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

美中贸易全国委员会对
《中华人民共和国数据安全法（草案）》（二次审议稿）的意见

2021 年 5 月 28 日

美中贸易全国委员会代表 245 余家会员企业，感谢有此机会向全国人大提交关于《中华人民共和国数据安全法（草案）》二次审议稿（以下简称草案）的意见。

我委员会收到的企业意见来自信息和通信技术、专业服务、金融等各个行业。

我们认可全国人大解决部分我们在第一次审议稿的意见中所提及的关切。第二次审议稿解释了中央政府在制定“重要数据目录”中的作用，而且更新了相关条款，与《网络安全法》进一步衔接。具体而言，草案将网络安全等级保护制度写进了数据安全保护条款，肯定了《网络安全法》在跨境数据流动相关议题中的主体地位。

尽管如此，我委员会会员企业的许多关切依然未得到解决，而新加入的个别澄清条款又引发了新的关切。我们理解数据监管的复杂性，期待中国政府有关部门能够破除影响数据自由流动的障碍，确保草案不会给企业增加不必要的负担。我们特别提出以下建议：

1. **管辖范围以及与其他法律的关系：**我们在之前的反馈意见中也曾指出，草案的范围过于宽泛，既包括电子数据，也包括非电子数据，几乎涉及任何与数据相关的商业活动。除此之外，其实现行的一些法律、法规和标准已经涵盖了本草案中的一些国家安全要素，如《网络安全法》、《民法典》、《国家安全法》、《数据安全管理办法（草案）》、《个人信息出境安全评估办法（草案）》。我们希望全国人大确保上述法律法规的监管一致性，减少现行法律法规与本草案的重复之处。我们还建议，将源于国外但在中国处理的数据排除在外，以便让数据范围管理更具实际操作性。

2. **重要数据**：我们坚持认为，草案应进一步明确定义“重要数据”和“重要数据的处理者”，同时限制重要数据风险评估的范围和必要性，从而进一步完善本法案。现行法规要求重要数据应接受数据本地化和跨境安全审查，而《数据安全管理办法（草案）》明确规定大部分企业数据不属于重要数据的范畴。我们因此建议，本草案的定义应与保持一致。我们理解全国人大已经考虑了此前反馈的意见，明确了中央政府将确定重要数据目录。但是，草案仍允许“各地区、各部门”制定各自的重要数据目录，从而增加了各个省市制定不同目录和合规要求的风险，可能会阻碍公司日常运营所需数据的自由流动。因此，我们建议制定重要数据的权力应当集中统一。
3. **跨境数据流动**：草案第 30 条扩大了重要数据出境的限制，超出了《网络安全法》对于关键信息基础设施运营商的限制。跨境数据流动关乎跨国企业与总部沟通以及“了解客户”、反洗钱等日常经营活动。全球范围内的数据自由流动和交换能促进创新和全球经济发展。我们因此建议根据《网络安全法》的规定，减少对关键信息基础设施运营商的重要数据出境限制。
4. **网络安全等级保护制度**：我们认可建立网络安全等级保护制度，并将其作为数据处理活动管理的基础框架，从而使草案与《网络安全法》保持一致。但是第 20 条提出国家应建立数据分类分级保护制度，似乎意味着将同时存在两个不同的数据保护制度。我们建议对该内容进行修订，明确其所指的国家的分类分级数据保护制度即网络安全等级保护制度。
5. **域外适用**：第 2 条规定，在中国境外开展数据处理活动，损害中国国家安全的组织和个人，适用本法。但是并未明确利用何种机制执行此条规定，哪些数据活动可定性为损害中国国家安全。这也导致企业对中国数据和网络监管中越来越多的与国家安全相关的规定和审查表示关切。另外，企业认为，第 2 条提及的问题可以通过《国家安全法》等更适当的法律来解决。我们因此建议删除第 2 条与域外适用相关的内容。
6. **监管**：草案未明确负责监督和执行本法的政府部门，导致可能出现监管重叠与混乱。为避免重复监管，建议草案应赋予不同的政府部门明确的执行和监督职责。

我们再次感谢有此机会提出意见，逐条建议详见下文。

美中贸易全国委员会
联系人：闫羽
010-6592-0727

条款号	条款	评价	建议
2	在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。 在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。	1. 数据处理活动的定义较为广泛，也可能包括常规的商业数据活动。如果在中华人民共和国境内的人员处理存储在中华人民共和国境外的数据，是否也适用于本法？需要进一步的解释 2. 域外效力的规定施行于未在中国经营或未处理中国数据的实体过于宽泛。如此宽泛的域外效力规定与国际法和国际条约相悖。 3. “安全监管”的具体指是什么？是否指第三条所定义的“数据安全”及第七条所指的承担数据安全监管职责行政部门?	1.我们恳请该条款能采用界限更为清晰，更具有可操作性的范围应用，例如，关注存储在中华人民共和国境内的数据处理活动。 2. 删除“安全监管”，若该文意与下文数据安全监管相同，则建议用同样的表达。
10	第十条 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。		建议将第 10 条设置为反垄断法下的豁免条款。
17	国家促进数据安全检测评估、认证等服务的发展,支持数据安全检测评估、认证等专业机构依法开展服务	1. 什么机构应被授权开展“数据安全检测评估、认证”等服务？该服务应在什么条件下提供？ 2. 就相关服务做出具体规定、定义和条件。明确授权服务提供方和授权方式。	建议就相关服务做出具体规定、定义和条件。明确授权服务提供方和授权方式。
18	国家建立健全数据交易管理制度,规范数		1. 建议添加如下定义：

	据交易行为,培育数据交易市场。		“数据交易管理制度”是对一个实体或个人将其从第三方获得的重要数据以商业销售或许可的方式提供进行管理的制度。 2. 建议明确对于交易记录的具体规定及保留期限
20	国家建立数据分类分级保护制度,根据数据在经济社会发展中的重要程度,以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用,对国家安全、公共利益或者公民、组织合法权益造成的危害程度,对数据实行分类分级保护,并确定重要数据目录,加强对重要数据的保护。各地区、各部门应当按照数据分类分级保护制度,确定本地区、本部门以及相关行业、领域的重要数据具体目录,对列入目录的数据进行重点保护。	1. 我们希望明确此条款中的“重要数据”与《网络安全法》第 37 条“重要数据”是否相同。不同法律法规的“重要数据”标准和定义应当保持一致。 2. 我们注意到，第 20 条中的数据分类分级保护制度与第 26 条中的网络安全等级保护制度可能存在重合与混淆。第 20 条要求国家建立数据分类分级保护制度，而第 26 条规定，根据《网络安全法》建立的网络安全等级保护制度应当成为数据安全管理的基础框架。这两条所指的是否都是网络安全等级保护制度。如果不是，有可能形成两个平行的数据风险管理分类制度， 从而造成不必要的复杂性。 3. 将权力下放给地方政府，允许其确定各自的“重要数据”保护目录，可能会导致合规要求混乱，阻碍中国境内不同地区间的数据自由流动。	1. 确定重要数据范围和定义的权力应当统一集中。 2. 如果无法集中，主要的行业监管部门应负责制定该行业的重要数据目录，如中国人民银行负责制定金融行业的重要数据目录。 3. 明确数据分级分类标准是否与现行行业和国家标准一致，如《工业数据分类分级指南（试行）》 《证券期货业数据分类分级指引》 (JR/T 0158-208)，以及《金融数据安全分级指南（草案）》等。 4. 明确多个行业共有的数据类型如何分类分级。 5. 对本条进行修订，明确 “数据分级分类保护制度”就是“网络安全等级保护制度”，从而与第 26 条保持一致。
21	二十一条 国家建立集中统一、高效权威	1. 建立集中统一、高效权威的数据安全风	1. 建议最后加一句话，“国家

	的数据安全风险评估、报告、信息共享、监测预警机制,加强数据安全风险信息的获取、分析、研判、预警工作。	险评估、报告、信息共享、监测预警机制的立法用意是好的，但是实施起来可能会有问题。安全策略对每个企业而言都是极度保密的，如果要求企业都将相关信息互为分享，可能造成不必要的担忧。	在建立该机制时应保护企业的商业秘密。”
23	国家建立数据安全审查制度,对影响或者可能影响国家安全的数据处理活动进行国家安全审查。 依法作出的安全审查决定为最终决定。	1. 什么层级的什么授权机构有权作出最终决定？ 2. 如何判定数据 处理活动影响或者可能影响国家安全？ 3. “数据安全审查制度”和网安法下的“网络安全审查制度”有什么关系？ 4. 国家安全审查的具体内容（如：国家安全审查的审查机构、启动审查的条件、审查范围）均未明确。 5. “依法作出……”有待后续出台详细的实施细则为审查机构的审查工作提供法律依据。 6. “……为最终决定”未能给审查对象提供救济途径，缺乏公平性。	1. 数据安全审查仅限于已在最高保护级别正确编目和分类的重要数据。 2. 建议尽快出台有关国家安全审查制度的实施细则，明确国家安全审查的审查机构、启动审查的条件。 3. 建议删除最后一句“依法作出的安全审查决定为最终决定。
25	二十五条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等		如前面对二十条及三十条评论所提及的，对互惠贸易的限制将最终导致与

	方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的,中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。		本法第五条中设立的数据自由流动、促进以数据为关键要素的数字经济发展的目标相冲突。具体请参考上述对第二十条、第三十条评论中对 WTO 义务的讨论。
26	开展数据处理活动应当依照法律、法规的规定，在网络安全等级保护制度的基础上，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。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。	目前等保的范围仅限于数据存储在中华人民共和国境内的系统和应用。所以我们认为只要遵循等保定义的范围和要求，即可视为符合本条款要求。	为了避免重复的工作量及额外的管理负担，我们建议直接采纳等保定义的范围和要求，而无需另外建立一套数据安全管理制度。
28	第二十八条 开展数据处理活动应当加强风险监测,发现数据安全缺陷、漏洞等风险时,应当立即采取补救措施;发生数据安全事件时,应当立即采取处置措施,按照规定及时告知用户并向有关主管部门报告。	1. 如我们对第 14 条的评论所述，“单独同意”的定义和适用不明确。具体而言，如果个人信息处理者已获得主体的同意，是否需要从主体处获得额外的“单独同意”？ 2.向他人提供个人信息需要“单独同意”的要求不可行或不必要，特别是当个人信息（如与企业员工履职相关的商业联系信息）作为企业数据的一部分提供且该个人信息对任何个人不敏感的情况下。	1. 建议修改为“开展数据处理活动应当加强风险监测,发现数据安全缺陷、漏洞等风险时,应当立即在其发现数据安全事件时采取补救措施;发生确定存在数据泄露的数据安全事件时,若该事件会实质性的损害数据源，应当按照规定及时告知数据源并向本地主管网络安全的公安机关报告。数据泄露指重要数据被第三方未经授权访问和/或泄露。” 2. 建议明确相关报告具体要求。

30	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重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定;其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。	第 29 条中的重要数据处理活动定期风险评估及评估报告报送要求是否与《网络安全法》或《个人信息保护法（草案）》中的数据出境安全和风险评估要求一致。	我们建议尽量缩小限制数据出境的范围。
32	从事数据交易中介服务的机构在提供交易中介服务时,应当要求数据提供方说明数据来源,审核交易双方的身份,并留存审核、交易记录。		建议明确相关记录保留期限应为多久。
35	第三十五条 中华人民共和国境外的司法或者执法机构要求调取存储于中华人民共和国境内的数据的,非经中华人民共和国主管机关批准,不得提供;中华人民共和国缔结或者参加的国际条约、协定有规定的,可以按照其规定执行。	1. 本条的适用范围很宽，包括了所有类型的境外诉讼和所有存储在中国境内的数据（无论是在中国境内或境外采集或生成的数据）。这是否会严重影响跨境贸易的争议解决并对数据进口造成不必要的担忧。 2. 哪个“主管机关”将有权做出批准？ 3. 后半句规定“中华人民共和国缔结或者参加的国际条约、协定有规定的 ,可以按照其规定执行”如何执行？“主管机关”的批准在这种情形下，仍然需要？ 4. 前半句，建议将“存储于中华人民共和国境内的个人信息”修改为“采集并存	1. 建议明确“主管机关”是哪个机关。 2. 后半句，建议修改为“中华人民共和国缔结或者参加的国际条约、协定有规定的 ，应按照其规定执行”。

		储于中华人民共和国境内的个人信息”。	
44	开展数据处理活动的组织、个人不履行本法第二十六条、第二十八条、第二十九条、第三十条规定的数据安全保护义务的,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;拒不改正或者造成大量数据泄露等严重后果的,处五十万元以上五百万元以下罚款,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五十万元以下罚款。	1. 对违反本法的直接责任人员进行罚款无异于让一家公司的员工都承担责任，因此将难以执行。另外，这些处罚对于首次违法行为并不相当。 2. 允许有关部门违法企业责令停业、吊销业务许可证的权力过于宽泛，可能会限制企业交易。	我们建议：1.取消对个人和员工的处罚。2.取消允许责令停业或吊销业务许可证的权力。
49	第四十九条 开展数据处理活动危害国家安全、公共利益，排除、限制竞争,或者损害个人、组织合法权益的,依照有关法律、行政法规的规定处罚。	如何将第十条中规定的行业组织制定数据安全行为规范及会员指导活动与第四十九条规定的限制竞争的处罚相协调？	
53	第五十三条 本法自 年 月 日起施行。		我们建议本法设置 24 个月的过渡期，给予各行业企业充足时间，做好执行准备。