确且无必要。并且，本条和第六条第（一）款的内容有重合。	删除第十五条。
17	**第十七条** 数据处理者在采用自动化工具访问、收集数据时，应当评估对网络服务的性能、功能带来的影响，不得干扰网络服务的正常功能。 自动化工具访问、收集数据违反法律、行政法规或者行业自律公约、影响网络服务正常功能，或者侵犯他人知识产权等合法权益的，数据处理者应当停止访问、收集数据行	依据本条，组织似乎可以利用自动化工具收集合法公开的公共数据？建议解释说明，并考虑采集、处理商业数据的情形。 建议澄清自动化工具收集的数据的合法形式，以及这类数据能否出境。 澄清“不得干扰网络服务的正常功能”的含义，什么行为构成干扰。 企业应该根据自身抗风险能力，自主决定是否运用这类	建议将本条修改为： “第十七条 数据处理者在采用自动化工具访问、收集数据时，应当评估对网络服务的性能、功能带来的影响，不得干扰网络服务的正常功能。自动化工具访问、收集数据违反法律、行政法规或者行业自律公约、影响网络服务正常功能，或者侵犯他人知识产权等合法权益的，数据处理者应当停止访问、收集数据行为并采取

	为并采取相应补救措施。	工具。比如，对于一些较为敏感的系统，企业需要加大投入才能达到同等级的保护标准。任何强制性规定都应该明确写入法规中。	相应补救措施。”
18	**第十八条** 数据处理者应当建立便捷的数据安全投诉举报渠道，及时受理、处置数据安全投诉举报。数据处理者应当公布接受投诉、举报的联系方式、责任人信息，每年公开披露受理和收到的个人信息安全投诉数量、投诉处理情况、平均处理时间情况，接受社会监督。	《个人信息保护法》中规定，大型网络平台必须定期发布个人信息保护社会责任报告，以供公众监督。但是，本条中，相关规定的范围扩大到了所有数据处理者均需要发布报告。对于几乎仅处理雇员个人信息的组织来说，个人信息安全投诉受理的情况没有任何意义。 对于重要数据而言，组织自然不会同公众分享重要数据。因此，建立一个公开且接受公众监督的渠道意义不大。再者，安全事件的披露可能会无意间吸引黑客的注意。另外，我们认为要求企业公开投诉细节和处理情况实属多余且不合理的行为。 此外，本条中关于投诉举报渠道的架构并不清晰。建议说明组织任命的责任人是否会负责整个投诉举报流程？ 建议对第二段的投诉范围进一步定义和明确。 比如，明确什么是个人信息安全投诉的含义；公开的投诉仅对于个人信息投诉还是包括所有数据安全投诉？另外，公司内部的员工的投诉是否也需要公开披露？	建议与《个人信息保护法》第五十八条的规定保持一致，将适用范围限定于大型互联网平台。对于个人信息处理者，应采用《个人信息保护法》中列出的投诉渠道，行使数据主体的权利。另建议删去关于公开披露个人信息投诉情况的规定。
第三章	**个人信息保护**		本章内容与《个人信息保护法》重复。建议直接删去，避免不必要的重复规定。
19	**第十九条** 基于个人同意处理个人信息的，应当满足以下要求： （一）处理的个人信息是提供服务所必需的，或者是履行法律、行政法规规定的义务所必需的； （二）限于实现处理目的最短周期、最低频次，采取对个人权益影响最小的方式； （三）不得因个人拒绝提供服务必需的个人信息以外的信息，拒绝提	此条款的第（一）款中的“或者是履行法律、行政法规规定的义务所必需的”和《个人信息保护法》第十三条第（三）款“为履行法定职责或者法定义务所必需”相冲突。《个人信息保护法》第十三条规定“为履行法定职责或者法定义务所必需”，不需取得个人同意，而此条款中却需要获得个人同意。	建议删除第（一）款，给予企业自由裁量权，使企业能够根据自身数据处理和风险承受能力，定义“必需”处理个人信息的含义。 对于积极践行合规的企业来说，减少数据收集和使用并不会干扰为用户提供的正常服务。建议网信办肯定此类合规行为，尽力将《个人信息保护法》建设为与国际标准（GDPR，APEC隐私）相适应的法律。

	供服务或者干扰个人正常使用服务。		
20	**第二十条** 数据处理者处理个人信息，应当制定个人信息处理规则并严格遵守。个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、简明通俗，系统全面地向个人说明个人信息处理情况。 个人信息处理规则应当包括但不限于以下内容： …… （四）以集中展示等便利用户访问的方式说明产品服务中嵌入的所有收集个人信息的第三方代码、插件的名称，以及每个第三方代码、插件收集个人信息的目的、方式、种类、频次或者时机及其个人信息处理规则； ……	考虑到互联网产品的复杂性和创新性，清单形式的列明所有个人信息目的、种类的方式存在实践难度，也会限制业务或产品功能的研发和拓展，包括产品功能或流程的更新。频次和时机尤其应该根据业务或技术的实际需求设定，而不应该提前限定。在满足合法性基础和必要最小化原则的前提下，具体个人信息处理规则的表达方式和形式并不能实质提升或降低对个人信息的保护水平。另外，此条款中的个人信息处理规则要求包含的内容太过细化，超出了《个人信息保护法》所要求的个人信息处理规则。比如：第（一）款和第（四）款都增加了“频次”和 “时机”，第（五）款中的所有第三方信息等 在《个人信息保护法》中并未提及。让跨国公司预先进行如此详细的说明是有困难的。	这一规定的目的是更好地保障用户的知情权，然而也应充分考虑企业现状。在个人信息处理规则中要求列出太过细化的内容对跨国公司来说是有困难的， 同时还会增加数据处理者的成本。因此，建议参考《个人信息保护法》和 GDPR 的要求，清晰简明可执行的个人信息处理规则的要求和范围。删除“以清单形式”和“频次或者时机”。 我们还建议明确，本条第（四）款中的“第三方”仅指代外部第三方，不包含同属一家母公司的子公司。例如，一个跨国企业的总部可能会为不同法域中的多个子公司主体集中提供 IT 服务，但他们所受的限制是完全一样的。这种情况不在本款讨论的范围内。
21	**第二十一条** 处理个人信息应当取得个人同意的，数据处理者应当遵守以下规定： （二）处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人单独同意； .... 对个人同意行为有效性存在争议的，数据处理者负有举证责任。	本条第（二）款和第七十三条规定并解释了“单独同意”，即组织需要在每项个人信息的处理活动前征求个人同意。 我们认为，如果个人能够审查每项待处理的个人信息、以及组织处理的具体方式，那么个人的同意充分且有效。这种情况下，要求个人逐一提供书面同意只会增加个人和组织的负担。 本条还规定了，数据处理者对个人同意行为有效性存在争议的事件负有举证责任。但是考虑到个人同意可以随时撤回，即使数据处理者负担举证，争议还是无法解决。	建议修改“单独同意”的定义和要求。鉴于“同意”可以随时撤回，建议认为数据处理者不应该负有举证责任。
22	**第二十二条** 有下列情况之一的，数	本条规定与《个人信息保护法》第四十七条关于删除权	第二十二条修改为如下：“有下列情

	据处理者应当在十五个工作日内删除个人信息或者进行匿名化处理： （一）已实现个人信息处理目的或者实现处理目的不再必要； （二）达到与用户约定或者个人信息处理规则明确的存储期限； （三）终止服务或者个人注销账号； （四）因使用自动化采集技术等，无法避免采集到的非必要个人信息或者未经个人同意的个人信息。 删除个人信息从技术上难以实现，或者因业务复杂等原因，在十五个工作日内删除个人信息确有困难的，数据处理者不得开展除存储和采取必要的安全保护措施之外的处理，并应当向个人作出合理解释。法律、行政法规另有规定的从其规定。	的规定有冲突，应在《个人信息保护法》规定的基础上进行细化，尤其应考虑到无需个人同意的情况下收集的个人信息，其删除规则理应区别于根据个人同意收集的个人信息。	况之一的，数据处理者应当主动删除个人信息；数据处理者未删除的，个人有权请求删除，数据处理者应当在十五个工作日内删除个人信息或者进行匿名化处理： （一）已实现个人信息处理目的或者实现处理目的不再必要； （二）达到与用户约定或者个人信息处理规则明确的存储期限； （三）终止服务或者个人撤回同意； （四）因使用自动化采集技术等，无法避免采集到的非必要个人信息或者未经个人同意的个人信息，但法律、行政法规规定无需个人同意的除外。 建议将本条修改为： 1. 15 个工作日内进行响应；或 2. 30 个工作日内完成处理。”
22	第**二十二条** 有下列情况之一的，数据处理者应当在十五个工作日内删除个人信息或者进行匿名化处理： （一）已实现个人信息处理目的或者实现处理目的不再必要； （二）达到与用户约定或者个人信息处理规则明确的存储期限； （三）终止服务或者个人注销账号； （四）因使用自动化采集技术等，无法避免采集到的非必要个人信息或者未经个人同意的个人信息。 删除个人信息从技术上难以实现，或者因业务复杂等原因，在十五个工作日内删除个人信息确有困难的，数据处理者不得开展除存储和采取必要的安全保护措施之外的处	“在十五个工作日内删除个人信息”， “向个人作出合理解释” 和第四款不在《个人信息保护法》中，公司在执行这些操作时是有困难的。而在《通用数据保护条例》（GDPR）中，设置的期限是一个月。 本条的规定非常令人担忧，因为结合第六十一条，企业如果违反第二十二、二十三条的规定，可能会承担高达百分之五营业额的罚金，而跨国企业则需要做出非常大的调整才能实现合规。 此外，第（四）款和现有的《反恐法》的第三十二条冲突。《反恐法》中其要求自动化采集的数据至少保存九十天（比如：CCTV 摄像头获取的个人影像等），而此条款却要求在十五天内删除。	建议参考《个人信息保护法》第四十七条，定义清晰可操作的数据删除相关要求，以避免不必要的误解而导致的违规操作。 强烈建议按照国际通用法律，将回应个人信息变更的期限从十五天延长至一个月。

	理，并应当向个人作出合理解释。		
23	**第二十三条** 个人提出查阅、复制、更正、补充、限制处理、删除其个人信息的合理请求的，数据处理者应当履行以下义务： （一）提供便捷的支持个人结构化查询本人被收集的个人信息类型、数量等的方法和途径，不得以时间、位置等因素对个人的合理请求进行限制； （二）提供便捷的支持个人复制、更正、补充、限制处理、删除其个人信息、撤回授权同意以及注销账号的功能，且不得设置不合理条件； （三）收到个人复制、更正、补充、限制处理、删除本人个人信息、撤回授权同意或者注销账号申请的，应当在十五个工作日内处理并反馈。 法律、行政法规另有规定的从其规定。	本条规定了如何回应数据主体的请求。建议为各组织核实数据主体身份留出时间，以及在无法确认身份时，给予企业拒绝请求的权利。根据《个人信息保护法》，组织需要承担无罪举证的责任，所以有权享受上述权利。 “限制处理”的定义和内涵不清晰可能导致企业无法落实或按照统一的标准来落实这一个人权利。	建议补充说明数据处理者有权核实数据主体的身份。解释“个人结构化”或删除该款。 澄清“限制处理”的具体含义，例如冻结或暂停处理。
24	**第二十四条** 符合下列条件的个人信息转移请求，数据处理者应当为个人指定的其他数据处理者访问、获取其个人信息提供转移服务： （一）请求转移的个人信息是基于同意或者订立、履行合同所必需而收集的个人信息； （二）请求转移的个人信息是本人信息或者请求人合法获得且不违背他人意愿的他人信息； （三）能够验证请求人的合法身份。 数据处理者发现接收个人信息的其	数据转移技术上除了存在相关数据是否通过自动化方式进行处理之外，还取决于第三方是否可以接受以及接受的形式。此外，相关个人信息如非本人信息，数据处理者并无能力验证转移请求是否“请求人合法获得且不违背他人意愿”。因此为确保可行性且损害第三方利益，建议增加限制性条件。	建议未来专门讨论本条所涉问题，结合行业力量建设数据交换的互认标准。目前本条的规定会加剧数据传输中的摩擦，企业也不得不匆忙采取合规行动，而导致没有时间商议更高效、更利于用户的统一标准。 如保留，删除第（二）款中“或者请求人合法获得且不违背他人意愿的他人信息”，增加 （i）“请求转移的个人信息系通过自动化方式处理且转移服务技术上可行” 以及（ii）请求转移不影响第三方的合法权益。

	他数据处理者有非法处理个人信息风险的，应当对个人信息转移请求做合理的风险提示。 请求转移个人信息次数明显超出合理范围的，数据处理者可以收取合理费用。		
26	**第二十六条** 数据处理者处理一百万人以上个人信息的，还应当遵守本条例第四章对重要数据的处理者作出的规定。	个人信息种类繁多，单纯的数据量已不再是衡量风险的有效指标，所以本条增加相关数据处理者的法律责任并无依据。国际条例中保护个人信息的目的是保护个人隐私和利益，与国家利益和国家安全无关。因此，将个人信息和国家安全相关的数据混为一谈，不符合国际惯例，也与 CPTPP，RCEP，DEPA 等多边协定的精神相左。	建议区分个人数据和重要数据，并删除第二十六条。
27	**第二十七条** 各地区、各部门按照国家有关要求和标准，组织本地区、本部门以及相关行业、领域的数据处理者识别重要数据和核心数据，组织制定本地区、本部门以及相关行业、领域重要数据和核心数据目录，并报国家网信部门。	说明“收集”是不是指监管机构会指挥、控制数据处理者如何处理重要或核心信息？	
28	**第二十八条** 重要数据的处理者，应当明确数据安全负责人，成立数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责： .... 数据安全负责人应当具备数据安全专业知识和相关管理工作经历，由数据处理者决策层成员承担，有权直接向网信部门和主管、监管部门反映数据安全情况。	处理重要数据的一方是否必须委派数据安全负责人，是否需要成立数据安全管理机构？	建议保留企业自主裁量权，设立符合自身条件的重要数据管理体系，并通过现有管理体系保护个人信息。

29	**第二十九条** 重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案，备案内容包括： （一）数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等； （二）处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身； （三）国家网信部门和主管、监管部门规定的其他备案内容。 处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。 依据部门职责分工，网信部门与有关部门共享备案信息。	既然各个行业主管部门会负责识别行业重要数据，那么重要数据的注册地就应该是行业主管部门，而不是网信办。	建议将本条修改为： “第二十九条 重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的行业主管部门备案，进一步与市级网络空间主管部门协调，备案内容包括： （一）数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等； （二）处理数据的目的、规模、方式、范围、类型、存储期限、存储地点等，不包括数据内容本身； （三）国家网信部门和主管、监管部门规定的其他备案内容。 处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。 依据部门职责分工，网信部门与有关部门共享备案信息。”处理数据的目的、范围、类型及数据安全防护措施等发生重大变化，组织应当重新备案。 依据各部门职责分工，网信部门与有关部门共享备案信息。
31	**第三十一条** 重要数据的处理者，应当优先采购安全可信的网络产品和服务。	建议澄清“安全可信”的定义和内涵，避免构成对外资企业的歧视。	建议删除本条，采纳技术中性的方法，允许公司依据自身经营需求，选择合适技术。
32	**第三十二条** 处理重要数据或者赴境外上市的数据处理者，应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并在每年 1 月 31 日前将上一年度数据安全评估报告报设区的市级网信部门，年度数	出于本条服务数据共享和贸易的宗旨，我委员会建议本条豁免受委托处理数据的处理者。此外，合同条款应明确约定受委托方和数据处理者之间的权利和义务。	建议对于向境外提供重要数据的数据处理者，将“数据安全评估”与第三十七条中“数据出境安全评估”合并，降低企业成本。 此外，我们认为年度评估过于频繁。

	据安全评估报告的内容包括：		建议将评估周期改为三年。建议将本条最后一句改为：“如果评估认为可能危害国家安全，经济发展或公共利益，数据处理者不应该共享、交易、委托处理、向境外提供数据。”
33	**第三十三条** 数据处理者共享、交易、委托处理重要数据的，应当征得设区的市级及以上主管部门同意，主管部门不明确的，应当征得设区的市级及以上网信部门同意。	如结合第二十六条的规定，处理一百万人以上个人信息的，似乎也需要征得同意。企业日常经营中对数据进行共享或委托处理是非常常规的操作，例如聘用第三方客服公司，如果均需获得主管部门同意，无疑会给企业正常经营带来不必要的阻碍，影响正常的商业运行。 并且，征得同意本质上构成一种行政许可。根据《行政许可法》，设定和实施行政许可，应当依照法定的权限、范围、条件和程序。	建议删除第二十六条，并且明确“同意”的实体和程序要求包括如范围、处理时限和复议流程。
第五章	**数据跨境安全管理**	第五章规定了数据跨境传输，但我们不清楚本章与《数据出境安全评估办法（征求意见稿）》之间的关系。如果本法是《中华人民共和国数据安全法》《中华人民共和国网络安全法》和《中华人民共和国个人信息保护法》的配套实施办法，那么它应该包含《数据出境安全评估办法（征求意见稿）》中的部分内容，并以更简单、清晰的方式呈现组织合规的路径。	公司内部跨境数据传输是跨国企业经营的基础，建立合规基础上的认证、报告、评估是跨国企业商业运营的内容，因此我们建议本章豁免跨国企业的子公司和母公司、地区总部之间的数据（包括个人信息）传输。因此，如果跨境数据传输受到影响，也会打击这些企业未来在华投资。
35	**第三十五条** 数据处理者因业务等需要，确需向中华人民共和国境外提供数据的，应当具备下列条件之一： （一）通过国家网信部门组织的数据出境安全评估； （二）数据处理者和数据接收方均通过国家网信部门认定的专业机构进行的个人信息保护认证； （三）按照国家网信部门制定的关于标准合同的规定与境外数据接收	第三十五条放大了《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》的适用范围，适用对象从跨境传输的情形扩拓展到了所有数据。这样过严的规定会对数据传输产生巨大影响。 本条第（三）款，“按照国家网信部门制定的关于标准合同的规定与境外数据接收方订立合同。 ”这里的标准合同与《个人信息保护法》第三十八条里的标准合同是否一致？	建议当局采纳国际上通用的、互认的方式，承认国际上取得的资质，比如GDPR、APEC、CBPR、欧盟标准合同条款（SCC）和东盟跨境数据流动示范合同条款（MCCs）。不建议重新制定新条文，也不要求企业重新起草国内的标准合同。

	方订立合同，约定双方权利和义务； （四）法律、行政法规或者国家网信部门规定的其他条件。 数据处理者为订立、履行个人作为一方当事人的合同所必需向境外提供当事人个人信息的，或者为了保护个人生命健康和财产安全而必须向境外提供个人信息的除外。	数据处理者需不需要为个人信息和非个人信息处理各签署一份单独的合同？ 本条最后一句中，如果数据处理依据合同必要要求，将个人信息传输至海外，是不是属于“数据处理者为订立、履行个人作为一方当事人的合同所必需向境外提供当事人个人信息”的情形，是不是说无需再满足前（三）款中的任一条件？	
36	**第三十六条** 数据处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意。收集个人信息时已单独就个人信息出境取得个人同意，且按照取得同意的事项出境的，无需再次取得个人单独同意。	本条概括性的要求所有个人信息的跨境提供都取得个人同意，和《个人信息保护法》第十三条的规定不一致，应该明确排除不需要同意的情形。 为了与《个人信息保护法》的规定保持一致，本条应该不包括受委托的信息处理者和日常信息传输（例如，由雇主发起的信息传输）。 此外，网信办应该考虑披露信息接收方的机密和敏感细节可能会影响企业供应链的完整性。	修改为“数据处理者向中华人民共和国境外提供个人信息的，应当向个人告知境外数据接收方的名称、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外数据接收方行使个人信息权利的方式等事项，并取得个人的单独同意，法律、行政法规规定不需要个人同意的除外。”
37	**第三十七条** 数据处理者向境外提供在中华人民共和国境内收集和产生的数据，属于以下情形的，应当通过国家网信部门组织的数据出境安全评估： （一）出境数据中包含重要数据； （二）关键信息基础设施运营者和处理一百万人以上个人信息的数据处理者向境外提供个人信息； （三）国家网信部门规定的其它情形。 法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。	1. 数量标准过低将导致达到安全评估申报数量门槛的企业过多，极可能不合理地增加相应企业的合规成本，阻碍正常的跨境数据流动和商业发展，而且可能不成比例地导致对行政资源的占用和消耗。 2. 并且，申报标准应综合考虑跨境传输场景的多样性。过于严格的跨境数据传输限制与中国寻求加入或已加入的国际公约不符。 3. 如果全国范围内的所有申报都最终需要国家网信部门审批，会导致申报积压从而产生评估效率问题。同时因为门槛过低，大量申报得不到及时处理，可能会大规模影响申报企业的正常运营。	建议对本条作如下修改： 1. 将评估和审批权下放至省级部门，以加快评估流程。 2. 针对本条第（二）款，建议提高并明确数据出境安全评估的申报门槛。

39	**第三十九条** 数据处理者向境外提供数据应当履行以下义务： ..... （九）个人信息出境后确需再转移的，应当事先与个人约定再转移的条件，并明确数据接收方履行的安全保护义务。 非经中华人民共和国主管机关批准，境内的个人、组织不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。	本条规定，数据处理者应当立即停止网信办认定不得出境的数据出境。但是，该要求可行性低，且会给贸易带来不必要的阻碍，将私营领域知识产权置于风险当中。 本条规定，网信办核验个人信息和重要数据类型和范围时，要求数据处理者解密个人信息，但该规定同时也会削弱用户隐私保护力度。 此外，数据处理者不应该被要求停止数据传输，而是应该被提供一个窗口补救期。 最后，本条还要求“事先与个人约定”传输条件。这一表述非常模糊，建议先明确行为当事人，因为这种情形下，我们不可能和数据主体进行商议。	建议删除本条，设立企业分享问题数据信息的机制。该平台只需涉及数据种类和范围，无需提供用户的真实个人信息。或者/同时，考虑点对点加密的信息传输方式，因为这种信息无法被企业解码。
40	**第四十条** 向境外提供个人信息和重要数据的数据处理者，应当在每年1月31日前编制数据出境安全报告，向设区的市级网信部门报告上一年度以下数据出境情况： （一）全部数据接收方名称、联系方式； （二）出境数据的类型、数量及目的； （三）数据在境外的存放地点、存储期限、使用范围和方式； （四）涉及向境外提供数据的用户投诉及处理情况； （五）发生的数据安全事件及其处置情况； （六）数据出境后再转移的情况； （七）国家网信部门明确向境外提供数据需要报告的其他事项。	重要数据跨境传输的有关规定可以参见《数据出境安全评估办法（征求意见稿）》，建议本条的最终版本参照此法，要求满足以下情形的数据处理者根据规定出具数据出境报告，提交至行业主管部门： 1. 出境数据中含重要数据； 2. 关键基础设施运营者或者向海外提供个人信息采集数量超过一万人或更多的数据处理者； 3. 国家网信部门明确向境外提供数据需要报告的其他事项。	建议删除本条。如保留，应根据《数据出境安全评估办法（征求意见稿）》将本条调整为： “第四十条 向境外提供个人信息和重要数据的数据处理者，应当在每年1月31日前编制数据出境安全报告，向主要行业主管部门报告上一年度数据出境情况，包括： （一）全部数据接收方名称、联系方式； （二）出境数据的类型、数量及目的； （三）数据在境外的存放地点、存储期限、使用范围和方式； （四）涉及向境外提供数据的用户投诉及处理情况； （五）发生的数据安全事件及其处置情况； （六）数据出境后再转移的情况； （七）国家网信部门明确向境外提供数据需要报告的其他事项。”

第五章	**跨境数据安全管理**	本章内容表述模糊不清。会让人误以为一般数据处理者也需要履行只有重要数据处理者和处理超过一百万人个人信息数据处理者才需要履行的义务。	清晰的定义和明确的范围可以帮助数据处理者更好地理解和合规地实施。
41	**第四十一条** 国家建立数据跨境安全网关，对来源于中华人民共和国境外、法律和行政法规禁止发布或者传输的信息予以阻断传播。 任何个人和组织不得提供用于穿透、绕过数据跨境安全网关的程序、工具、线路等，不得为穿透、绕过数据跨境安全网关提供互联网接入、服务器托管、技术支持、传播推广、支付结算、应用下载等服务。 境内用户访问境内网络的，其流量不得被路由至境外。	目前技术层面关于虚拟专用网络（VPN）和网关、网络内容等方面的规章管理已经非常严格。建议删除本条中的提议，避免冗余。 建议解释本条中部分术语“穿透”、“流量”、“境内网络”、“路由至境外”的意思。	建议删除本条。如果设立本条的目的是限制“流量被路由至境外”，建议补充详细解释，或直接整条删除。 如保留，我委员会希望明确规定：在华运营的外企或者在中国境内的外企子公司在使用中国电信服务商提供的企业虚拟专用网络（VPN）时，不会被视为境内用户。允许外国公司及其中国子公司自由发声至关重要，这是跨国企业实现国际运营和网络建设的基本前提。
42	**第四十二条** 数据处理者从事跨境数据活动应当按照国家数据跨境安全监管要求，建立健全相关技术和管理措施。	本条应根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》和《中华人民共和国个人信息保护法》重新调整适用范围，不应涵盖所有企业和行为、非个人信息和非重要信息。	建议删除本条。如保留，建议与《中华人民共和国数据安全法》《中华人民共和国网络安全法》和《中华人民共和国个人信息保护法》保持一致性，将本条修改为： “第四十二条 个人信息处理者或者重要数据处理者从事跨境数据活动应当按照国家数据跨境安全监管要求，建立完善的相关技术和管理措施。”
43	**第四十三条** 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，及时披露制定程序、裁决程序，保障平台规则、隐私政策、算法公平公正。..... 日活用户超过一亿的大型互联网平		考虑到人身安全、隐私安全、网络安全，建议删除本条中关于发布平台规则、隐私政策制定前需要“公开征求意见，确保用户能够便捷充分表达意见”的规定。

	台运营者平台规则、隐私政策制定或者对用户权益有重大影响的修订的，应当经国家网信部门认定的第三方机构评估，并报省级及以上网信部门和电信主管部门同意。		
44	**第四十四条** 互联网平台运营者应当对接入其平台的第三方产品和服务承担数据安全管理责任，通过合同等形式明确第三方的数据安全责任义务，并督促第三方加强数据安全管理，采取必要的数据安全保护措施。 第三方产品和服务对用户造成损害的，用户可以要求互联网平台运营者先行赔偿。 移动通信终端预装第三方产品适用本条前两款规定。	相关上位法《消费者权益保护法》《电子商务法》中的先行规定是以“网络交易平台提供者不能提供销售者或者服务者的真实名称、地址和有效联系方式” 为条件的。	我们建议删除本条，因为这会在平台运营商和第三方之间引入现行法律不支持的法律和其他责任风险。 “第三方产品和服务对用户造成损害的，并且互联网平台运营者不能提供销售者或者服务者的真实名称、地址和有效联系方式的，用户可以要求互联网平台运营者先行赔偿″
46	**第四十六条** 互联网平台运营者不得利用数据以及平台规则等从事以下活动： …… （二）利用平台收集掌握的经营者数据，在产品推广中实行最低价销售等损害公平竞争的行为； ……	“在产品推广中实行最低价销售”表述不清楚，并且不一定属于损害公平竞争的行为。	建议明确该行为的具体内容，或者明确指向该行为可能违反的《反不正当竞争法》《反垄断法》等具体法律法规的具体条款。
47	**第四十七条** 提供应用程序分发服务的互联网平台运营者，应当按照有关法律、行政法规和国家网信部门的规定，建立、披露应用程序审核规则，并对应用程序进行安全审核。对不符合法律、行政法规的规定和国家标准的强制性要求的应用程序，应当采取拒绝上架、督促整改、下架处置等措施。	明确安全审核的具体规则。	建议由应用程序的所有人，而非分发平台承担法律责任。 因为要求平台依据法规对所有应用程序有关全部法律法规的合规情况开展定期检测过于繁重，建议将本条第二句话的重点置于对所有不合法的应用程序下架处置时应该遵循的政策、程序、规定。

48	**第四十八条** 互联网平台运营者面向公众提供即时通信服务的，应当按照国务院电信主管部门的规定，为其他互联网平台运营者的即时通信服务提供数据接口，支持不同即时通信服务之间用户数据互通，无正当理由不得限制用户访问其他互联网平台以及向其他互联网平台传输文件。	建议明确“用户数据互通”与第六章互联网平台运营者义务之间的关系，或这一概念与整部意见稿之间的关系。	
49	**第四十九条** 互联网平台运营者利用个人信息和个性化推送算法向用户提供信息的，应当对推送信息的真实性、准确性以及来源合法性负责，并符合以下要求： .... （三）允许个人删除定向推送信息服务收集产生的个人信息，法律、行政法规另有规定或者与用户另有约定的除外。	《个人信息保护法》仅规定了不得进行不合理的差别待遇，以及提供退出机制。本条附加了没有上位法依据的额外义务，例如单独同意。	建议修改为： “第四十九条 互联网平台运营者利用个人信息和个性化推送算法向用户提供信息的，应当对推送信息的真实性、准确性以及来源合法性负责，并设置易于理解、便于访问和操作的一键关闭个性化推荐选项，允许用户拒绝接受定向推送信息。”
52	**第五十二条** 国务院有关部门履行法定职责需要调取或者访问互联网平台运营者掌握的公共数据、公共信息，应当明确调取或者访问的范围、类型、用途、依据，严格限定在履行法定职责范围内，不得将调取或者访问的公共数据、公共信息用于履行法定职责之外的目的。 互联网平台运营者应当对有关部门调取或者访问公共数据、公共信息予以配合。	建议澄清公开数据或公共信息不属于重要数据或核心数据的意义。	

55	**第五十五条** 国家网信部门负责统筹协调数据安全和相关监督管理工作。 公安机关、国家安全机关等在各自职责范围内承担数据安全监管职责。 工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。 主管部门应当明确本行业、本领域数据安全保护工作机构和人员，编制并组织实施本行业、本领域的数据安全规划和数据安全事件应急预案。 主管部门应当定期组织开展本行业、本领域的数据安全风险评估，对数据处理者履行数据安全保护义务情况进行监督检查，指导督促数据处理者及时对存在的风险隐患进行整改。		建议各个行业主管部门负责重要数据的管理，成为各行业汇报情况、了解相关规定的联络点。行业主管也可以借此机会与网信办展开合作。
56	**第五十六条** 国家建立健全数据安全应急处置机制，完善网络安全事件应急预案和网络安全信息共享平台，将数据安全事件纳入国家网络安全事件应急响应机制，加强数据安全信息共享、数据安全风险和威胁监测预警以及数据安全事件应急处置工作。		我委会建议建立一个精简的应急响应机制，将行业监管机构作为各自行业的协调机构，并建立行业监管机构与国家机构进一步协调的机制。这可以减少重复工作，并允许更好的部门管理和监督。
57	**第五十七条** 有关主管、监管部门可以采取以下措施对数据安全进行监督检查： （一）要求数据处理者相关人员就监督检查事项作出说明； （二）查阅、调取与数据安全有关的文档、记录；	强烈反对将检查以及将检查工具与企业网络相连。 这类检查本身具有潜在破坏性，会给企业的全球运营带来直接风险。脱离运营环境的检查系统和应用程序恐会扰乱公司运营。在联通度极高的金融业，检查可能会影响金融稳定性，危及全球金融体系。	建议将本条修改为： “第五十七条 有关主管、监管部门可以采取以下措施对数据安全进行监督检查： （一）要求数据处理者相关人员就监督检查事项作出说明；

	（三）按照规定程序，利用检测工具或者委托专业机构对数据安全措施运行情况进行技术检测； （四）核验数据出境类型、范围等； （五）法律、行政法规、规章规定的其他必要方式。 有关主管、监管部门开展数据安全监督检查，应当客观公正，不得向被检查单位收取费用。在数据安全监督检查中获取的信息只能用于维护数据安全的需要，不得用于其他用途。 数据处理者应当对有关主管、监管部门的数据安全监督检查予以配合，包括对组织运作、技术系统、算法原理、数据处理程序等进行解释说明，开放安全相关数据访问、提供必要技术支持等。	检查结果是企业高度敏感且至关重要的信息，应由企业自身掌管，不应分享给任何第三方。 建议网信办肯定保护企业专有信息、商业秘密的重要性，删除“开放安全相关数据访问和提供必要技术支持等”。 我委员会期待和网信办展开合作，依据现有法规，共同制定合理的管理条例，为企业规避风险。	（二）查阅、调取与数据安全有关的文档、记录； （三）按照规定程序，利用检测工具或者委托专业机构对数据安全措施运行情况进行技术检测； （四）核验数据出境类型、范围等； （五）法律、行政法规、规章规定的其他必要方式。 有关主管、监管部门开展数据安全监督检查，应当客观公正，不得向被检查单位收取费用。在数据安全监督检查中获取的信息只能用于维护数据安全的需要，不得用于其他用途。 数据处理者应当对有关主管、监管部门的数据安全监督检查予以配合，包括对组织运作、技术系统、算法原理、数据处理程序等，开放安全相关数据访问、提供必要技术支持等进行说明。
58	**第五十八条** 国家建立数据安全审计制度。数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。 主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。	我们呼吁安全审计尊重个人隐私，且认为审计过程中没有必要获取个人信息或敏感个人信息。	建议将本条修改为： “第五十八条 国家建立数据安全审计制度。处理一百万人以上个人信息的数据处理者，和重要数据处理者应当委托数据安全审计专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。 主管、监管部门组织开展对重要数据处理活动的审计，重点审计数据处理者履行法律、行政法规规定的义务等情况。”

59	**第五十九条** 国家支持相关行业组织按照章程，制定数据安全行为规范，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。 国家支持成立个人信息保护行业组织，开展以下活动：.... （五）违法处理个人信息、侵害众多个人的权益的行为，依法向人民法院提起诉讼。	任何行业自律条例和行业组织都应该以市场需求为主，自然自发形成。应该删除本条，自发成立的行业组织应顺应市场。	建议删除本条。
60	**第六十条** 数据处理者不履行第九条、第十条、第十一条、第十二条、第十三条、第十四条、第十五条、第十八条的规定，由有关主管部门责令改正，给予警告，可以并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可以处一万元以上十万元以下罚款；拒不改正或者导致危害数据安全等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、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五万元以上二十万元以下罚款。	我委员会认为，本管理条例应该是对《中华人民共和国数据安全法》《中华人民共和国网络安全法》和《中华人民共和国个人信息保护法》的澄清和解释。因此，任何法律责任的认定都应该以上述三部法律中的规定为准。在此条例中重复规定法律责任，会使前三部法律中关于法律责任的划定失去意义。	建议删除第六十条至第七十二条，或者依据《中华人民共和国数据安全法》《中华人民共和国网络安全法》和《中华人民共和国个人信息保护法》做出相应调整。
61	**第六十一条** 数据处理者不履行第十九条、第二十条、第二十一条、第二十二条、第二十三条、第二十四条、第二十五条规定的数据安全保护义务的，....；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、高级管理人员和个人信息保护负责人。		若企业违反第二十二条至二十四条对用户权利规定，我们建议免除百分之五营业额的罚款，并说明比例制的处罚适用的情形。

	有前款规定的违法行为，情节严重的，由有关部门责令改正，没收违法所得，并处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或者停业整顿、通报有关主管部门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、高级管理人员和个人信息保护负责人。		
73	**第七十三条** 本条例下列用语的含义： （一）网络数据（简称数据）是指任何以电子方式对信息的记录。 （二）数据处理活动是指数据收集、存储、使用、加工、传输、提供、公开、删除等活动。 （三）重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。包括以下数据：	本条款是对重要数据的定义。这条定义很有意义，但我委员会认为，网信办应采用列举的方式，进一步说明哪些数据不属于重要数据。 比如，第（三）款第 1 项强调了未公开的政务数据、工作秘密、情报数据和执法司法数据，那么公开的政务数据、工作秘密、情报数据和执法司法数据是否属于重要数据？ 本条第（三）款第 3 项规定，国家经济运行数据、重要产业的商业数据、科研成果数据，都属于被保护或者出口受到管制的重要数据。但是这一规定非常模糊。组织如何判定自己的数据符合上述描述呢？如果这类数据是公开的，还属于重要数据么？ 根据本条第（八）款，即便是在充分公开和自由选择的基础下（比如公开数据处理的目的和手段），用户给予知情同意，单独对每项个人信息的处理给予同意并不会从实质上提升个人信息的保护力度，只会影响客户体验和产品的正常功能。	建议本条第（三）款规定豁免以下情形： 1. 已披露的重要数据或由政府部门提供给企业的重要数据 2. 经邮件获得的未获得同意的重要数据 3. 政府部门公开发布在网上的重要数据 同时，我委会建议政府部门对重要数据进行适当安全分级。数据控制者可能委托数据处理者展开数据处理活动（参本条第（七）款），因此数据控制者（指控制数据并对所收集的数据负责的主体，在本意见稿第六条中称数据处理者）和数据处理者应该有明显的权责区分。委托情形下，数据控制者应该承担法律责任，因为被委托的数据处理者并不清楚数据的全貌，且处理者受到与控制者签署的合同或其他法律文件限制无法访问数据。第（七）款只将委托定义成一种行为，

			但是没有具体说明受委托的主体是否应该承担数据控制者的法律义务。 此外，建议将第（八）款修改为：“单独同意是指数据处理者应就某一数据处理目的所需的某项或某类个人信息取得明确个人同意，不包括一次性针对多种处理目的的同意。”
75	**第七十五条** 本条例自 年 月 日起施行。	应当在最终版的管理条例生效后，为企业设置缓冲期。	考虑到企业合规的重担，建议在最终版的管理条例生效后，设置至少二十四个月的缓冲期，为企业做出必要调整留足时间。 如果不设置缓冲期，建议明确：当企业已在合规方面尽了最大努力，却仍违反了管理条例时，不会被视作违法。