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）》的反馈意见

美中贸易全国委员会（下称我委员会）谨代表220余家会员企业就《中华人民共和国个人信息保护法（草案）》（下称草案）向全国人大提出意见。

自草案公开征集意见起，我委员会收到多家家会员企业建议，来自信息与通讯技术（ICT）、能源、制造业、汽车和金融服务等多个相关行业。

本草案是构建中国互联网安全机制、在个人信息处理全过程中维护组织和个人权益的关键。我委员会支持中国政府的通过立法手段保护中国境内组织和个人的信息隐私和安全，同时期待立法过程中能重点斟酌以下问题以及相关条款，解决企业的关切：

1. **域外适用问题：**根据第三条，草案适用于在中国大陆之外的个人信息处理者分析、评估境内自然人，或向境内自然人提供产品或者服务的情形。而且本条第二款第（三）项为兜底规定，还一步将草案的域外适用扩大至所有“法律、行政法规规定的其他情形”。综合这两点，我委员会认为本条对于草案适用情形的描述不甚明确，企业将很难评估合规负担。

2. **管辖部门模糊：**根据第五十六条，国家互联网信息办公室将负责统筹协调个人信息保护工作和相关监督管理工作，各级地方人民政府有关部门共同参与执法。这会增加个人信息处理者不必要的合规负担，因为其不仅必须在常规运营中自行判断合适的报送对象，而且在发生个人信息泄露时，由于不清楚应当通知哪一部门，只能重复通知各个可能负责的部门。

3. **达标“门槛”缺失：**草案将“处理个人信息达到国家网信部门规定数量”作为衡量标准，判断跨境数据传输是否需要经过安全评估，以及信息处理者是否需要指定个人信息保护负责人并报送履行个人信息保护职责的部门。然而，考虑到企业收集的个人信息种类各异，所涉风险大小不同，信息量并不是一个有价值的风险评判指标。此外，草案并未对国家网信部门的各类“规定数量”设置相应的达标“门槛”，所以企业无法准确衡量合规要求。

4. **数据本地化及相关要求不合理：**第四十条规定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（即非关键信息基础设施运营者），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。但本条与《中华人民共和国网络安全法》（下称《网络安全法》）有关规定存在冲突。因为后者只要求关键信息基础设施运营者遵守数据本地化规定。其实，在数据本地化的要求下，无法联通至全球网络、完成分散存储的数据将会面临更大的安全隐患。例如，存储在本地的数据可能被全部摧毁，或者因为区域断电造成损害无法正常读取，如果遇到此类极端情况，企业将很难恢复数据。在极端情形下，如果黑客得知中国境内的企业将海量的本地数据全部存储在境内，他们会受巨大的利益驱使更频繁地攻击这些企业。最重要的是，对于全球运营的企业而言，在本地存储、处理数据，既不经济、也不实际。如果出台此类规定，将会影响企业在华投资。

5. **个人信息收集规定仍待补充：**草案没有明确允许企业实体基于“合法利益”收集、处理个人信息。虽然第十三条已经补充列举了个人信息处理者在“取得个人的同意”之外可以处理个人信息的情形，但是没有明确为“企业处理雇员个人信息”提供法律基础。如果按照当前规定，在企业尝试管理雇员培训或查看其它属地的雇员信息时，将面临不必要的繁琐程序。

我委员会非常重视此次提交意见的机会，并通过以下表格提供关于具体条款的详细意见和建议。如条件允许，我委员会也愿意携企业代表与立法机构进一步交流。联系人：闫羽，电话：010-6592-0727。

美中贸易全国委员会北京代表处

2020 年 11 月 19 日

反馈意见汇总表			
条/款号	**条/款内容**	**意见**	**建议**
第一章	总则		
3	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)为分析、评估境内自然人的行为; (三)法律、行政法规规定的其他情形。	整体而言，本条表述过于模糊，如需适用本条，需要澄清有关概念。 例如，第（二）项中的“分析、评估”可以依字面狭义理解为“在中国境内阅读新闻报道的任意个人行为”。但根据立法目的，此处应指“利用大数据分析和数据剖析工具，分析、评估境内自然人的行为”。 第（三）项中“其他情形”的表述类似兜底条款，企业无法依此条文准确衡量合规负担。 此外，不清楚本条是否适用于以下情形： 1. 依据第二十二条和三十八条，与中国境外的分公司订立合同，委托处理个人信息； 2. 公司以和中国境内企业达成交易为目的，而非以向境内自然人提供产品或者服务为目的（第二款第（一）项），收集个人信息。例如，签订合同时需要公司董事签名；为达成交易，需要获取销售代表的联系方式。	缩小第（二）项的适用范围，将表述修改为“利用大数据分析和数据剖析工具，分析、评估境内自然人的行为”。 删去第（三）项，并增添豁免规定，排除中国境外的分公司需要处理雇员个人信息；或为达成交易，需要收集个人信息的情形。
4	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、公开等活动。	赞同本条关于“个人信息”的定义。该定义与欧盟《通用数据保护条例》（GDPR）中的相关表述一致。相较于此前发布的《网络安全法》和《中华人民共和国民法典》（下称《民法典》），本条关于个人信息的定义新增了“可识别的自然人有关的”信息，范围界定更加完整。	明确“个人信息”是否排除假名数据、聚合数据（Pseudonymized or aggregated data）。
8	为实现处理目的,所处理的个人信息应当准确,并及时更新。	如果按照本条规定，信息处理者需要积极采取行动，保证他人提供的个人信息准确。但是许多企业处理的数据量很大，如果需要自主确定信息准确性，将会面临沉重负担。	增添补充说明：向个人信息处理者提供信息时，个人信息主体应当为信息的准确性负责。

		应允许数据处理者假定他人提供的数据是准确的。	
9	个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。	原则上，“个人信息处理方”和“个人信息控制方（Controller）”承担的责任不同，但本条未作区分。 如果依照第二十二条的规定，个人信息处理者委托处理个人信息的，应当与受托方约定委托处理的目的、处理方式、个人信息的种类、保护措施以及双方的权利和义务等。 两则条文存在冲突。	豁免“受个人信息处理者委托，处理个人信息”的情形。
10	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。	“危害国家安全、公共利益的个人信息处理活动”的表述过于宽泛。	列举被视为危害国家安全的活动。 删去“公共利益”这一表述。
第二章	个人信息处理规则		
13	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)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; (六)法律、行政法规规定的其他情形。	赞同根据《网络安全法》和《民法典》调整、补充本条中除“取得个人的同意”以外，其他合法处理个人信息的情形。 但本条缺少关于“基于个人信息处理者的合法利益”处理信息的相关规定。 欧盟《通用数据保护条例》（GDPR）和巴西《通用数据保护法》（LGDP）都包括这类表述，其实际适用范围非常广泛，可以为大量合法的信息处理行为提供法律依据： ● 雇主对雇员的信息处理。当企业需要以培训为目的处理雇员信息时，并不能完全依赖雇员的同意； ● 提供的个人信息处理服务中包括非合同当事人的信息。例如，当卡车制造商向某个卡车司机提供远程协助时，需要使用司机的地理位置数据，但司机并不是合同当事人。此时订立合同的双方为	在现条文基础上增添“基于个人信息处理者的合法利益”处理个人信息的情形。如果本项所称的“合法利益”侵害个人信息权益和自由，或遭到个人反对，则本项无效。 增添“为保护数据主体的切身利益”处理个人信息的表述。进一步明确在“取得个人的同意”以外，其他合法处理个人信息的情形。 将第（三）项中“为履行法律职责或法定义务所必需”中的“法律职责”“法定义务”拓展至外国法律法规领域，因为金融机构也有可能成为个人信息处理者。确保规定的一致性，可以帮助金融机构在金融和个人信息两方面履行合规义务。 厘清第（五）项中的“合理范围”。

		卡车制造商和运输企业，企业是卡车的所有者。 此外，引进“基于个人信息处理者的合法利益”的表述，可以让企业在遇到同意可能被撤回的情形时，有明确的法律依据可循。这类情形包括：向第三方提供信息（第二十四条），跨境个人信息传输（第三十九条），个人信息公开（第二十六条）。 此外，第（五）项中 “在合理的范围内”指代不明。对“合理范围”的任意解释可能导致个人信息的公开超出所需限度。	
14	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、明确作出意思表示。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。	如果在每次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时都重新取得个人同意，企业将面临沉重负担。 同时，条款中“单独同意”指代不明。	增添豁免规定：如果在变更发生前，个人信息处理行为就无需取得个人同意，且变更后信息处理目的、方式和信息种类仍然符合变更发生前的情形，无需重新取得个人同意。 或收窄本条的适用范畴，仅要求在各类变更发生前就应当取得个人同意的个人信息处理行为，在变更发生后重新获取个人同意。 区分“同意”“书面同意”和“单独同意”，明确两个术语的定义和适用情形。
16	基于个人同意而进行的个人信息处理活动，个人有权撤回其同意。	即使个人撤回其同意，如果符合其他法律、行政法规规定的其他情形，有必要保留个人数据的，仍应保留。	明确指出本条的适用需要参照其它法律、行政法规规定。
18	个人信息处理者在处理个人信息前,应当以显著方式、清晰易懂的语言向个人告知下列事项: (一)个人信息处理者的身份和联系方式; (二)个人信息的处理目的、处理方式，处理的个人信息种类、保存期限; (三)个人行使本法规定权利的方式和程序;	如果要求在个人信息处理前，主动告知个人本条所列举的全部事项，企业将面临较大负担。特别是个人没有提出相关请求时，主动告知的意义有限。 “便于查阅和保存”这一表述中“保存”语义模糊，不清楚是否可以解读为要求企业公开隐私规定，并为个人提供“打印”和“下载”选项。 第一款“个人信息处理者在处理个人信息前”的“前”语义模糊。一般而言，只有在他人提供数据后	将表述修改为：仅要求企业在个人提出请求时，告知个人信息处理规则。在个人信息处理前，无需主动告知。此外，还可以合理要求企业通过可公开访问网页即时更新数据处理规则，代替逐一直接告知。删去“便于查阅和保存”中的保存，避免语义模糊。

	(四)法律、行政法规规定应当告知的其他事项。 前款规定事项发生变更的,应当将变更部分告知个人。 个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的,处理规则应当公开，并且便于查阅和保存。	（例如通过邮件方式），信息处理者才能向个人告知。	
21	两个或者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,依法承担连带责任。	需注意的是，在两个或两个以上的个人信息处理者之间，存在多种不同的形式的“共同决定”。共同对信息处理活动“负责”，并不等同于“承担连带法律责任”。 实际上，共同处理个人信息时，任何一个方应承担的法律责任多寡，都应该具体情况、具体分析。	修改本条表述为：“个人信息处理者共同处理个人信息，侵害个人信息权益的，视具体情形，依法承担连带责任。”
22	个人信息处理者委托处理个人信息的,应当与受托方约定委托处理的目的、处理方式、个人信息的种类、保护措施以及双方的权利和义务等,并对受托方的个人信息处理活动进行监督。 受托方应当按照约定处理个人信息,不得超出约定的处理目的、处理方式等处理个人信息,并应当在合同履行完毕或者委托关系解除后,将个人信息返还个人信息处理者或者予以删除。 未经个人信息处理者同意,受托方不得转委托他人处理个人信息。	在大多数情况下，受托方会具备专门的信息保护技术和相应能力，确保个人信息安全。因此，应当首先要求受托方拥有必要的信息保护手段。个人信息处理者应依靠受托方履行相应职责来保障个人信息在处理过程中的安全，并以此方式实现尽责。	为避免权利义务混淆，建议增加关于“受托方”的定义，清晰划分信息处理者和受托方之间相应权利和义务关系。
23	个人信息处理者因合并、分立等原因需要转移个人信息的,应当向个人告知接收方的身份、联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式的,应当	对于许多企业而言，“向个人告知并取得其同意”的要求无法实现，因为一些公司会大批量买入和卖出商业簿（Portfolios/books of business）。商业簿包含大量客户信息，逐一取得信息主体的同意显然不实际。	建议移除本条关于“取得同意”的相关规定，或者直接豁免第十三条中列举的所有合法处理个人信息的情形。 明确需要在并购（M&A）过程中的哪一阶段告知个人。出于保密要求，企业很难在并购完

	依照本法规定重新向个人告知并取得其同意。	以保险行业为例，如果保险机构因合并、分立等原因需要转移个人信息，原先的信息处理目的、处理方式的也会变更。如果依照本条规定，没有重新向个人告知并取得其同意的，个人信息便无法转移。这会导致保险失效，严重损害被担保个人的利益。	成之前告知个人接收方的身份、联系方式。
24	个人信息处理者向第三方提供其处理的个人信息的,应当向个人告知第三方的身份、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。接收个人信息的第三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。第三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向个人告知并取得其同意。 个人信息处理者向第三方提供匿名化信息的,第三方不得利用技术等手段重新识别个人身份。	本条中部分表述可能引起疑义，部分要求业可能增加企业的运营成本： 1. 根据本条规定，企业需要在向第三方提供其处理的个人信息前，取得个人的“单独同意”。但第十三条也列出了其他不用取得个人同意，也可以合法处理个人信息的情形。两则条款存在冲突。 2. 本条的立法目的在于帮助个人信息主体了解“个人信息处理者向第三方提供其处理的个人信息”的流程，提升该行为的透明度，但具体规定不具备可行性。要求企业告知个人每个第三方的联系方式、处理目的和处理方式，和要求第三方告知个人并取得同意，都是不切实际的。原则上，个人信息处理者应依据具体合同，要求第三方确保个人信息安全。 3. 多种商业交易行为都可能牵涉个人信息在多个交易方之间转移，要求个人信息接收方取得个人信息主体的同意，也是不切实际的。	将表述修改为：如符合第十三条对可以合法处理个人信息的任何一个情形的描述，便允许信息处理者向第三方提供其处理的个人信息。 1. 参照欧盟《通用数据保护条例》，将“告知个人信息接收方的身份”改为“告知个人信息接收方的类型”。 3. 增添豁免规定：当个人信息处理者已经明确告知个人，自己的个人信息处理实践中包括向第三方公开信息，并提供详细说明时，无需在向第三方公开信息时再次取得个人单独同意。 4. 增添豁免规定：本条不适用于受委托处理个人信息的个人信息处理者。
25	利用个人信息进行自动化决策,应当保证决策的透明度和处理结果的公平合理。个人认为自动化决策对其权益造成重大影响的，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。 通过自动化决策方式进行商业营销、信息推送,应当同时提供不针对其个人特征的选项。	保证个人信息处理结果“公平”“合理”的客观标准，何种行为会“对权益造成重大影响”，以及何种行为会被视为违反上述原则，三项表述均不明确。 现代人工智能算法本质上具有高度不确定性和不可解释性，如果运用人工智能算法进行自动化决策，显然无法满足本条对“保证决策透明度和处理结果的公平合理”的要求。	以下建议均参照欧盟《通用数据保护条例》等国际惯例： 为本条第二款关于“应当同时提供不针对其个人特征的选项”的规定增添以下豁免情形： 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。

			限制本条适用范围。仅在进行自动化决策可能对个人信息主体造成重大影响时，“保证”决策的透明度和处理结果的公平合理。 进一步解释“公平”“合理”，明确这类原则的适用范畴。
27	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;取得个人单独同意或者法律、行政法规另有规定的除外。	在公共场所收集、处理个人信息，或者处理个人信息以确定保险的赔付情况，或防止欺诈时，很难取得个人同意。例如，在一个跌倒案例的理赔中，就需要借助公共场所收集、处理的个人信息，评估应个人承担的责任。	说明在此类情形下，取得个人单独同意的具体方法；并为无法取得个人同意的情况提供替代解决方案。
29	个人信息处理者具有特定的目的和充分的必要性,方可处理敏感个人信息。 敏感个人信息是一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息,包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。		删去本条对敏感个人信息包括哪些信息的列举结束后的“等”字。另外，“个人行踪”不应属于敏感个人信息的范畴。
30	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。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。	在商业活动中，一方商业主体向另一方公开个人信息的情形非常普遍。要求个人信息接收方提前获取相关个人信息主体的同意，是不切实际的。	增添补充说明：允许个人信息接收方，基于公开个人信息的一方同意处理个人信息。而且，由公开个人信息的一方负责取得个人同意。 增添豁免规定：本条不适用于以防止诈骗和保障信息安全为目的，处理敏感个人信息的情形。
第三章	个人信息跨境提供的规则		
38	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;	对于国际化运营的跨国企业而言，在中国境外保存和处理中国境内的分公司或者子公司雇员的个人信息是很普遍的情况。如果不设置豁免，将本条适用于雇员的个人信息处理，跨国企业的管理负担和运营成本都会无必要地大幅增加。	修改方向如下： 1. 豁免雇员个人信息跨境传输。 2. 规定本条仅适用于在中国境内收集的个人信息。

	(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)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。	亦不清楚本条所指“个人信息”是否泛指任何在中国境内收集的个人信息，或是否包含个人信息处理者在中国境外收集的、但存储在中国境内的个人信息。 赞同第（三）项的规定，通过与境外接收方订立合同的方式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。	3. 澄清第（一）项中的“安全评估”是否遵循《个人信息出境安全评估办法（征求意见稿）》有关规定。
39	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。	在欧盟《通用数据保护条例》（GDPR）这一类国际法律法规中，向境外传输个人信息的组织需要提供个人信息处理行为的“具体细节”，以及境外接收方的身份或者类型。但法律并未明确规定“具体细节”需要涵盖的内容。 但本条明确列举了跨境数据传输时“应当向个人告知”的各类事项，包括境外接收方身份、联系方式，还要提供个人向境外接收方形式本法规定权利的方式。 跨国企业在华公司与中国境外的分公司共享个人信息，或者通过不在其管辖范围内的第三方处理个人信息是很普遍的现象。告知个人境外接收方或个人信息处理方的身份或类型属于合理要求，但是无必要提供联系方式。不为实现具体目的，单纯提供联系方式只会让告知的内容过于冗长。 当信息主体提出查阅信息、删除信息或修改信息的要求时，应直接向信息处理者反应，而不是向任何信息处理生态链上的一方（例如境外信息接收方）行使本法规定的权利，以免把问题复杂化，造成不必要的混乱。 个人信息处理生态链上的每一方，都必须严格按照合同约定处理个人信息，行为不得超出约定范畴。 “单独同意”指代不明。个人信息处理者在使用和传输数据时，原本就需要取得个人信息主体的同意，	修改方向如下： 1. 合并第三十八条和第三十九条，统一列举满足向中国境外传输数据应当具备的条件。 2. 参照欧盟《通用数据保护条例》，将“告知个人信息接收方的身份”改为“告知个人信息接收方的类型” 3. 将“单独同意”改为“同意”。 4. 移除“个人信息处理者向个人告知境外接收方联系方式以及向境外接收方行使本法规定权利的方式”这一规定。 5. 明确区分本条与第三十八条的适用范围。本条应该仅适用于非商业目的个人信息跨境传输。

		这类“一般”同意和单独同意之间的区别不清楚。	
40	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。	本条不仅比照《网络安全法》相关规定，要求关键信息基础设施（CII）运营者实现数据存储的本地化要求；还将不属于关键信息基础设施运营者的“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”也纳入了规制范围。 实际上，如果某类信息只能在当地处理和存储，个人和企业的敏感信息和专属信息反而会面临更高的安全风险。因为不论企业的规模大小，当今绝大部分企业的信息都是存储在分布式网络，也就是分散在各地的多台服务器上的，这是企业合理规避风险的体现。如果改变当前的分布式信息存储模式，采用集中存储，相应风险自然会增加。 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，某一跨国机构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。 最后，按照目前的草案，此条款需要进一步明确数据本地化存储要求实施的门槛。	建议修改方向如下： 1. 不实行“数据本地化”规定，改为要求“信息存储在境外的，需要提供足够、有效的信息保护”。 2. 如不采纳以上建议，可以比照《网络安全法》相关规定，澄清本条仅适用于关键信息基础设施（CII）运营者。
41	因国际司法协助或者行政执法协助,需要向中华人民共和国境外提供个人信息的,应当依法申请有关主管部门批准。 中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息有规定的,从其规定。		增添豁免规定：本条不适用于对公众公开的信息、商业联络信息或雇员个人信息。
第四章	个人在个人信息处理活动中的权利		
44	个人对其个人信息的处理享有知情权、决定权,有权限制	不清楚个人对其个人信息的处理享有何种“决定权”。	增添豁免规定：为合法商业利益处理个人信息的情况除外。

	或者拒绝他人对其个人信息进行处理；法律、行政法规另有规定的除外。		如果此处的决定权是指“有权利决定他人是否可以对其个人信息进行处理”，应使用前文出现的术语“同意”来表达意思，避免理解错误。
45	个人有权向个人信息处理者查阅、复制其个人信息;有本法第十九条第一款规定情形的除外。 个人请求查阅、复制其个人信息的,个人信息处理者应当及时提供。	当个人为实现某一类目的（包括但不限于维护公共利益、保护其他个体权益或其他合法理由）而行使权利时，应限制其权利行使范围。 第四十九条明确指出“拒绝个人行使权利的请求的，应当说明理由”。这一规定的存在说明个人信息处理者有权拒绝个人提出的请求，但由于缺乏相应法律解释，实施层面或许存在困难。	增添豁免规定：通过列举多项条件，允许个人信息处理者或相应组织在满足某一条件时，拒绝个人对查阅、复制其个人信息的请求。例如，个人请求查阅、复制其个人信息时可能影响信息保密性或侵犯其他个人隐私的，个人信息处理者可以拒绝请求。
47	有下列情形之一的,个人信息处理者应当主动或者根据个人的请求,删除个人信息: (一)约定的保存期限已届满或者处理目的已实现; (二)个人信息处理者停止提供产品或者服务; (三)个人撤回同意; (四)个人信息处理者违反法律、行政法规或者违反约定处理个人信息; (五)法律、行政法规规定的其他情形。 法律、行政法规规定的保存期限未届满,或者删除个人信息从技术上难以实现的,个人信息处理者应当停止处理个人信息。	本条不适用于雇员个人信息处理。	建议规定本条不适用于同意可能被撤回的多种情形；明确本条不适用于对雇员个人信息的处理。
48	个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。		增添豁免规定：个人信息处理者出于保护交易秘密或知识产权的必要，可以不按照个人要求对个人信息处理规制做解释说明。
49	个人信息处理者应当建立个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的,应当说明理由。		进一步说明在何种情形下，个人信息处理者可以拒绝个人信息主体的请求。 另外，当个人信息主体请求查询、复制其信息的范围超出了合

			理限度，应允许个人信息主体收取手续费。
第五章	个人信息处理者的义务		
51	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。 个人信息处理者应当公开个人信息保护负责人的姓名、联系方式等,并报送履行个人信息保护职责的部门。		1. 为“达到国家网信部门规定数量”这一标准设立“门槛”，即最低数值。 2. 个人信息处理者应秉承“自愿原则”公开个人信息保护负责人的详细资料，报送履行个人信息保护职责的部门，免除个人信息处理者或组织不必要的成本和负担。
52	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。	如果境外的个人信息处理者在境内的指定代表可能发生变化，“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护职责的部门”的过程将较为繁琐。	建议参照欧盟《通用保护条例》有关规定，修改本条为：当信息处理行为具有临时性，处理的数据不包含大量敏感个人信息，或不可能侵害其他自然人的权益和自由时，中华人民共和国境外的个人信息处理者不需要在境内指定代表。 将“应当报送”改为“自愿报送”，或移除本条，避免增添不必要的负担。
53	个人信息处理者应当定期对其个人信息处理活动、采取的保护措施等是否符合法律、行政法规的规定进行审计。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。	“定期审计”“委托专业机构”表述模糊。 对于绝大部分个人信息处理者而言，定期审议意义有限。而且，具有强制性、且以处罚为目的的审计机制会影响目前网络安全和数据保护领域的投资活动。	仅对关键信息基础设施运营者进行强制审计。如无法采纳此意见，可以规定审计的周期，避免企业增加不必要的运营成本。
54	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; (二)利用个人信息进行自动化决策; (三)委托处理个人信息、向第三方提供个人信息、公开个人信息;	本条描述的活动范围过于宽泛。如按本条规定，对处理所有敏感个人信息、所有利用个人信息进行自动化决策（ADM）的情形，都进行事前风险评估，大量常规的商业运营也会被纳入规制范围，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。	建议修改方向如下： 1. 仅在个人信息处理者的行为可能使个人面临较高风险或重大风险时，要求在事前进行风险评估,并记录处理情况。 2. 参照欧盟 GDPR 等国际惯例，仅在利用个人信息进行自动化决策（ADM）对个人造成法律效力或产生极大影响时，进行事前风险评估，并记录处理情况。

	(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。	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）。 此类严苛规定应仅适用于高风险情形，否则一般个人可能会面临重大法律风险。	
55	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; (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。	如按本条规定，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，那么当意外发生的、不会影响个人的非敏感信息泄露也将被涵盖在内。 这类过于宽泛的规定可能增加监管者和企业的管理负担；长期以往，还可能让监管者无法辨别真正具有危害性的信息泄露情形。	本条修改方向如下： 1. 补充关于“个人信息泄露”的定义。 2. 将“个人信息泄露”限制在可能潜在危害或严重影响相关个人的情形。 3. 为发现信息泄露的个人信息处理者实施通知行为设置合理期限。例如，自知道信息泄露事件的当日起，设置 45 至 60 日的缓冲期，供个人信息处理者展开调查、评估。
56	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	“履行个人信息保护职责的部门”指代不明。按本条表述，多级政府的数个部门都拥有执法权。这类规定会增加个人信息处理者的合规成本。例如，不清楚在发生个人信息泄露时，应当通知哪一部门；不清	明确划分各部门履行的职责，避免交叉执法和信息重复报送。

	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。	楚向哪一部门报送个人信息保护负责人的姓名、联系方式。	
第七章	法律责任		
62	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。 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。	本条规定所涉罚款金额波动范围极大，涵盖了多种不同的数量级，且处罚力度均偏重。 这可能会限制企业合法处理个人信息的行为，因为在其它法域，出现类似情形，违法者面临的处罚远轻于此。 如实行本条规定，执法部门必须： 1. 确保适用范围不包含合法的商业信息处理行为。这是因为企业犹豫是否处理信息时，会牺牲潜在的经济增长利益。 2. 确保适用范围仅包含本法域中的企业行为，否则处罚会偏重。	将第二条修改为：仅在违法犯罪情节极其严重时，并处五千万元以下或者上一年企业在华运营营业额百分之五以下罚款。 详细说明个人可能面临各级罚款的具体情形。
第八章	附录		
69	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。	根据第（四）项的表述，个人信息的“匿名化”处理应该是“不能复原”的。从技术层面来看，这是对目前的“匿名化”技术提出了极高的要求。因为，随着技术的不断发展，即使是当前已经被匿名化处理的个人信息，也很可能在不久的将来实现“去匿名化”。 另外，草案中“个人信息处理者（Personal information processor）”的定义类似于欧盟	移除第（四）项中关于匿名化信息“不能复原”的表述。 参照国际法律法规，使用统一术语。将草案中的“个人信息处理者”、“接收方”，全部替换为“数据控制方”、“数据处理方”。

	(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。	《通用数据保护条例》中的“数据控制方（Data controller）”；而草案中的“受托方（Entrusted party）”类似于“数据处理方（Data processor）”。 术语不统一可能导致企业起草合同时面临困难。例如，订立一份跨境数据传输合同，需要大量援引中国和欧盟相关法律文件中的这类术语。	