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
《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》的反馈意见

美中贸易全国委员会（下称“我委员会”）谨代表260余家会员企业就《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》（下称“意见稿”）提出意见。我委员会收到的会员企业意见来自包括能源、汽车、信息与通讯技术（ICT）、制造业在内的多个领域。

作为近期实施的《数据安全法》的一项重要配套施行办法，意见稿就工业和信息化领域的数据管理工作做出了澄清，我委员会对此表示欢迎。但与此同时，我委员会及会员企业期待工业和信息化部能积极回应各行业的关切，并考虑以下建议：

简化数据分类分级流程：意见稿的第八、九和十条将一般数据、重要数据以及核心数据明确为企业必须制定合规流程的类别。但由于这些分类所涉表述较为宽泛、模糊，企业在制定合规流程时，可能会面临过重负担；企业的日常运营以及中国境内的客户服务也有可能会被干扰或影响。鉴于本意见稿要求对整合后的数据集进行分类，建议依照《数据安全法》简化这一流程，规避部分法律冲突问题。

确保强制性的政府审查透明、高效：有企业指出，当产品出现问题时，企业需要针对相关事件发布跨境监督报告。在这个过程中，信息和数据的自由流动是基本前提，因为企业需要迅速收集、分析来自世界各地的数据。但是，意见稿第二十四条有关政府对跨境数据转移审查的强制性规定，可能会妨碍、甚至抑制企业完成这一系列必要程序的能力。因此，审查机制的透明、高效对于企业来说尤为重要，也是企业为中国消费者提供安全、即时服务的关键。

不应要求重要数据存储本地化：目前，众多跨国企业都采用了全球化的信息集成系统。这些系统不仅能够高效处理数据，还能帮助企业做出迅速、安全的决策，是企业为客户提供优质服务的重要保障。但是，意见稿第二十四条要求企业将数据集中存储在中国境内的某一个地点。实际上，这么做不仅不利于数据安全，还会影响信息集成系统分享重要数据，削弱企业在面临安全事件或者消费者投诉时的应急处理能力。我委员会希望中国政府妥善考虑与重要数据存储本地化有关的规定，或者以不妨碍企业日常运营为基准，尽量收窄重要数据的定义。

移除本意见稿中关于个人信息的规定：虽然《中华人民共和国个人信息保护法》已经对个人信息做出了明确规定，但在本意见稿中，不少有关数据安全的规定仍然囊括了个人信息。数据安全和个人信息隐私不可被混淆，相关法律在立法目的和监管要求上也有显著差异。目前，意见稿中关于个人信息的规定，可能会增加法律法规管辖范围重合或冲突的几率，以及企业和执法部门对法律产生不同解读的可能性，给合规、执法带来双重负担。如果将意见稿中关于个人信息的部分移除，便能有效规避以上问题。

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

美中贸易全国委员会
2021 年 10 月 29 日

条款号	条款	评价	建议
第三条	工业和电信数据处理者是指对工业、电信数据进行收集、存储、使用、加工、传输、提供、公开等数据处理活动的工业企业、软件和信息技术服务企业和取得电信业务经营许可证的电信业务经营者等工业和信息化领域各类主体。	“企业”的定义和相关范围需要进一步澄清。	建议对“工业企业”给出具体的描述和定义，或提供一个列表或平台，方便企业查询。以帮助企业明确职责范围。
第七条	【分类分级方法】工业和电信数据处理者应当坚持先分类后分级，定期梳理，根据行业要求、业务需求、数据来源和用途等因素对数据进行分类和标识，形成数据分类清单。数据分类类别包括但不限于研发数据、生产运行数据、管理数据、运维数据、业务服务数据、个人信息等。 工业和信息化部按照国家有关规定，根据数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益等造成的危害程度，将工业和电信数据分为一般数据、重要数据和核心数据三级。	这种分类的目的不明确。 关于梳理的时间、标识和目的，没有具体的要求和指引。	对于“一般数据”的处理，应该赋予处理者一定的自由裁量权。

第九条和第十条	【重要数据】危害程度符合下列条件之一的数据为重要数据：（一）对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全； （二）对工业、电信行业发展、生产、运行和经济利益等造成影响； （三）造成重大数据安全事件或生产安全事故，对公共利益或者个人、组织合法权益造成严重影响，社会负面影响大； （四）引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响； （五）恢复数据或消除负面影响所需付出的代价大； （六）经行业监管部门评估确定的其他重要数据。 【核心数据】危害程度符合下列条件之一的数据为核心数据：（一）对政治、国土、军事、经济、文化、社会、科技、网络、生态、资		建议在相关的法律法规中，对于数据分类和定级建立统一而清晰的定义和评估标准，以避免不必要的错误理解。 建议量化或细化数据影响程度的定义，帮助企业进行更准确的评估和数据分类分级。

	源、核安全等构成严重威胁，严重影响海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全相关数据的安全；（二）对工业、电信行业及其重要骨干企业、关键信息 基础设施、重要资源等造成严重影响；（三）对工业生产运营、电信和互联网运行和服务等造成重大损害，导致大范围停工停产、大面积网络与服务瘫痪、大量业务处理能力丧失等；（四）经工业和信息化部评估确定的其他核心数据。		

第十一条	【分类分级工作要求】工业和信息化部组织制定工业和信息化领域数据分类分级、重要数据和核心数据识别认定及数据分级防护等制度规范，形成行业重要数据和核心数据具体目录并实施动态管理，指导开展数据分类分级防 护工作。 地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业数据分类分级防护及重要数据和核心数据识别认定工作，形成本地区行业重要数据和核心数据具体目录并上报工业和信息化部。 工业和电信数据处理者应当建立健全数据分类分级管理制度，将重要数据和核心数据目录报送地方工业和信息化主管部门或通信管理局，并采取措施开展数据分级防护，对重要数据进行重点保护，对核心数据在重要数据保护基础上实施更严格的管理和保护。不同级别数据同时被处理且难以分别采取保护措施的，应当按照其中级别最高的要求实施保护。	根据《数据安全法》，数据处理者无需将重要数据和核心数据目录报送地方有关部门。数据处理者不应负责重要数据和核心数据的目录的制定工作。	1. 建议将第二款调整为，“地方工业和信息化主管部门、通信管理局组织开展本地区工业、电信行业数据分类分级防护工作”，移除对形成目录、上报目录的要求。 2. 行政机关应当明确说明其管理措施是否会要求数据处理者提供数据或允许访问其数据。

第十二条	【重要数据和核心数据备案管理】工业和信息化部建立工业和信息化领域重要数据和核心数据备案管理制度，统筹建设备案管理平台。备案内容包括数据的数量、类别、处理目的和方式、使用范围、主体责任、安全保护措施等基本情况，数据提供、公开、出境、承接，以及数据安全风险、事件处置等情况。 地方工业和信息化主管部门、通信管理局应当分别对本地区工业、电信行业重要数据和核心数据备案内容进行审核，对不符合有关备案要求的，应当督促企业及时完善并重新进行备案。 工业和电信数据处理者应当按照有关要求进行备案，备案内容发生变化的，应在三个月内报备变更情况，同时对整体备案情况进行更新。	《数据安全法》中未对数据备案做任何规定。保证重要数据和核心数据的安全的确很有必要，但建立备案管理制度可能并不是最佳途径。备案制的必要性有待商榷，它可能为政府机构和企业增添不必要的负担。	建议删除本条。

第十四条	【工作体系】涉及重要数据和核心数据的，工业和电信数据处理者应当建立覆盖本单位相关部门的数据安全工作体系，设置专门的数据安全管理责任部门，本单位党委（党组）或领导班子对数据安全负主体责任，主要负责人是数据安全第一责任人，分管数据安全的负责人是直接责任人，明确各部门数据安全职责及人员，建立常态化沟通与协作机制。		当个人可能要承担责任时，应该明确地说明个人将如何以及何时会以个人身份承担责任。此外，应具体说明个人的责任承担方式（比如金额或其他方面）。
第十五条	【关键岗位管理】工业和电信数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。	一些规模较小的企业不需要设立这一岗位。	建议将本条调整为“【关键岗位管理】涉及重要数据和核心数据的工业和电信数据处理者应当确认数据处理关键岗位及人员，签署数据安全责任书，记录数据处理活动。”

第十七条	【数据收集】工业和电信数据处理者收集数据应当遵循合法、正当、必要的原则，不得窃取或者以其他非法方式收集数据。 数据收集过程中，应当采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录。 通过间接途径获取数据的，应当要求数据提供方做出数据源合法性的书面承诺，并承担相应的法律责任。	本条中对必要性原则的体现更适用于收集个人信息的情形，而非收集数据。建议移除有关表述。 在实际运营中，要求企业“对数据收集的时间、类型、数量、频度、流向等进行记录”是不实际的。 不清楚何种行为构成“通过间接途径获取数据”。	解释如何“通过间接途径”获取数据。 建议删除本条关于必要性的要求，将表述调整为，“工业和电信数据处理者收集数据应当遵循合法、正当、~~必要的原则~~，不得窃取或者以其他非法方式收集数据。数据收集过程中，~~应当~~鼓励采取配备技术手段、签署安全协议等措施加强对数据收集人员、设备的管理，并对数据收集的时间、类型、数量、频度、流向等进行记录”。
第十八条	【数据存储】工业和电信数据处理者应当依据法律规定或者与用户约定的方式和期限存储数据。存储重要数据的，还应当采用校验技术、密码技术等措施进行安全存储，不得直接提供存储系统的公共信息网络访问，并实施数据容灾备份和存储介质安全管理。存储核心数据的，还应当实施异地容灾备份。	对这种存储数据有要求的，应进一步说明。	

第十九条	【数据使用加工】工业和电信数据处理者未经 个人、单位等同意，不得使用数据挖掘、关联分析等技术手段针对特定主体进行精准画像、数据复原等加工处理活动。 利用数据进行自动化决策的，应当保证决策的透明度和结果 公平合理。使用、加工重要数据和核心数据的，还应当加强 访问控制，建立登记、审批机制并留存记录。 工业和电信数据处理者提供数据处理服务，涉及经营电 信业务的，应当按照相关法律、行政法规规定取得电信业务经营许可.	获取个人、单位同意的具体要求不明。 比如，对于有 B2B 业务的企业，什么时候需要获取单位同意？获取单位哪一主体的同意（管理人，销售，IT 还是其他？）以及同意具体包含哪些内容？	《个人信息保护法》规定了收集个人信息时需要明示的内容，以及需要获得个人同意的情形。 本条款中还包含了获得单位同意，所以也需要进一步说明相应要求。帮助企业正确地执行，以避免不必要的误解。

第二十条	【数据传输】工业和电信数据处理者应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。传输重要数据的，还应当采取校验技术、密码技术、安全传输通道或者安全传输协议等措施，涉及跨组织机构或者使用公共信息网络进行数据传输的，应当建立登记、审批机制。跨不同数据处理主体传输核心数据的，还应当通过国家数据安全工作协调机制审批。	“跨组织机构”的定义和范围需要进一步澄清。 比如：总公司下属不同分公司之间的数据传输属于跨组织机构吗？	在多个国家/地区拥有运营足迹的跨国企业，通常会对中国境内的运营数据实行集中管理和传输。 考虑到跨国公司可能在中国境内设有不同的分公司，需要明确“跨组织机构”的定义和范围，以避免不必要的误解。 又或者，在具体执法中，建议将跨国公司在中国境内的所有子公司视为“同一组织”，减轻企业进行跨境数据传输时的合规负担。

第二十一条	**【数据提供】**工业和电信数据处理者应当依据行业数据分类分级管理要求，明确数据提供的范围、数量、条件、程序等。提供重要数据的，还应当采取数据脱敏等措施，建立审批机制。提供核心数据的，还应当通过国家数据安全工作协调机制审批。 工业和电信数据处理者应当事先对数据接收方的数据安全保护能力进行核实，并与数据接收方签订数据安全协议，明确数据提供的范围、使用方式、时限、用途以及相应的安全保护措施、违约责任，并督促数据接收方予以落实。	“明确”一词指代的具体行为不清楚。在传输重要数据或者核心数据时，数据处理者是否需要另外聘用有资质的测试评估机构，对数据潜在接收方的安全保护能力进行评估？ 根据第二十六条，委托他人开展数据处理活动的，是否也要遵循上述流程？	
第二十二条	【数据公开】工业和电信数据处理者公开数据应当真实、准确，并在公开前开展安全评估，对涉及个人隐私、个人信息、商业秘密、保密商务信息以及可能对公共 利益及国家安全产生重大影响的，不得公开。	本条似与《中华人民共和国个人信息保护法》第二十五条的规定不一致。根据该法条，“个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外”。	比照现有的隐私和数据相关法律法规修改本条。

第二十三条	【数据销毁】工业和电信数据处理者应当建立数据销毁策略和管理制度，明确销毁对象、流程和技术等要求，对销毁活动进行记录和留存。销毁重要数据和核心数据的，不得以任何理由、任何方式对销毁数据进行恢复。 符合以下情况之一的，工业和电信数据处理者应当销毁相应数据： （一）因业务约定，需要销毁的； （二）个人依据其合法权益请求销毁的； （三）组织基于保护国家安全、社会公共利益目的，且有第三方机构提供证明，请求销毁的。	由于本条没有区分三类数据，这大大增加了企业的义务和潜在合规成本。 此外，根据第二款第三项，组织基于保护国家安全、社会公共利益目的，且有第三方机构提供证明，请求销毁的，工业和电信数据处理者应当销毁相应数据。此处关于“组织”的表述过于宽泛。另外，不清楚哪些“组织”可以请求销毁数据。	建议将 “组织”限定在法律法规授权的一至两个监管部门之内。 “一般数据”是最不敏感的，应该由企业自行酌情处理。
第二十六	【委托处理】工业和电信数据处理者委托他人开展数据处理活动的，应当对被委托方的数据安全保护能力、资质进行核实，确保符合国家、行业主管部门的相关要求，并通过合同约束、现场核查等方式对被委托方落实数据安全保护措施的情况进行监督管理。委托处理重要数据和核心数据的，还应当委托取得相应认证资质的检测评估机构对被委托方进行	厘清“相关要求”可以帮助并指导数据处理者评估和核实第三方的数据处理活动的规范性。	需要明确“相关要求”的具体内容。

	安全评估。除法律、行政法规另有规定外，未经委托方同意，被委托方不得将数据提供给第三方。		
第二十八条	【监测预警机制】工业和信息化部统筹建立工业和信息化领域数据安全风险监测机制，建设数据安全监测预警平台，对数据泄露、违规传输、流量异常等安全风险进行监测和预警，及时组织研判重要数据和核心数据安全风 险并进行预警。 地方工业和信息化主管部门、通信管理局建设数据安全 监测预警平台，组织开展本地区工业、电信行业数据安全风 险监测，按照有关规定及时发布预警信息，通知本地区工业 和电信数据处理者及时采取应对措施。 工业和电信数据处理者应当开展数据安全风险监测，及时排查安全隐患，采取必要的措施防范数据安全风险。		建议工信部就此数据安全风险监测机制的运作过程，以及它将如何影响企业合规提供更多信息。
第三十四条	【监督检查和协助义务】工业和信息化部组织制定数据安全监测接口标准。行业监管部门对工业和电信数据处		建议工信部提供更多“数据安全监测接口”的相关细节，并设置保障机制，杜绝

	理者落实本规定要求的情况进行监督检查。工业和电信数据处理者应当配合行业监管部门依法开展监督检查，并预留检查接口。		接口的不当使用，避免对公司日常运营的干扰。
第三十六条	【保密要求】行业监管部门、其委托的数据安全检测评估机构、及该等部门和机构的工作人员对在履行职责中知悉的工业和电信数据处理者的数据（包括个人信息和商业秘密等），仅可用于履行与数据安全相关之职责，应当严格保密，不得泄露、出售或者非法 向任何第三方提供		原内容上移至第 26 条