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
《中华人民共和国个人信息保护法（草案二次审议稿）》的反馈意见

2021 年 5 月 28 日

美中贸易全国委员会（以下简称“我委员会”）谨代表 240 多家会员企业，感谢有此机会就《中华人民共和国个人信息保护法（草案二次审议稿）》（以下简称“《草案》”）向全国人大提交建议。我委员会赞赏中国政府在强化个人信息保护，以及给予企业清晰的指导意见方面所做出的努力。

我委员会已收到受《草案》影响的多个行业的会员企业的来函意见。首先，我委员会赞赏《草案》强调通过明确个人信息收集者、加工者、以及处理者的标准，来建立一个强有力的隐私制度。《草案》还为发生信息泄露时的最佳实践提供了指引，并为收集数据时取得用户同意的基本要求方面做了概述。

与此同时，我委员会及会员企业期望网信办将对可能影响美企的若干问题的反馈纳入考量，尤其是和上一稿保持一致、没有做出调整的条款。本次反馈意见中的重点内容如下：

- **与国际惯例的一致性：**我委员会建议《草案》立法者尽可能与其它国际框架保持一致。这将确保跨国企业在多个司法管辖区遵守个人信息保护的要求时，法律得以平稳施行。在强化个人隐私保护的同时，也促进商业的稳健发展。
- **信息存储本地化规定：**第四十条包含的信息存储本地化的规定与包括欧盟的《通用数据保护条例（GDPR）》以及美国加州的《加州消费者隐私保护法案（CCPA）》在内的其它国际框架不一致。相关规定对公共部门和私营部门的利益起到适得其反的效果，因此应被给予重新考虑。这些规定会抑制行业发展，降低互联网安全和风险管控的有效性。因此，我委员会强烈建议移除该项规定。另外，考虑到企业收集的个人信息种类各异，所涉风险大小不同，信息“数

量”并非确定风险的有意义的方法。不应该对信息处理的数量设置门槛，或借此判断信息处理者是否应当将信息存储在境内。

- **跨境数据传输：**根据第三十八条第三款规定，个人信息的跨境传输需要中国境内的个人信息提供方按照网信办制定的标准合同与境外接收方订立合同。我委员会建议移除此项规定，或者网信办建议的标准合同符合国际惯例（例如欧盟《标准合约条款》）；如果采纳此类标准合同，我委员会要求为其设置 24 个月的过渡期，并为建议的标准合同公开征集意见。
- **个人信息收集的法律依据：**根据第十三条，取得个人同意是收集个人信息的首要法律基础。我委员会建议额外增设同意规定的例外情况，包括“合法利益”并/或涉及尽职调查、法律申索、引荐、安全、以及处理业务联系信息的使用案例。在包括新加坡、巴西、韩国的众多司法管辖区内，“合法利益”是收集个人信息的法律基础。这些例外规定将为应对日益复杂的信息环境的企业提供更宽广的运营空间。
- **要求单独同意理由不充分：**根据第二十四条，个人信息处理者与任何“其他方”共享数据时，每次都需要重新取得个人同意。考虑到企业可能需要经常在其子公司或公共机构之间共享数据，这项规定可能较难执行。当个人信息处理者已经依赖其他法律基础——例如，履行合同义务或者其它法律义务——获取个人信息时，要求其每次取得个人的同意是不切实际的。为解决这一障碍，我委员会建议第二十四条明确允许在未经个人的单独同意的情况下也可以向第三方披露信息的条件。这些情况可能包括为履行合同、法律、公共卫生、以及紧急情况的义务而需要披露信息的时候。另外，我委员会建议在将向个人告知的内容改为信息接收方的类别，而非直接告知接收方的真实名称。这种方法既能减轻企业负担，又能让用户在了解自身信息如何被使用时获得更具可操作性且有价值的资讯。这一调整与欧盟《通用数据保护条例（GDPR）》的规定保持一致，对于信息处理者和个人来说都更为友好。
- **过度繁重的通知规定：**第五十六条规定，个人信息处理者发现所有个人信息泄露，都应当通知履行个人信息保护职责的部门和个人。这一条文的适用门槛过低，宽泛的报告机制还可能导致过度报告，增加监管者和企业的管理负担。我委员会建议根据泄露可能造成的风险程度采取相应措施，仅在信息泄露可能造成重大损害时才要求强制通知，这种做法还可以让各个组织和监管部门将资源有效聚焦在具有真正风险的问题上。

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

附件：

条款号	条/款	意见	建议
1	为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，制定本法。	1. 在第一次征求意见稿中，本条的表述为“规范个人信息处理活动，保障个人信息依法有序自由流动，促进个人信息合理利用”；根据这一版本，“保障个人信息依法有序自由流动”的表述被删除了，但在同一天公示的《中华人民共和国信息安全法》第二稿征求意见稿中仍然保留。不清楚在本法中将这段文字删除的理由，以及相关影响。 2. “促进个人信息合理利用”表意不明。	1. 除非有特殊原因，建议恢复第一稿中的描述，保留“保障个人信息依法有序自由流动”。 2. 明确定义“促进个人信息合理利用”，或删除此表述。
3	第三条 组织、个人在中华人民共和国境内处理自然人个人信息的活动，适用本法。 在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法： （一）以向境内自然人提供产品或者服务为目的； （二）分析、评估境内自然人的行为； （三）法律、行政法规规定的其他情形。	第三条第二款指出“分析、评估境内自然人的行为”适用本法。这一表述过于宽泛，可能包括很多本不该属于本法管辖范围的行为。例如，如果依字面狭义解释，在中国境内阅读新闻报道的行为也可以适用本法。 此外，本法目前给出的定义并没有明确指出企业内部处理个人信息或者托管于中国境外的应用软件处理中国公民个人信息的情形是否适用本法。	本草案中，第三条第二款旨在针对大数据分析和采样的使用。 建议缩小第三条第二款的适用范围，改为“以采样为目的，利用大数据分析来分析、评估境内自然人的行为”。

4	第四条 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。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。	正如我们在上一稿中所建议的，本条对个人信息的定义包含了那些使用于商业场景的信息，如名片上的商业联系信息（例：商业电子邮件地址、办公室直线、职务等）。这与现有法规（如《征信业管理条例》）的规定不一致，也会在执法上造成冲突。 在实践中，与企业员工履行职责有关的信息（如商业联系信息）总是包含在企业数据中，特别是企业信用报告与评级服务、企业数据服务、企业风险控制服务、供应商管理服务等各方面。如果个人信息的定义没有赋予个人信息处理者依照本草案第十三条的规定依法处理该信息的权利，并且总是需要主体同意，则会给个人信息处理者带来不必要的困难，危及数据服务，特别是企业数据服务和信用报告及评级服务业发展。	1. 重新定义个人信息，使其与现行法律法规保持一致。例如，将“企业董事、监事、高级管理人员与其履行职责有关的信息”排除在个人信息定义之外。 2. 如有必要保留现有定义，可参考新加坡《个人数据保护法令》设置一个例外条款，即授权个人信息处理者在处理与履行职责有关的商业联系信息时，无需获得有关个人的同意。 3. 澄清已故人士的信息是否属于“个人信息”。
10 (&42)	第十条 任何组织、个人不得违反法律、行政法规的规定处理个人信息，不得从事危害国家安全、公共利益的个人信息处理活动。 第四十二条 境外的组织、个人从事损害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，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	1. 如何界定“从事危害国家安全、公共利益的个人信息处理活动”却又未构成“违反法律、行政法规的规定处理个人信息”的情形？按照第七十条的规定，该等情形应该已经包含在违法行为条款中了。 2. 第十条已经明确禁止了“从事危害国家安全、公共利益的个人信息处理活动”，在此情形下，第四十二条的规定还是否适用？	1. 删除或明确界定何为“从事危害国家安全、公共利益的个人信息处理活动”。 2. 澄清第十条和第四十二条之间的关联。

	告，并采取限制或者禁止向其提供个人信息等措施。		
13	第十三条 符合下列情形之一的,个人信息处理者方可处理个人信息： （一）取得个人的同意； （二）为订立或者履行个人作为一方当事人的合同所必需； （三）为履行法定职责或者法定义务所必需； （四）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； （五）依照本法规定在合理的范围内处理已公开的个人信息； （六）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； （七）法律、行政法规规定的其他情形。 依照本法其他有关规定，处理个人信息应当取得个人同意，但有前款第二项至第七项规定情形的，不需取得个人同意。	欧盟《通用数据保护条例（GDPR）》中提及的“合法利益（legitimate interest）”，或者新加坡《个人数据保护法令（PDPA）》中提及的“业务改进（business improvement）”，可以视为与本条具有同等效力的国际标准。具体而言，欧盟《通用数据保护条例（GDPR）》在严格规定个人信息处理者要取得个人同意的同时，还认可“合法利益”作为处理信息的有效理由。 本条规定中没有将“合法利益”纳入处理个人信息的有效理由，这可能会损害中国境内处理个人信息的个人和中小企业的利益。对企业而言，在从事一些必要且合理的信息处理活动时将会无法可依，例如： 1) 雇主处理雇员信息。例如，当企业需要以培训为目的处理雇员个人信息时，雇佣合同中没有相关规定，因此以“在履行协议的基础上”为由是不合法的，但也不能根据雇员的自由意愿来处理信息。 2) 个人信息处理服务中包括非合同当事人的信息。 此外，根据本条第五项，“依照本法规定在合理的范围内处理已公开的个人信息”无需取得个人同意。然而，如何界定“合理范围	我们建议扩充不需取得个人同意便可处理个人信息的情形，涵盖“合法利益”的情形并/或尽职调查、诉讼、引荐、安全和处理商业联系信息等情形。 “合法利益”已在多个法域中被认定为合理的豁免个人同意的情形。具体可参见新加坡、巴西、韩国等国规章，以及香港《个人资料（隐私）条例》第八部分。

		内”并不明确，该项存在宽泛解释或滥用的风险。	
14	第十四条 处理个人信息的同意，应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。 个人信息的处理目的、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。	在本条中涉及三类“同意”：明确作出的同意、单独同意和书面同意。 然而，这三类同意之间的区别不明确，与现有法规和国家标准中关于“同意”的界定不一致。	建议第二款修改为，只有在个人信息处理目的和变更后与原先信息处理方式不一致，或原先取得的个人同意只在原先的信息处理条件下合理的情况下，才应当重新获取个人同意。 明确定义“明确作出的同意”“单独同意”和“书面同意”这三个概念。
21	第二十一条 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应当约定各自的权利和义务。但是，该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。 个人信息处理者共同处理个人信息，侵害个人信息权益的，应当承担连带责任。	本条没有做出改动。仍不清楚有两个以上的个人信息处理者时，如何认定连带责任。	建议只有在两个以上的个人信息处理者没有约定各自权利义务或约定根据实际相关情况认定各自责任的情形下，才考虑连带责任。
24	第二十四条 个人信息处理者向他人提供其处理的个人信息的，应当向个人告知接收方的身份、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。接收方应当在上述处理目的、处理方式和个	1. 第二十四条中对“个人信息处理者向他人提供其处理的个人信息的”的范围限定并不明确。“供其处理的个人信息”是否仅限于数据再加工？是否包括数据出售？不作为出售的数据分享？	1.我们建议 明确本条适用范围，厘清“个人信息处理者向他人提供其处理的个人信息的”意涵。将相关表述调整为，符合第十三条中列举的任一情形的，个人信息处理者可以向第三方公开信息。

	人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。	很多情形下，例如个人信息处理者已经为履行合同或者其它法律义务处理个人信息时，再要求其取得个人同意，是不切实际的。同理，如果原先的处理目的、处理方式变化时，需要重新取得个人同意，在实践中也会有困难。例如，接收方可能已经与个人信息处理者订立了合同，要求信息处理者在此类情形出现时履行告知义务，而不是由接收方重新取得个人信息主体的同意。 本条与第十三条规定冲突。本条忽视了个人同意不应基于信息处理机构是否告知个人有关信息公开的必要细节，而应基于其他单独的法律根据。为了避免冲突，应将本条调整为“当信息处理者依法委托第三方处理个人信息时，个人信息处理者无需再次取得单独同意”。 2. 由个人信息处理者向个人告知每个接收方的身份、联系方式、及信息处理方式，是不切实际的。当个人信息处理者委托一第三方机构代表自己处理个人信息时，信息处理者会订立合同以确保第三方保障个人信息安全并在个人信息处理者的指导下处理信息。本法不应要求第三方直接联系个人信息主体 3.要求变更原先信息处理目的和方式的接收方直接取得个人对进一步公开信息的同意并不现实。建议澄清表述，当接收方要变更原	即，“符合以下情形之一的，个人信息处理者向第三方公开信息时，不需要取得个人同意： （一）为订立或者履行个人作为一方当事人的合同所必需； （二）为履行法定职责或者法定义务所必需； （三）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。” 第三方无需直接联系个人信息主体。 2. 建议将个人信息处理者向个人告知的内容改为接收方类别，而非接收方的具体身份信息，从而与包括《通用数据保护条例（GDPR）》在内的国际惯例保持一致。 3. 建议明确规定，当一个主体向另一个主体公开个人信息时，如果信息接收方（个人信息处理者）要求进一步公开信息，仅需取得公开方的同意（无需联系个人信息主体）；再由信息公开方负责取得个人同意。

		先的处理目的、处理方式时，接收方可以依凭信息公开方（原个人信息处理者）所提供的个人同意，而信息公开方（通常与与个人信息主体有雇佣或其它关系）应当负责取得个人同意。	
24	第二十四条 个人信息处理者向他人提供其处理的个人信息的，应当向个人告知接收方的身份、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。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。	1. 第十四条和本条中关于“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。当个人信息（如与企业员工履职相关的商业联系信息）是企业数据的一部分，提供该个人信息对任何个人都不敏感时，无需设置单独同意。	建议将“与该个人履行职责相关的信息如商业联系方式”作为本条“单独同意”的例外情形。
25	第二十五条 利用个人信息进行自动化决策，应当保证决策的透明度和结果公平合理。 通过自动化决策方式进行商业营销、信息推送，当同时提供不针对其个人特征的选项，或者向个人提供拒绝的方式。 通过自动化决策方式作出对个人权益有重大影响的决定，个人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。	本条的适用门槛不清楚。不知何时应当保证利用个人信息进行的自动化决策透明、结果公平合理。 根据第七条，公开、透明是适用于所有个人信息处理活动的原则，但是本条特别指出“应当保证处理结果公平合理”。 现代人工智能及算法犹如黑匣子，具有高度的不确定性，决策过程“难以解释”，对结果做出规定是不合理的。 此外，本条第三款规定，通过自动化决策方式作出对个人权益有重大影响的决定时，个	将本条表述调整为“仅在自动化决策对个人产生重大影响，或侵害个人合法权益时，排除自动化决策”。 此外，建议为本条增设以下例外情形： 1. 取得个人信息主体同意的； 2. 根据合同规定，具有必要性的； 3. 法律、行政法规规定的其他情形。 以上建议符合欧盟《通用数据保护条例（GDPR）》等国际惯例。

		人有权要求个人信息处理者予以说明并拒绝个人信息处理者仅通过自动化决策的方式作出决定。但在实际操作中，“对个人权益有重大影响的决定”的具体意义并不明确。	
27	第二十七条 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。 所收集的个人图像、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，取得个人单独同意的除外。	“公共场所”的概念不明确。 公司是否可以使用监控摄像头来保护自己的财产，避免在工厂或办公区发生盗窃？	
28	第二十八条 个人信息处理者处理已公开的个人信息，应当符合该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，应当依照本法规定取得个人同意。 个人信息被公开时的用途不明确的，个人信息处理者应当合理、谨慎地处理已公开的个人信息。利用已公开的个人信息从事对个人有重大影响的活动，应当依照本法规定取得个人同意。	和上一版本相比，本条没有做出改动。本条没有充分考虑到对于“已公开的个人信息”或者可以公开获得的个人信息，取得个人同意是不实际的。因为这类信息已经丧失了时效性，取得信息主体的同意需要付出极大的努力。	本条在规范此类信息的处理时，考虑到个人信息及信息处理的性质，个人信息主体的合理期待，以及个人信息控制方的地位，应当允许援引其它法律依据，而不是将个人同意作为依据。
30	第三十条 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。	在商业活动中，一方商业主体有可能向另一方提供一定的敏感个人信息。此时要求接收方直接联系个人取得同意，是不切实际的。	建议明确规定，接收方在处理个人信息时，可以向信息公开方征求同意，再由信息公开方（与个人信息主体系雇佣或其它关系）负责取得个人同意。

	法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。		
38	第三十八条 个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当至少具备下列一项条件： （一）依照本法第四十条的规定通过国家网信部门组织的安全评估； （二）按照国家网信部门的规定经专业机构进行个人信息保护认证； （三）按照国家网信部门制定的标准合同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； （四）法律、行政法规或者国家网信部门规定的其他条件。	本条规定显著扩大了数据本地化的实施范围，大量非关键信息基础设施运营者所收集产生的个人信息也将面临数据本地化要求。而根据《中华人民共和国网络安全法》第三十七条，只有“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”。 全球运营的跨国企业通常借助其在中国境外的统一的信息系统来保存处理在中国境内的分公司或者子公司雇员的个人信息。本条相关措施会使得跨国企业不必要的管理负担和运营成本大幅增加。因此，建议将企业处理雇员个人信息和非雇员相关信息的情形区分开来，并考虑允许跨国企业以更简便易于操作的方式处理雇员个人信息。 另外，需进一步澄清“向中华人民共和国境外”提供个人信息的定义。跨国企业中通常借助在全球不同国家的技术人员提供 IT 系统维护和运营支持。因此，在一个法域内的技术人员可能会在不进行实体或电子个人信息跨境传输的情况下，拥有另一个法域内的信息/计算机系统的访问权。	建议如下： 1. 明确定义符合“向中华人民共和国境外提供个人信息的”情形。 2. 为本条的一般性规定增设一些特殊的豁免情形。例如，为履行义务提供信息，提供的个人信息与个人信息主体履行商业合同相关，属于企业信息，或为企业安全调查所需要的信息。 3. 增设个人信息处理者因业务需要或其它需求，可以向中华人民共和国境外提供个人信息的条件。例如： 1) 在集团内部遵循公司既有规定传输个人信息； 2) 个人信息接收方的信息保护标准等同于或者高于《中华人民共和国个人信息保护法》中的保护标准。 4. 明示国家网信部门组织的安全评估的内容、要求、具体标准。 5. 列举有资质进行个人信息保护认证的专业机构名单。 6. 解释第三十八条与第三十九条之间的联系。在已设立第三十八条成立的基础上，应取消第三十九条中“取得个人的单独同意”的要求。因为个人信息处理者如果不具备

			相应条件，基本没有可能向境外提供个人信息。这一规定也无益于保护个人信息主体的权利。
38.3	（三）按照国家网信部门制定的标准合同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；	根据第三十八条第三款，跨境数据传输需要中国境内的个人信息提供方和境外接收方，按照网信办制定的标准合同，订立合同。鉴于网信办属于中国政府，标准合同很有可能是中文的。但是本条中的境外接收方很可能并不具有中国籍，或不是中国境内的企业。这份中文版的标准合同也可能无法适用于其它国家。 此外，个人信息处理者因业务需要或其它需求，向中华人民共和国境外提供个人信息的时，至少需要具备一个条件，但本条一共只列举了三个条件可供满足。	我们建议： 1. 移除第三十八条第三款。 2. 如不移除，可以将第三款表述修改为“与境外接收方订立合同，约定双方的权利和义务，并监督境外接收方的个人信息处理活动达到本法规定的个人信息保护标准”，与上一版本保持一致。 3. 如不移除，可以附上一份与国际标准一致的草拟版标准合同供订立合同的双方参考。建议网信部门提供的标准合同，从形式和内容上均与欧盟的《标准合约条款》保持高度一致。部分企业已经按照欧盟条款订立了相关规定，这样可以帮助企业维持内部规定的一致性，统一规范它们在集团内部的和涉及第三方的跨境数据传输活动。 4. 如准备出台“标准合同”，应从本法律生效且标准合同出台时起，设置至少 24 个月的过渡期。同时，草拟版的标准合同也应该公开征集意见。
39	第三十九条 个人信息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接收方的身份、联	第三十九条是个人信息处理者向中国境外提供个人信息时，应当服从的各项规定。但本条与第二十四条、第三十八条的关系并不清	1. 移除本条关于“取得个人单独同意”的规定：

	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接收方行使本法规定权利的方式等事项，并取得个人的单独同意。	楚。例如，当一个中国境内的组织委托一个外国主体处理个人信息时，中国境内的组织是否需要承担本条列举的责任？当企业需要向境外提供个人信息时，是否需要同时满足第三十八条和第三十九条中所有平行出现的规定？ 而且，对于个人信息跨境传输而言，“取得单独同意”的严苛要求既不必要，也不实际。在欧盟《通用数据保护条例（GDPR）》的框架下，关于取得个人同意的要求不是一般性条款，而是例外规定。但在本草案中，第三十九条更像是对第三十八条的补充。这两条针对跨境数据的规定将会影响中国各行各业的发展。 在法律施行阶段，如果企业为履行商业合同中所规定的权利义务提供个人信息，还必须取得“单独同意”，会对企业与外界的联通造成不必要的阻挠，影响跨境交易的透明度。 “向个人告知境外接收方的身份”也是不实际的，因为跨国企业拥有众多数据接收方数，且接受方的名单会随着各类商业需求发生变动。考虑到未来的接收方是无法预知的，部分企业可能需要不断地更新接受方名单，并向个人告知最新变动，这无疑会成为它们的负担。	1) 将第十三条第二项“为订立或者履行个人作为一方当事人的合同所必需”应用于此处个人信息跨境传输的情形。 2) 将“取得个人单独同意”作为例外规定，仅在个人信息处理者不具备第三十八条中列举的条件时适用。 3) 当企业为履行商业合同中所规定的权利义务提供个人信息时，仅要求在涉及“个人信息”时取得个人同意；或者将企业提供“商业联系信息”设为要求取得个人同意的例外情形。 2. 如不移除第三十九条，建议合并第三十八条与第三十九条。规定企业只要具备其中任一条件，即可向境外提供个人信息。 3. 与《通用数据保护条例（GDPR）》相关规定保持一致，将向个人告知的内容改为“信息接收方的种类”，而非直接告知实际接收方的真实信息。
40			

	第四十条 关键信息基础设施运营者和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，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。 确需向境外提供的，应当通过国家网信部门组织的安全评估；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. 与欧盟《通用数据保护条例（GDPR）》，新加坡《个人数据保护法令（PDPA）》以及其他国家或地区的个人信息保护法律相比，本法关于数据本地化的要求和跨境传输的限制过于严苛。这些规定并不能解决信息安全问题，因为信息是否安全与存储地点无关。 此外，本条关于跨境数据传输的规定将非关键信息基础设施运营者也纳入了规制范围，这与《网络安全法》相冲突。 数据本地化要求会对跨国企业的全球运营和未来在华投资造成负面影响。在全球贸易的背景下，数据的自由流动至关重要。安全评估以及任何阻碍数据流动的规定都会扰乱跨国企业的日常运营，甚至导致暂时性的商业关停。限制中外民众在商业、公共事件、体育赛事、文化、电影等方面的信息交流，也会让中国与世界脱钩。数据本地化所带来的这种高度不确定性、付出巨额代价的风险，以及对商业造成的不可逆打击，可能让跨国企业逐渐远离中国。 2. 将处理的个人信息“数量”作为门槛评判个人信息处理者地位的相关规定，与国际惯例不一致。考虑到个人信息的种类众多、性质各异，信息量并不是一个有价值的风险评判	建议如下： 1. 移除本条中的如下要求。 1）关于数据本地化的要求。 2）移除本条中政府关于信息处理达到“规定数量”后应当将信息存储在境内，并通过安全评估的要求。如移除以上内容较为困难，建议设立一个合理的、公开的“数量”门槛。 2. 应确保传输至境外的数据被充分保护。 3. 应为法律施行设立合理的过渡期。 4. 在本条中补充说明除了通过安全评估之外的跨境信息传输机制，来增强规定的灵活性。

		指标。也不清楚这里的“数量”是指一个组织存储的信息量，还是传输的信息量。对于已公开的商业个人信息而言，数量多少更是不值一提。根据第五十二条，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。不清楚这两处关于数量认定的门槛是否统一，也不清楚这两处规定是否出于对同一问题的考量。 3. 根据本条，向境外提供个人数据的，应当通过国家网信部门组织的安全评估。但不清楚必须展开评估的最低门槛。 此外，从法律角度也可以解释“在中国境外存储个人信息，同时不危害国家安全或个人权益”的情形。例如，某一跨国组织可能需要将某位雇员的部分信息传输至总部，来帮助组织实现更高效地人力资源安排和管理。在此类情形下，很难限制在中国境外存储个人信息的行为。	
41	第四十一条 中华人民共和国境外的司法或者执法机构要求提供存储于中华人民共和国境内的个人信息的，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. 本条适用范围过于宽泛。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）都可以涵盖在内。这一规定可能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. “主管机关”指代不明。	1. 将“存储于中华人民共和国境内的个人信息”的表述调整为“采集并存储于中华人民共和国境内的个人信息”。 2. 明确“主管机关”。

		3. 根据本条，“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”表述不充分。在这种情形下提供个人信息是否仍需经过“主管机关”批准？ 4. 主管机关批准的流程不明确，关键时限和例外情况不清楚。	3. 将本条相关表述调整为“中国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”。
42	第四十二条 境外的组织、个人从事损害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，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。	本条指出国家网信部门可以将境外组织列入限制或者禁止个人信息提供清单，但未说明相应的申诉程序。	应该为被列入清单的组织设置申诉程序。
44-50	第四章 个人在个人信息处理活动中的权利	草案第四章，即第四十四条至第五十条说明了个人权利，但没有限制个人权利。限制个人权利的必要性包括但不限于：保护公共利益，保护他人的权利，或其它合法理由。根据第五十条，“拒绝个人行使权利的请求的，应当说明理由”。这表明在某些情形下，可以拒绝个人行使权力的请求。但由于本条规定较为模糊，施行层面可能会遇到阻碍。	为第四十五条增设例外条款。允许个人信息控制方将重复、多余、费力的申请设为例外情形。例如，当一名企业（前）员工要求获取与他相关的所有邮件的备份。建议针对此类行为列举一系列组织无需回复个人请求的情形。
52-53	第五十二条 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	第五十二条和第五十三条规定，特定个人信息处理者要“将有关机构的名称或者指定代表的姓名、联系方式等报送履行个人信息保	个人信息保护负责人和指定代表均为组织或部门任命。因此，应移除对任命人员信

	对个人信息处理活动以及采取的保护措施等进行监督。 个人信息处理者应当公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。 第五十三条 本法第三条第二款规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理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。	护职责的部门”。考虑到个人信息保护负责人和指定代表可能发生变化，这一报送过程将较为繁琐。	息的要求，或将报送改为自愿行为，避免为组织和部门增添不必要的负担。
54	第五十四条 个人信息处理者应当定期对其个人信息处理活动遵守法律、行政法规的情况进行合规审计。	和上一版相比，本条移除了“履行个人信息保护职责的部门有权要求个人信息处理者委托专业机构进行审计”这一表述。我委员会赞同这一改动，希望本条进一步补充关于审计频率、范围的内容，并列举具有资质的审计公司。	建议审计周期不得短于一年。
55	第五十五条 个人信息处理者应当对下列个人信息处理活动在事前进行风险评估，并对处理情况进行记录： （一）处理敏感个人信息；	第五十五条规定了一系列需要进行风险评估的活动，其中包括所有处理敏感信息的情形，所有利用个人信息进行自动化决策的情形，和所有委托第三方处理个人信息的情形等等。	根据风险程度采取相应措施，维护信息安全，推动科创行业发展。 将本条表述调整为“仅在面临高风险，或可能危害个人时，对个人信息处理活动在事

	（二）利用个人信息进行自动化决策； （三）委托处理个人信息、向他人提供个人信息、公开个人信息； （四）向境外提供个人信息； （五）其他对个人有重大影响的个人信息处理活动。 风险评估的内容应当包括： （一）个人信息的处理目的、处理方式等是否合法、正当、必要； （二）对个人的影响及风险程度； （三）所采取的安全保护措施是否合法、有效并与风险程度相适应。 风险评估报告和处理情况记录应当至少保存三年。	但以上情形中也包含一些商业“日常运营”活动，例如： 1. 以行政管理或安排雇员福利为目的，向跨国组织总部发送雇员信息。 2. 将运营事务外包给服务提供商（例如，委托保险公司负责雇员保险事务）。 严格的风险评估应仅适用于高风险情形，否则可能会导致个人面临重大法律风险。 此外，本草案第五章，即第五十一条至第五十八条中关于信息保护的规定适用于“所有”组织，同样也应该适用于个人信息处理的“所有”方面。承担法条规定的相关义务可以降低在商业“日常运营”中处理个人信息的风险。	前进行风险评估，并对处理情况进行记录”。 在利用个人信息进行自动化决策时，建议“仅在自动化决策对个人产生重大影响，或侵害个人合法权益”时进行风险评估。 以上建议符合欧盟《通用数据保护条例（GDPR）》等国际惯例。
56	第五十六条 个人信息处理者发现个人信息泄露的，应当立即采取补救措施,并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项： （一）个人信息泄露的原因； （二）泄露的个人信息种类和可能造成的危害；	根据本条规定，个人信息处理者发现“所有类型的”个人信息泄露，都应当通知履行个人信息保护职责的部门和个人。这一条文的适用门槛过低，会将意外发生、不会影响个人的非敏感信息泄露也涵盖在内。宽泛的报告机制还可能导致过度报告，增加监管者和企业的管理负担；长期以往，还可能让监管	建议： 1. 将第三项表述调整为“已采取或准备采取的补救措施”。 2. 根据泄露可能造成的风险大小程度采取相应措施。为个人信息处理者在信息泄露后的通知义务设定门槛：仅在信息泄露可能造成重大危害时，要求必须通知履行个人信息保护职责的部门和个人。这类规定

	（三）已采取的补救措施； （四）个人可以采取的减轻危害的措施； （五）个人信息处理者的联系方式。 个人信息处理者采取措施能够有效避免信息泄露造成损害的,个人信息处理者可以不通知个人；但是，履行个人信息保护职责的部门认为个人信息泄露可能对个人造成损害的，有权要求个人信息处理者通知个人。	者无法辨别真正具有危害性的信息泄露情形。 建议根据泄露可能造成的风险大小程度采取相应措施。仅在信息泄露可能造成重大损害时，通知履行个人信息保护职责的部门和个人。 医疗、银行、消费、制造业等不同行业面临的个人隐私风险大小各异。基于风险采取相关措施可以关照到这些差异，让各个组织、监管部门和个人将资源有效集中在真正的风险上。	可以保证监管者集中资源，关注真正的风险，在最被需要的时候给出指导意见，履行监督职责。 3. 将本条的表述调整为“个人信息处理者发现重大个人信息泄露的，应当立即发出通知……”使个人信息处理者有时间先对事件进行适当调查，再向监管机构进行报告。
57	第五十七条 提供基础性互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务： （一）成立主要由外部成员组成的独立机构,对个人信息处理活动进行监督； （二）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者,停止提供服务； （三）定期发布个人信息保护社会责任报告，受社会监督。	本条适用范围不清楚。“基础性互联网平台服务”“用户数量巨大”“业务类型复杂”指代不清。 公司网页是否属于“基础性互联网平台服务”？此外，我们需要进一步明确“主要由外部成员组成的独立机构”需要满足何种条件？是否只有符合资质的专家才能组成独立机构？本条是否仅适用于中国境内的基础性互联网平台服务？	明确解释“基础性互联网平台服务”“用户数量巨大”“业务类型复杂”这三个并列表述。 此外，个人信息处理者履行本条所规定的义务需要负担高昂的成本，动用大量资源。在划定相关标准，解释概念，或提出指导意见时，希望有关部门三思。 说明“发布个人信息保护社会责任报告”“成立主要由外部成员组成的独立机构”相关表述中所包含的具体义务。

58	第五十八条 接受委托处理个人信息的受托方，应当履行本章规定的相关义务，采取必要措施保障所处理的个人信息的安全。	本条新增的表述非常宽泛，且拟将第五章中规定的义务拓展到“受托方”，亟需厘清意涵。 接受委托个人信息的“受托方”，在委托范围内代表个人信息处理者履行义务或从事信息处理活动的，不应和信息处理者履行同等义务。	考虑到个人信息处理者可能要承担所有面向消费者的义务，需要划清各个主体的角色和责任。
59	第五十九条 国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。 县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。 前两款规定的部门统称为履行个人信息保护职责的部门。	根据本条，网信办、国务院有关部门和县级以上地方人民政府有关部门将负责个人信息保护和监督工作。这是否表明，草案中所有的“有关部门”均可作同样解释？是否还存在负责向公众就数据隐私问题提供合规方面的指导、建议，确保法律施行的其它部门？以上问题对于企业合规来说尤为重要。	明确列出不同城市中负责个人信息保护和监督管理工作的部门名单。
65	第六十五条 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，由履行个人信息保护职责的部门责令改正，没收违法所得，给予警告；拒不改正的,并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。		各主体承担责任的门槛应设置得较高，仅在情节严重时（例如，排除疏忽的故意违法）进行追责。尽力避免立法的“寒蝉效应”，为处理大量个人信息的主体免除不必要的负担，也让它们在处理个人信息时也无需过于谨慎。

	有前款规定的违法行为，情节严重的，由履行个人信息保护职责的部门责令改正，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、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；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。		另外，建议本条与欧盟《通用数据保护条例（GDPR）》保持一致，将罚款金额直接设为上一年营业额额度的百分之四。
68	第六十八条 个人信息权益因个人信息处理活动受到侵害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。 前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定；个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。	在发生任何损害时，个人信息处理者要证明自己没有过错是比较困难，甚至是很困难的。	第二款中“依据实际情况”确定赔偿数额可能会导致诉讼增加。建议由个人承担举证责任，证明自身隐私权被个人信息控制方侵害。例如，将表述调整为“当个人可以说明自身权益因个人信息处理活动受到侵害时，……”。
72	第七十二条 本法下列用语的含义： （一）个人信息处理者，是指自主决定处理目的、处理方式 等个人信息处理事项的组织、个人。 （二）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	第二项中“利用个人信息对个人的……通过计算机程序自动分析、评估并进行决策的活动”表述不明确。 第四项中关于“匿名化”定义对该项技术提出了极高的要求。考虑到技术更迭，我们极难	明确“利用个人信息对个人的……通过计算机程序自动分析、评估并进行决策的活动”仅限于没有任何人工参与或判断的全自动化过程。

	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。 （三）去标识化，是指个人信息经过处理，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。 （四）匿名化，是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。	证明匿名化处理后自然人信息无法识别或不能复原。	对第四项进行补充，将表述调整为“个人信息经过处理后，符合行业关于信息匿名化的标准”。
73	第七十三条 本法自年 月 日起施行。	考虑到企业解读最终版本的法律并做出相应调整需要时间，应设置 24 个月的缓冲期，为各个行业的企业留出充分的准备时间。	设立 24 个月的缓冲期。