关于中国《个人信息保护法（草案）》的立法建议

尊敬的全国人大常委会法制工作委员会：

我们非常荣幸能有机会就《个人信息保护法（草案）》（以下简称“**个信法**”）为法工委提供参考意见。我们信息政策领导中心（Centre for Information Policy Leadership, 以下简称 “**CIPL**”或“**中心**”）作为何威安卓律师事务所（Hunton Andrews Kurth LLP）的全球数据隐私和网络安全智库[1]，一直致力于促进全球数据隐私保护工作，并促进全球商业领导者、隐私和安全专业人士、监管机构和政策制定者之间富有建设性的互动。

我们非常高兴看到中国正在构建一个结合《网络安全法》和《数据安全法（草案）》的坚实数据保护体系，也非常认同全国人大法工委所作的努力，牵头制定了这部先进的、全面的个人信息保护法律草案，并认为这部综合性法律将成为中国数据保护体制的一大关键支柱，将有着重大的深远影响。

我们非常仔细、认真地研读了个信法的草案条款。在本立法建议材料中，我们针对部分草案内容提出了相关立法建议和意见。该等立法建议旨在加强当前这部法律草案的影响，让中国在这个相互操作性越来越强且必不可少的数字世界中跻身全球领导者之列。我们特别提出了一些修改建议，以避免对中国数字经济的创新和持续发展造成不必要的不利影响。我们诚挚地希望法工委适当考虑这些建议和意见，并予以合理采纳，这不仅是为了确保中国在国际数据保护领域的地位，也是为了确保对中国公民、企业和政府数据的保护[2]。

[1] 信息政策领导中心（Centre for Information Policy Leadership, “CIPL”或“中心”）是何威安卓律师事务所（Hunton Andrews Kurth LLP）的全球数据隐私和网络安全智库，由该律所以及全球经济重要领域内领先的 83 家成员公司提供支持。该中心以参与领导思想和制定最佳实践为使命，确保在现代信息时代有效地保护隐私和负责任地使用个人信息。中心的工作将促进全球商业领导者、隐私和安全专业人士、监管机构和政策制定者之间富有建设性的互动接合。如需更多信息，请访问中心网站 http://www.informationpolicycentre.com/。本提交材料中的任何内容均不得解释为代表中心的任何成员公司或何威安卓律师事务所（Hunton Andrews Kurth）的观点。

[2]请注意，本提交材料中的意见基于《个人信息保护法（草案）》的非官方翻译版本。因此，可能存在我们对特定议题的特定意图或微妙差异发生误解的可能性。如果任何特定意见确实发生此情形，请将该部分忽略。

立法建议和意见概要

本概要列明了本提交材料所包括的主要建议。这些建议根据特定主题进行整理。如需了解按照个信法逐条整理的完整建议，敬请参阅下文的详细建议内容。

信息处理的隐私原则和法律依据

- 在个信法中纳入“合法权益”处理依据。
- 建议明确以下内容：“如果个人信息处理目的发生变更且该变更与原目的相兼容，组织机构可以依凭原先处理依据对该等个人信息进行处理。如果新目的与原目的不相兼容，则需要提出新的法律依据”。

儿童个人信息

- 针对组织机构启用一套基于风险的评估方法，以确定组织机构是否在混合受众网站环境下处理未成年人的个人信息以及是否必须获得监护人的同意。

敏感个人信息

- 针对敏感个人信息的处理启用一套基于风险的评估方法，而不是提供预定义的敏感信息类别。
- 如果个信法中保留了预定义的敏感信息类别，建议将“金融账户信息”和“个人行踪”从定义中删除，并明确阐明如何定义、由谁定义“其他”形式的敏感个人信息。
- 建议明确阐明敏感个人信息可基于个信法中所列的所有合法处理依据进行处理，且对该等信息的处理不限于依据同意作出的处理。例如，紧急情况下为保护个人生命或健康而进行的处理。

个人信息的跨境提供

- 建议明确阐明必要的监管范围，以确保境外接收方处理来自中国的个人信息符合个信法列出的保护标准。
- 建议解释需要满足什么条件才能通过国家网信部门的安全审核，以将相关个人信息合法提供至境外接收方。
- 建议明确阐明第 38 条中对于跨境提供的“个人信息保护认证”是否可以使中国参与亚太经合组织 (APEC) 跨境隐私规则体系。
- 建议在个信法已罗列的个人信息跨境提供机制中增加行为准则和企业规则。
- 除满足个信法中的其他跨境提供要求之外，建议删除同意要求。

境外个人信息处理者任命在中国的专门机构或指定代表

- 建议修改将“将专门机构或指定代表的联系信息披露给相关主管部门并在相关部门登记”这一要求，只要求登记是否已任命该等个人信息负责人并确保该等任职信息是否准确且是最新的。

- 建议将任命“个人信息保护负责人”这一要求的触发条件与《个人信息安全规范》中的条件保持一致。

- 根据诸如 GDPR 等其他隐私法律中的豁免情形，建议为境外个人信息处理者应“在中国境内设立专门机构或指定代表”这一要求提供可豁免的情形。

风险评估

- 建议明确第 54 条所列的“事前风险评估”的要求：在个人信息处理活动之前应开展初步预筛查。如该等筛查表明对个人存在高风险时，则实施第 54 条要求开展的全面风险评估，进行“事前风险评估”。

信息泄露通知

- 建议设定并提高个人信息泄露必须报告相关部门和通知个人主体的最低数量。

- 建议将泄露通知时间要求从“发现后立即”改为“在可能的最快时间内，不得有不合理的延迟，且不得晚于实体/个人信息处理者发现数据泄露后的指定天数（例如 30 天或 45 天）后”。

向第三方提供数据

- 建议明确阐明个信法中第三方服务商的角色。

匿名化

- 建议修改匿名化的定义，以反映更为切合实际的合理匿名化的处理标准，外加程序、法律和行政性的保护措施。

公开信息

- 建议修改个信法，确保个信法中公开信息的使用规则与《亚太经合组织(APEC)隐私框架》和中国《个人信息安全规范》的规定相一致。

处罚

- 建议明确阐明个信法项下“严重”违法行为的构成要件。

- 建议明确阐明罚款按固定金额或按营收比例征收的条件，并阐明该营收是在中国国内的营收。

- 建议明确阐明第 62 条项下的个人责任仅适用于为获取经济利益而实施故意行为或重大疏忽的公司高级职员或董事。

生效日期

- 建议规定相关组织、个人在个信法通过之日起有两年过渡时间完全遵守该法律。

具体意见

第 3 条：地域范围

根据第 3 条，个信法适用于中国境外的组织机构出于以下目的而对中国境内个人的个人信息进行的处理：（1）以向境内自然人的个人提供产品或者服务为目的，（2）为分析和评估境内自然人的行为；（3）法律或行政法规规定的其他情形。

鉴于数据的全球化性质和流转，在个信法中加入该等条款可以让在境外传输或处理数据的组织机构明确其哪些活动受到法律的约束。但是，我们认为基于“法律或行政法规规定的其他情形”让境外组织机构受个信法约束产生不确定性，包括潜在的法律冲突情形。因此，我们建议删除第 3 条中的此部分内容，并在触发个信法下域外管辖范围的法律通过后，以相关主管部门发布中英文指南的方式详细阐明此种情形。这样可以确保所有利益相关者更加明确在中国境外处理个人数据的组织机构的责任。

建议：修改个信法第 3 条，删除“依据法律或行政法规规定的其他情形”使境外组织机构受个信法约束的条款，并以相关主管部门发布中英文指南的方式进一步阐明触发个信法下其他域外管辖范围的法律。

第 6 条：目的限制

个信法第 6 条规定个人信息处理应当具有明确、合理的目的，并应当限于实现处理目的最小范围，不得进行与处理目的无关的个人信息处理。

我们建议明确此条所说的“最小范围”是指“将相关且必要的个人信息处理局限于实现该等目的”，这一表达更为清晰，可以避免组织机构对于个信法当前版本中所述的“最小范围”的意义产生混淆。

建议：在第 6 条中明确阐明“最小范围”系指“将处理限于相关且必要以实现目的”。

第 13 条：数据处理的法律依据

我们非常认同个信法下将处理个人信息的多项法律依据一并纳入，包括：（1）取得个人的同意；（2）为订立或者履行个人作为一方当事人的合同所必需；（3）为履行法定职责或者法定义务所必需；（4）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；（5）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；或（6）法律、行政法规规定的其他情形。

但是，我们发现在当今的数字社会中，单凭这六项法律依据所界定的范围，可能无法实现某些日常的、常见的且非常重要的个人信息处理。

除了基于同意进行的个人信息处理外，个信法中所述的处理依据均与非常具体的信息处理情形有关，且该等情形仅仅是日常进行的数以百万计的处理操作的一小部分。此外，尽管同意本身仍然

适用于许多情况下的数据处理，但同样存在许多其他情形，在这些情形下，获取同意是不现实的、不可能的、无效的，乃至是无意义的。例如，包括（1）与个人没有直接互动的情形；（2）数据的使用非常常见、琐碎并且不存在实际隐私风险的情形；（3）处理大量重复性数据的情形（如果每次处理都需要寻求同意，可能因同意疲劳而变得不可行或者无意义）；或（4）获取同意会获得反效果的情形，例如出于网络和信息安全目的或者预防诈骗或犯罪目的而进行的数据处理。

我们建议纳入第七项处理依据，该依据类似于包括欧盟 GDPR、巴西 LGPD 和新加坡 PDPA 在内的其他隐私法律中的"合法利益"法律依据[3]。合法利益处理依据让组织机构可以在收集和处理个人信息的同时，确保其对数据处理负责，并充分尊重个人的数据保护权利。一般而言，该等条款会要求组织机构开展平衡检验或评估，证明其或第三方具有处理个人信息的合法利益，且该等利益不会被接受处理的数据所属的个人的权利所无效化。此外，该平衡检验必须可向隐私权主管执法部门证明。

更具限制性的个人信息保护规则并不一定意味着为公民带来裨益或者为公众利益服务。社会应允许企业和其他组织机构在必要的情况下处理个人信息，例如用于侦察、防止或调查诈骗或犯罪，这一点非常重要。

例如，在侦察和防止经济犯罪、恐怖主义融资或反洗钱阴谋时，获取处理个人信息的同意是不合适的。如果要求获得同意，不法分子只需拒绝提供同意，就可以在不受侦察的情况下实施非法行为。我们可以通过制定法律来应对某些形式的犯罪，然后再对数据进行处理，从而遵守法律义务，这样确实可以应对部分此类活动，但我们要记住犯罪的形式多种多样，不是所有犯罪都可以被法律所涵盖。此外，个信法中目前所列的其他处理依据没有适用于该等情形下的个人信息处理。因此，我们建议加入"合法利益"处理依据，使该等形式的重要处理成为可能。

对于中国而言，在个信法中加入该等处理依据不仅可以增强中国消费者沟通和线上交易的信心，而且可以确保私营部门和政府能够针对犯罪活动实施防范和执法。此外，中国民法典包含多项个人信息处理责任豁免依据，包括出于保护公共利益或自然人的合法权利而实施的行为[4]。纳入合法利益依据，让用于预防和侦察犯罪和诈骗的个人信息处理成为可能，这一做法符合民法典的规定，构成出于保护公共利益或自然人的合法权利而实施的行为。个信法应建立在民法典所创造的基础之上，让该等形式的信息处理成为可能。

我们必须要注意，合法利益处理依据不仅仅是与预防诈骗和犯罪相关的处理所必需的。该等依据可能适用的其他处理情形包括信息、网络、系统和网络安全；雇佣背景下的个人信息处理；企业运营和尽职调查；产品开发、增强；通信；营销和商业智能[5]。事实上，在不断发展的数据经济中，合法利益处理依据对于数字经济的正常运转和组织机构的创新能力而言非常必要的数据处理活动方面发挥越来越重要的作用。此外，我们必须注意，由于"合法利益"处理依据所固有的必要风险/利益评估（必须可向执行机关证明）以及根据补救和控制风险的相关要求，合法利益处理依据为个体的个人信息保护提供了一个高标准。

---

[3]请参阅 GDPR 第 6(1)(f)条和巴西 LGPD 第 7(IX)条。请注意，新加坡近期更新了其《个人数据保护法》，将合法利益处理依据纳入其中。

[4]请参阅主席令第 45 号《中华人民共和国民法典》第 1036 条。

[5]请参阅 2017 年 5 月 19 日 CIPL 关于 GDPR 项下透明性、同意和合法利益的实施建议白皮书 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_recommendations_on_transparency_consent_and_legitimate_interest_under_the_gdpr_-19_may_2017-c.pdf。

关于针对新闻报道在合理范围内进行处理，以便开展公众舆论监督和其他出于公共利益的行动的合法处理依据，个信法中对“合理范围”的含义不甚明确。我们建议全国人大法工委在下一次的个信法审议中进一步阐明该表述背后的意图。

建议：在个信法中加入“合法利益”处理依据，并明确阐释针对新闻报道进行处理，开展公众舆论监督和其他出于公共利益的行动中“合理范围”指什么。

第 14 条：同意和处理目的的变更

关于处理个人信息的同意，个信法规定任何同意均须由个人在充分知情的前提下作出自愿、明确的意思表示。目前，对于“充分知情”的意义不甚明确。事实上，许多个人在使用在线服务之前不会去阅读冗长的隐私政策，而建立这样一种预期会让组织机构极难证明该同意的取得完全符合第 14 条的规定。此外，“充分知情”是一个主观性的标准，无法在所有个人中作出统一的衡量。我们建议全国人大将第 14 条修改为“如果作出同意的意思表示对数据处理是合适的，须获得自愿、明确的同意”。

我们无法指望个人对其日常使用的数以百计的数字服务充分知情，并且对于许多处理操作而言，获取同意是不合适的。在该等情况下，通过合法利益处理依据（如上所述）可以给个人提供更好的保护，根据合法利益处理依据，组织机构有责任平衡相关利益，采取适当的补救措施，并在个人利益的重要性超过组织机构的利益时不进行处理。

此外，个信法第 14 条规定如果处理个人信息的目的发生变更，必须重新获得个人的同意。我们认为在特定情况下，如果进一步处理个人信息的目的与原目的“相兼容”，则应允许进行处理，无需重新获得同意。当然，根据具体情况，组织机构可能需要将新的处理目的通知个人。如果未来的使用情形与原先目的相符、可以共存并且不会损害或否定该原先目的，则应允许基于“兼容性”的进一步处理。该等使用情形必须以有力的问责制保护措施做支撑，包括益处和风险评估，以确保新的使用情形不会使个人面临扩大的风险或不利影响。

如果处理目的的变更与原目的不兼容，则需要按照新的法律依据进行个人信息处理。

建议：修改第 14 条，将有效的同意必须基于个人“充分知情”这一前提要求删除，因为该标准过于主观，在实际中不可行。在第 14 条中阐明“如果变更的处理目的与原目的相兼容，组织机构可以继续依赖原有的处理依据。如果新目的与原目的不相兼容，则必须依照新的法律依据（可能包括取得同意）进行处理”。

第 15 条：儿童数据

对于年龄在 14 岁以下的未成年人，如需处理个信法项下的儿童数据，个人信息处理者（许多其他国家隐私法律中称为“数据控制者”）必须获得监护人的同意。这一要求的触发取决于个人信息处理者是否知道或应该知道其所处理的个人信息系年龄在 14 岁以下的未成年人的个人信息。对于某些专为儿童设计的在线服务和产品而言，这一点相对容易确定。但是，对于混合受众网站而言（例如，网站并非专门面向儿童，但儿童可以使用该服务），情况会更加复杂。核实混合受众网

站的所有到访用户的年龄，确定哪些人是儿童、哪些人不是，从而遵守征得未成年人监护人的同意的要求，这对组织机构而言是一个巨大的负担。此外，这样做需要收集更多的个人信息，例如身份证件，有悖于个信法将信息处理限制到实现处理目的所需的最小范围这一原则。再者，要求用户自主报告年龄的限制机制并不十分可靠，因为儿童可能通过撒谎绕过这些限制。

我们建议修改个信法第 15 条，使个人信息处理者可以通过适当的风险测试，根据具体情况确定其是否可能处理未成年人的个人信息。其中包括考量多重因素，例如所提供的在线服务/产品的性质、服务的可访问性、服务对于儿童的潜在吸引力以及儿童是否已被类似服务或竞争对手的服务所吸引、网站/服务的注册流程是否反映了用户年龄超过 14 岁的假设，等等。

这种方式符合取得同意的要求，即个人信息处理者“应当”知道其在处理未成年人的个人信息。而且，这种方式将确保个人信息处理者征得未成年人的监护人的同意，而无需核实所有用户的年龄以及收集更多的信息来核实。

*建议：*确保个人信息处理者基于诸多因素作出适宜的决定，以确定他们是否正在处理未成年人的信息，从而符合第 15 条对于混合受众网站和服务的要求。

第 21 条：共同个人信息处理者

个信法第 21 条规定，如果个人信息处理者共同处理个人信息，侵犯个人权益的，应当依法承担连带责任。

重要的是要考虑共同个人信息处理者可能在他们处理的数据方面扮演差别较大的角色。因此，共同责任不意味着共同连带责任，因为其中的一个个人信息处理者可能实际开展大部分或主要的处理活动。责任水平应结合处理活动、实际情况以及哪些处理活动侵犯了个人权利和权益等因素进行评定。我们建议全国人大修订个信法第 21 条，规定“如果共同个人信息处理者的活动侵犯个人权益的，应依法并结合有关情形共同承担责任”。

此外，个信法第 65 条规定，能够证明自己无过错的个人信息处理者，可以减轻或者免除责任。这将支持对第 21 条做出上述修订。

*建议：*修订第 21 条，明确共同个人信息处理者的共同责任水平应以处理行为的范围和情况为前提。

第 23 条：兼并、拆分后或因其他理由变更处理的目的

个信法规定，如果合并、分立之后的接收方变更原先的处理目的或处理方式，该接收者应通知个人并应根据个信法的规定重新获得该等个人的同意。我们想强调，如果数据接收者将处理的目的变更为与原处理活动兼容的目的，则无需重新获得同意。如上所述，如果处理目的变更与原先处理目的不兼容，处理个人信息将需要新的合法依据。

建议： 修订第 23 条，阐明在合并和分立的情况下，如果使用数据的新目的与原目的不兼容，个人信息的接收者只需依照新的合法依据处理个人信息。这包括重新获得同意或者依照不同的合法处理依据。

第 24 条：向第三方提供个人信息

个信法第 24 条规定，如果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。

需要强调的是，在某些情况下，向第三方提供信息不要求组织机构单独获得同意。例如，如果处理数据用于履行在线购物交易合同，则可能需要向第三方快递服务提供个人的姓名和地址，以便向个人交付产品。

此外，获得个人的同意并非始终可行。例如，如果个人信息处理者因为疑似税务欺诈需要向税务机关发送财务账户信息，征求个人同意将适得其反。

再者，许多公司利用第三方服务商处理个人数据，用于数据分析和广告。要求单独取得同意以进行该等常规或普通的数据处理活动，将为组织机构（包括目前免费享有许多在线服务的个人）带来重大困难并大幅增加费用。为了避免该等情况，我们建议个信法应加入合法利益作为数据处理的依据（参见以上第 4-5 页）。

而且，第三方接收者在收到数据后其责任的范围不明确。许多第三方是代表个人信息处理者的服务提供商。个信法似乎没有区分个人信息提供商（在一些其他国家的隐私法中被称为“数据控制者”）和第三方服务提供商。我们建议全国人大明确第三方提供商在个信法项下的责任（参见以下第 19 页的更多注释）。

建议：修订第 24 条，说明组织机构向第三方提供信息时不需要获得单独同意的情况。明确第三方服务提供商在个信法项下的责任。

第 25 条：自动化决策

个信法第 25 条规定，利用个人信息进行自动化决策时，个人信息处理者应保证其决策的透明度，并向个人提供拒绝服从自动化决策的权利。

本条目的是保护消费者免遭自动化决策产生的不公正歧视或负面影响。尽管我们了解某些类型的自动化决策需要保护措施，但我们认为第 25 条中拒绝权的适用范围应排除有关 B2B 场景下风险和信用评级分析的自动化决策，因为该等分析有益于提高商业效率和促进公众利益。因此，在 B2B 场景下围绕信用进行的自动化决策不应受限于该等拒绝权。

建议： 修订个信法第 25 条，使该条项下的拒绝权可提供一个例外，即该等拒绝权应不适用于 B2B 风险和信用评级分析的自动化决策。

第 28 条：处理已公开的个人信息

个信法指出，处理已经公开的个人信息时，应当符合该个人信息被公开时的用途。如果处理超出了与所述用途相关的合理范围，个人信息处理者应依法向个人告知并取得其同意。

作为 APEC 的一个成员经济体，中国已经批准了 APEC 隐私框架[6]。该框架第 II 部分指出，对公开可获取的信息具有有限的适用性。其中规定，在信息已经公开以及个人信息控制者未直接向相关个人收集信息的情况下，通知和选择要求一般没有必要。该框架将公开的政府记录或新闻广播或媒体发布的信息列为公开可获取信息的示例。

此外，根据《个人信息安全规范》第 5.6 条[7]，从合法和公开来源（例如新闻报道或政府来源）收集的个人信息，无须向个人征求使用该等数据的同意。

我们建议全国人大根据 APEC 隐私框架和《个人信息安全规范》修订个信法第 28 条。

建议： 修订个信法第 28 条，使个信法与 APEC 隐私框架和中国《个人信息安全规范》对于公开可获取信息的使用规则一致。

第 29 条：敏感数据

根据个信法，敏感个人信息被定义为“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、国籍、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“。

我们不建议设立一个事前确定的“敏感个人信息”类别，因为处理和信息的敏感性大多视情境而定。特定类别的个人信息在各种处理情境中所面临的风险可能并不相同。我们建议隐私保护采取基于风险的方式，要求对所有处理活动进行风险分析，并要求组织机构确定与涉及的实际风险相适应的补救和控制措施。这并不意味着个信法不能列举哪些个人信息可能是敏感信息，但该等列举在开展背景风险评估时应被视为指导方针，而非自动、不变的触发更严格的要求或限制使用该等个人信息。但是，如果全国人大法工委决定在法律中包括该类别，个信法对敏感个人信息的定义有待商榷。

该定义目前将“金融账户信息”和“个人行踪”纳入了敏感信息的类型。该等类型的个人信息定期由个人信息处理者处理，将它们纳入到定义中将妨碍一些常见的处理操作。例如，工作场所常常会出于薪资目的处理财务账户信息。在防范诈骗的背景下也会处理财务账户信息。定期处理个人行踪信息，以提供基于位置的各种服务，包括共享单车和出租车服务、GPS 和地图应用程序以及天气预报信息。征求个人对于处理该等信息的同意对组织机构而言可能过于繁琐，可能引起个

[6]APEC 隐私框架由 21 个 APEC 成员经济体制定，最初于 2005 年确定。参见 APEC 隐私框架，获取链接 https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf。该框架的一部分在 2015 年进行了更新并吸收了 OECD《隐私保护和个人数据跨境流通的指南》（1980 年，于 2013 年更新）引入的概念，适当考虑了 APEC 地区不同的法律特点和背景 https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)。

[7]参见第 5.6(h)条 同意的例外情况，信息安全技术——个人信息安全规范，中华人民共和国国家标准，GB/T 35273-2020。

人产生同意疲劳的问题。我们建议从敏感个人信息的定义中删除“金融账户信息”和“个人行踪信息”（如果该定义在个信法中保留）。

而且，该定义包括一个开放式的“其他信息”类别。目前尚未不清楚“其他信息”如何定义以及由谁定义。这可能会造成法律上的不确定性，并导致组织机构停止处理后续被视为敏感的现有个人信息并征求个人同意。我们建议全国人大法工委在个信法中说明如何确定以及由哪个机关确定该等“其他信息”。此外，在更多类别的个人信息被视为敏感信息之前，个信法应当规定一个公开咨询程序，以便提供适当的通知、接纳利益相关者的意见。

*建议：*修订个信法，针对敏感个人信息的处理启用一套基于风险的方法，而非提供已设定好的预定义敏感信息类别。如果该等预定义的类别在个信法中保留，从定义中删除金融账户信息和个人行踪信息。此外，针对其他敏感个人信息，要明确如何定义以及由哪个机构定义。在个信法范围内添加更多类别的敏感信息之前，应当与所有利益相关者一起开展公开咨询程序。

第 30 条：处理敏感个人信息的同意

个信法第30条规定，基于个人同意处理敏感个人信息的，个人信息处理者应取得个人的单独同意。

现条文未能清楚地指出，除同意以外的其他法律依据是否可用于处理敏感个人信息。首先，第30条规定，如果处理敏感个人信息应以同意为条件，则必须获得单独的同意。如果处理敏感个人信息的第一种情形基于其他依据（例如在紧急情况下为了保护个人的生命和健康而进行处理），这意味着什么？ 个人信息处理者应当能够单独依赖该依据，而无须征求个人的任何同意。

此外，须强调的重要一点，征求同意不适用于许多依赖敏感数据的信息处理形式。例如，使用人脸识别信息确定已知的入店扒窃者或者将生物统计信息用于安全、验证和认证目的。这方面的另一个例子是使用生物统计行为数据阻止试图模仿人类行为的自动化机器人的复杂攻击。为了阻止这些攻击，欺诈预防工具必须依赖关于个人生物特征的信息。如果处理自动化机器人的生物统计数据需要同意，诈骗者可能会选择拒绝同意，以避免被诈骗预防工具发现。

我们建议全国人大法工委明确个人信息处理者可以依赖的其他处理依据，以结合与风险水平相称的适当保护措施处理敏感个人信息。

*建议：*明确第30条确保可基于个信法列明的所有合法处理依据处理敏感个人信息，而且处理该等信息不限于征得同意的依据。

第 36 条：访问政府数据

个信法规定，国家机关不能公开其处理的个人信息，除非法律或行政法规另有规定，或者已获得相关个人的同意。我们想强调政府基于重要研究、创新和其他公共利益目的分享商业数据的重要性。

在中国合理访问政府数据的权限尤其重要，因为很大一部分有用的数据受政府控制。例如，大多个人信用数据由中国人民银行控制，与交通相关的数据由公安部控制。如果被授予访问该等数据的权限，在适当的情况下分析公司可帮助实现更低的汽车保险费和更低的贷款利率，使中国消费

者受益。私营领域也可以使用政府数据为国家、城市和城镇政府机构建立专门的应用程序平台。例如，帮助税务机关防止退税欺诈、帮助银行监管者开展反洗钱或使交通管理部门能够改善当地社区交通堵塞的平台。

*建议：*修改个信法第 36 条，规定为了重要研究、创新和其他公共利益目的而可分享政府数据的情形。

第 38 条：数据跨境提供

我们理解，个信法认可个人信息可为了商业需要可进行跨境提供。个信法第 38 条允许跨境提供个人信息，但个人信息处理者需满足以下条件之一：(1) 依法通过国家网信部门的安全评估；(2) 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；(3)与境外接收方签订合同，约定双方的权利和义务，并监督其个人信息处理活动达到法律规定的个人信息保护标准；或者(4)符合法律、行政法规或国家网信部门规定的其他条件。

为了商业需要跨境传输个人信息的许多组织机构将依赖与境外接收方签订合同的选项，该合同将规定双方的权利和义务，并监督接收者的个人信息处理活动，以确保符合个信法规定的标准。

我们建议明确使个人信息接收者达到个信法中所列标准所需的监督范围。这可以通过国家网信部门的指南完成，该指南规定适当的监督包括在与境外接收方签订合同之前开展尽职调查，在合同中明确传输的目的和接收方的责任，并在个人信息处理者发现接收方有违反合同义务的情况下采取适当的措施。

而且，目前条文未明确通过国家网信部门的安全评估或通过由专业机构进行的个人信息保护认证所涉及的内容。在通过个信法之前或之后，应当尽快优先明确该等事宜。例如，中国已于 2011 年批准 APEC 跨境隐私规则(CBPR)体系[8]，而且作为 APEC 的一个经济体，可以在该跨境传输认证中寻求积极的参与。明确第 38 条提及的认证是否能够确保中国未来参与 APEC CBPR 体系很有用。除了确保跨境传输认证，如同其他主要新的隐私法或立法提案，例如欧盟通用数据保护条例（EU GDPR）（即 GDPR 行为准则和有约束力的公司规则）以及印度提议的个人数据保护法案（即操作规范和集团内计划），个信法还应为相同目的启用行为准则和公司规则。

*建议：*明确个人信息处理者所需的监管范围，以确保个人信息的接收者符合个信法中详细列明的保护标准。说明国家网信部门的安全评估和获得专业机构进行的个人信息保护认证涉及的内容。而且，第 38 条明确的认证是否能够使中国参与 APEC CBPR 并在个信法的现有传输机制中加入行为规范和公司规则。

第 39 条：数据跨境提供的同意

[8] APEC CBPR 的获取地址为：https://cbprs.blob.core.windows.net/files/CBPR%20Policies,%20Rules%20and%20Guidelines%20Revised%20For%20Posting%203-16.pdf。

如果个人信息处理者跨境提供个人信息，个信法第 39 条要求其告知个人境外接收方的身份和联系信息、处理目的和处理方式、拟处理的个人信息类型以及个人可对接收者行使权利的方式。要传输个人信息，个人信息处理者必须还获得个人的单独同意。

首先，我们想强调，除个信法第 38 条列明的要求外，提出获得个人同意的要求是全球数据保护法律相悖，将严重影响组织机构以合法和实益目的进行跨境提供数据。

除其他要求外，需要征得同意可能面临的主要问题包括：

- 该同意要求并不会为个人提供额外的保护。安全评估、个人信息保护认证、与接收者签订合同或中国法律、行政法规或国家网信部门规定的其他要求旨在首先为个人提供强大的保护。事实上，该等机制对数据接收方提出了更多的要求，相比同意提供了更多的保护，因为同意仅向个人提供了选择接受所带来的任何风险。

- 需要征得同意会向个人发出关于传输的不适当讯息，令人不明所以。要求所有跨境传输征求同意可能误导人们认为该等传输可能存在固有的错误或风险。在当代数字经济中，跨境传输对于向消费者提供广泛的产品和服务而言是必要的。

- 要求征得同意给个人施加了不必要的负担。征求个人对每次个人信息传输的同意。将大幅增加个人收到的同意请求数量，为个人增加负担，并会冲淡、损害同意的效力。

- 要求征得同意使个人信息处理者承受了不必要的负担。为了准备满足个信法的要求，组织机构在传输个人信息时必须执行与获得个人信息传输同意相关的机制和程序。这可能使新企业和现有企业产生大额费用，对已经按照许多全球数据保护法律的通常方式建立跨境传输个人信息机制的组织机构造成干扰。

- 要求每次传输个人信息都取得同意未必始终可行。在一些情况下，由于组织机构与个人信息被传输的个人缺乏关系和/或没有其联系信息，无法就传输个人信息获得同意。

除了上述担忧之外，很重要的一点，在国际上，许多国家已经改变了要求跨境传输个人信息征求同意的做法。例如，在传输不能根据充分决定或适当保护进行且个人被告知传输可能有风险的情况下，GDPR 仅允许使用明确的同意作为传输依据。根据 GDPR，征得同意已从跨境传输的一般规则中废除。而且，加拿大隐私专员办公室(OPC)在 2019 年针对跨境数据传输所需的同意开展了一次关于变更其政策立场的公开咨询。在咨询结束时，OPC 最后决定传输不需要征求同意，现行的基于责任追究的方式仍然可用。

如上所述，中国是 APEC 的一份子，已帮助制定并批准 APEC 隐私框架，而且还帮助制定了 APEC 跨境隐私规则体系。APEC 隐私框架的一个核心目标是确保数据在亚太地区自由流动，并推动“避免信息流动壁垒的有效隐私保护”[9]。该框架特别援引了 CBPR 在强化隐私和保持信息在 APEC 经济体以及其交易伙伴之间流动的作用，并鼓励个人信息的责任追究制度[10]。确实，该框架的一个基本假设是创造“信息可以安全和负责任地（例如通过 CBPR 系统）流动的条件”。根据该框架，CBPR

[9]示例参见 APEC 隐私框架前言和序言第 4 段，获取地址 https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf。

[10]*同上*，序言第 8 条。

系统的建立使“个人相信他们的个人信息受到保护”，不管它流向何处[11]。APEC 隐私框架[12]，特别是关于跨境传输部分规定如下：

- *70. 对跨境个人信息流动设置的任何限制应当与传输带来的风险相称，并考虑信息的敏感性以及跨境传输的目的和背景。*

而且，值得注意（而不令人惊讶）的是 APEC CBPR 计划的要求未就跨境数据传输提供选择或个人同意。该等选项与 APEC 和 CBPR 不管在何处为信息提供基于责任的保护前提不一致[13]。

中国建议引入同意要求，因此与 APEC 隐私框架的目标以及 CBPR 的具体目的和要求不一致：使个人信息的地理位置不相关，因为保护措施会随着信息而流动，不管它流向何地。鉴于根据个信法提议的传输框架，已存在充分的保护和适当的措施，鉴于征得同意不能解决额外的风险，也不能增加保护，对跨境传输造成额外障碍。

尽管 APEC 隐私框架和 CBPR 未明确禁止超过 APEC 要求的国内隐私保护，执行与 APEC 和 CBPR 隐私框架前提不一致的新要求值得仔细考虑。中国有朝一日会加入的 CBPR 的部分承诺是，在 APEC 地区（可能扩大到其他地方）统一隐私和数据保护实践。这将是 CBPR 认证为组织机构提供的一个主要益处和激励。因此，任何不必要的国家性背离有可能直接损害一致化的益处，并长期损害 CBPR 的相关性和有效性。

考虑上述因素，我们建议全国人大法工委删除第 38 条针对跨境个人信息传输需要取得单独同意的要求。

此外，第 39 条规定，个人信息处理者向个人提供境外接收方的身份和联系信息，以及个人针对该等接收者行使权利的方式。关于该等第三方的联系信息和身份，法工委应当要考虑每天发生的国际传输规模。取决于传输的性质和个人信息处理者与个人之间的关系，向每个人提供接收方的具体联系信息和身份可能特别繁重且不可行。

而且，关于该权利，个人应当向原来收集他们信息的组织机构提出所有权利请求。当接收方收到与其没有直接关系的个人提出的权利请求时，需要向另一组织核实其收到了该个人的请求。这可能无法核实，因为组织机构可能已从数百家不同的组织机构接收信息，且视传输数据的类型而定，可能无法将该个人与收到的特定信息联系起来。我们建议修订第 39 条，删除此项规定：“个人向境外接收方行使本法规定权利的方式”。在与个人沟通的过程中，重点说明他们如何在必要的情况下向可追溯第三方的个人信息处理者行使他们的权利。

建议： 修订第 39 条，删除第 38 条所列要求之外向境外传输个人信息需要单独同意的要求。删除提供关于个人信息境外接收方的联系详情以及如何针对该实体行使权利的信息的要求。

[11] *同上，第 IV,B,III 部分第 65 和 67 段。*
[12] *同上，第 IV,B,IV 部分第 69 和 70 段。*
[13] 这只有一个有限的例外。该框架的责任原则（第 III 部分，原则 IX，第 32 段加注释）规定，如果国内或国际传输中的个人信息不能通过实施尽职调查或其他合理措施得到保护，组织机构应当获得同意“以确保该信息按这些原则得到保护”。但是，这不属于 CBPR 项下的情形或者用于传输个人数据的任何机制须以确保以适当的水平持续提供保护的适当责任追究措施为前提。

第 40 条：网信部门安全评估

第 38 条所列向境外传输个人数据的选择之一是根据个信法第 40 条完成由国家网信部门组织的安全评估。第 40 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，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中国境内。第 40 条指出，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。

我们理解出于公众利益和国家安全目的，若干形式的信息须在境内存储。然而， 我们建议不要在隐私权法中实行任何形式的数据本地化。鉴于数字化经济的全球性，我们认为，在确保能够通过组织问责制和合理的数据传输机制保护有关信息的情况下，各国应该保证个人信息的自由流动。这种情况在个信法中一个明显的例子就是，各组织机构需通过合同约束双方的权利和义务，进行跨境数据传输 。本地存储个人信息的要求可能会带来以下后果：

- 禁止使用依赖于全球和分销网络的技术（例如数据分析、云计算和人工智能）和机器学习应用。

- 强迫创建冗余存储系统。在中国运营的国际组织可能需要在中国创建冗余存储系统以存储数据，这将产生费用成本、中断业务进程并造成信息安全风险。

- 将成本增加到不利于本地和外国中小型企业的限制性水平。新型市场进入者可能无法利用竞争性云计算服务，而这一点却能使他们能进入市场并与更大的组织展开竞争。外国企业可能没有资金在中国创建冗余存储系统，这事实上阻止了他们进入市场，并阻止了他们为中国消费者提供服务的能力。

- 危及数据安全性。要求将个人信息集中在中国防止组织对遍布全球服务器的数据进行分区处理，这可以提供额外的保护防止黑客入侵，并可以在发生自然灾害时提供业务连续性。

鉴于上述后果，我们建议网信办仔细定义组织触发第 40 条要求而必须处理的个人信息量。该数量应该足够大，以避免对几乎所有组织实施数据本地化要求。为了计算出合理的数量，应该考虑互联网用户的群体和人数。

此外，我们建议个信法为境外跨国公司进行公司内部传输（包括与员工相关的信息传输）提供安全评估的例外。该传输为日常运营所需，将促进对中国投资的增加，因为组织将无须为在中国市场开展业务而成立完全独立的业务实体。

最后，重要的是，安全评估须符合中国《网络安全法》以确保组织的确定性和一致性。

建议： 谨慎定义触发第 40 条安全评估要求的个人信息量。为达到第 40 条基准数量的跨国公司在中国境外进行公司内部提供个人信息（包括与员工相关的信息传输）提供例外。确保第 40 条的要求与中国《网络安全法》内容一致。

第 42 条：外国个人信息处理活动对个人造成危害的后果

个信法第 42 条指出，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,国家互联网信息办公室可以将其列入限制或者禁止个人信息提供名单，予以公告，并采取限制或者禁止向其提供个人信息等措施。

目前尚不清晰在已经向外国组织提供个人信息之后，个人信息处理者组织必须采取哪些措施。我们建议个信法概述，如果该组织的义务只是遵守网信部门规定的措施，还是它必须采取具体的补救措施。这一点可以帮助组织在传输个人信息之前，评估他们的风险和义务。

建议： 概述当网信部门根据第 42 条针对从事损害处理行为的外国个人信息处理者采取措施后，已经向境外实体传输数据的组织必须采取的措施。

第 43 条：针对其他国家和地区的相应措施

个信法规定，任何国家和地区在个人信息保护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该地区采取相应措施。

尽管这些是很实际的问题，但我们相信，此类措施往往是政治和双边贸易讨论的主题，并且不能说明个信法规定的组织义务或个人权利。此外，其他个人信息保护法中通常未规定的这一条款，该条款可能会损害数据保护法应为组织提供法律确定性的意义，无论是在一般合规性还是跨境数据传输方面。我们建议删除个信法第 43 条并通过其他途径解决有关问题。

建议： 删除个信法第 43 条。

第 47 条：删除权

个信法规定个人在若干情况下拥有要求删除他们个人信息的权利。这包括当个人撤回同意时。

在某些情况下，撤回同意导致数据被删除可能会存在很大问题。例如，在医学研究方面，假如某人撤回处理一项临床试验的同意，从试验结果中删除他们的信息可能会影响更广泛领域的试验结果。我们建议个信法对此类情形作出规定并明确第 16 条（撤回同意的权利）仅适用于可以追溯删除数据的删除权且不会妨碍最初所使用数据的整体处理操作。如果这会阻碍处理，则可以选择限制进一步处理数据。

建议： 明确通过撤回同意进行删除的权利仅适用于可以追溯删除数据的情况，并且不会妨碍最初所使用数据的整体处理操作。如果处理被阻碍，则可以选择限制进一步处理数据，而非删除。

第 51 条：指定和登记个人信息保护负责人的义务

个信法第 51 条指出，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。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。另外，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。

这与 2020 年 10 月生效的《个人信息安全规范》中的要求类似，该规范要求在组织处理或预期将处理超过 1,000,000 人的个人信息时，或者处理超过 100,000 人的敏感个人信息时，指定一名内部个人信息保护专员[14]。为了确保个信法和个人信息安全规定之间的一致性，我们建议，同样的上限适用于根据个信法指定一名个人信息保护负责人。

我们建议不需要求向有关当局披露和登记个人的联系信息。这将增加各组织不应有的负担，产生不必要的费用，这些组织在每次雇员离开时以及指定一名新的个人信息保护责任人时必须更新登记。相反，应要求该组织登记其已指定了一名个人信息保护责任人，并随时更新这一任职信息。

*建议：*修改将个人信息保护负责人的联系信息披露给相关主管部门并在相关部门登记的要求，仅需登记该保护负责人是否已获指定并确保该任职信息准确且最新。将指定个人信息保护负责人这一要求的触发条件与《个人信息安全规范》中的条件保持一致。

第 52 条：设立专门机构或指定代表的义务

个信法第 52 条规定，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。

就设立专门机构而言， 我们建议全国人大阐明此类机构可以包括一家组织的关联公司。

关于指定代表，我们建议个信法纳入对该项规定的具体豁免情况。例如，根据 GDPR，并无要求在临时处理数据时须指定一名代表，在考虑处理的性质、背景、范围和目的后，其并不构成处理大规模敏感信息的情形，不大可能致使自然人的权利和自由面临风险。

*建议：*阐明一家组织的关联公司可以出于第 52 条规定的目的担任专门机构。根据诸如 GDPR 等其他隐私法律中的豁免情形，为在中国境内指定代表这一要求添加豁免情形。

第 53 条：进行审计的义务

个信法要求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。第 53 条也规定，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。

我们建议，个信法要求相关机构向个人信息处理者提供合理充分的通知，要求其聘用专门实体进行有关审计。在聘用新的实体，提供系统、政策、控制权和敏感业务信息之前，可能需要完成内部流程。因此，各组织可能需要一些时间在审计之前做好准备。

*建议：*增添一项要求：要求相关机构向组织提供合理充分通知，以聘用专门实体进行审计。

[14]请查看第 11.1(b)条，载明责任部门和个人，信息安全技术—个人信息安全规范，中华人民共和国国家标准，GB/T 35273-2020。

第 54 条：事前风险评估

个信法要求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：(1) 处理敏感个人信息；(2) 利用个人信息进行自动化决策；(3) 委托处理个人信息、向第三方提供个人信息、公开个人信息；(4)向境外提供个人信息；或(5) 其他对个人有重大影响的个人信息处理活动。

值得注意的是，各组织每天按第 54 条所列活动从事数百万次处理活动。各组织不可能事先对每一项行动进行全面的风险评估。我们认为，应允许组织对其处理活动进行初步风险预筛查，并且仅在筛查或初步风险评估表明处理可能导致个人面临高风险的情况下，才要求进行全面的风险评估。要求在所有数据处理之前进行*全面*风险评估，企业可能无法有效实施。预筛查或初步风险评估将能够从全面风险评估的要求中去除许多无风险或低风险的信息处理活动。

此外，在将个人信息提供给境外第三方时，各组织已经需要遵守个信法第三章中的要求，这使得进行进一步风险评估的要求变得多余。关于对个人产生重大影响的处理活动，目前尚不清楚何种情况构成个信法规定的“重大影响”。网信办应就可能产生重大影响的处理类型提供明确的指导，这些处理类型可通过组织进行的风险评估进行阻止。这将为何时需要进行此类风险评估增加一些明确的参数和指南。

*建议：*明确阐明对第 54 条所列的处理活动进行初步预筛查以及在该等筛查表明对个人存在高风险的情况下，实施全面风险评估，该举措足以充分满足第 54 条中对于开展“事先风险评估”的要求。

第 55 条：泄露通知

个信法第 55 条要求个人信息处理者在发现个人信息泄露时，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。

目前，个信法没有提供需向当局通报数据泄露事件的造成危害的基准数。对于个人而言，如果个人信息处理者已采取措施有效避免因泄露而造成的损害，则无需通知。因此，个人信息处理者必须毫无区别地将所有泄露行为通知有关当局。这可能导致各组织报告过多，并可能出现通知疲劳和当局负担过重的风险。我们建议全国人大在个信法中增加一个限制，即只有那些可能对个人造成伤害或风险的个人信息泄漏才需要通知有关当局。对于发送给个人的通知， 我们建议设定相同或更高的基准（这在其他隐私和泄露通知法律中是常见的）。

此外，通知的时机在个信法中并不清晰。对于立法者来说，确定适当的时机义务是一个重要的挑战，他们试图平衡不适当的延迟与仓促通知的相关风险。一方面，延迟通知可能会阻止受影响的个人收到有关其数据风险的可操作信息，以及可能采取的保护措施。另一方面，仓促通知会增加各组织对问题的性质和范围没有足够的信息，从而过早发出通知的可能性。这将对受影响的个人和相关组织产生负面影响[15]。目前，个信法规定，通知必须在发现数据泄露后立即进行。实际上，

[15]寻求解决方案：统一跨境数据泄露通知规则，Hunton Andrews Kurth 和美国商会，2019 年，获取链接 https://www.huntonak.com/en/insights/seeking-solutions-aligning-data-breach-notification-rules-across-borders.html。

遵守这一要求是不切实际的。组织需要时间来确定违规行为是如何发生的，了解违规行为的严重程度，通过聘请外部专业人员进行司法调查，了解内部必须采取哪些行动来恢复受影响系统的合理完整性，收集所有相关事实以进行报告等。这可能需要很多天，甚至几周才能完成。我们建议个信法要求在最适宜的时间内提供通知，不得有不合理的延迟，且不得晚于实体发现数据泄露 后的指定天数（例如 30 天或 45 天）后。这一要求表明当实体(1) 确定发生了泄露；或 (2) 收到发生泄露的通知(例如收到来自执法机构或服务提供商的通知)时，将开始计算通知的时限[16]。

*建议：*在第 55 条中，增加并提高触发报告有关当局和通知个人数据泄露的造成危害的基准数量。修订通知泄露的要求，从“确认后立即”改为在最快的时间内，不得有不合理的延迟，且不得晚于实体发现数据泄露后的指定天数（例如 30 天或 45 天）后”。

第 58 条：当局的职责

个信法第 58 条指出，国家网信部门和国务院有关部门按照职责权限组织制定个人信息保护相关规则、标准，推进个人信息保护社会化服务体系建设。

目前尚不清楚这种制度意味着什么，也不清楚这种制度对公司的要求是什么。

我们建议国家网信部门和国务院有关部门说明推进这种制度需要举行公众咨询，以听取利益相关者的意见，并应在制度生效前作出解释。

*建议：*澄清如何推进个人信息保护社会化服务制度，需要就建议的服务进行公众咨询，解释该制度并征集利益相关者的意见。

第 62 条：责任和罚款

个信法第 62 条规定，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。第 62 条还指出，如果违法行为情节严重的，履行个人信息保护职责的部门还可另行处五千万元以下或者上一年度营业额百分之五(5%)以下罚款。

我们认同侵犯个人信息的违法行为的第一级罚款符合《中国网络安全法》第 64 条的规定。就第二级罚款而言，尚不清楚何种情形构成“情节严重”的违法行为。我们建议全国人大在个信法的下一次审议中澄清这种行为的定义。对于情节严重的违法行为的罚款数额，目前尚不清楚，在哪些情况下，罚款金额将高达五千万元以下或营业额百分之五(5%)。澄清(1)罚款的设定金额或营收的百分比相应的情形，以及(2)所指营收与在中国的营收相关的情况。

个信法还就任何违反个人信息的违法和严重非法行为对任何负责人或其他直接责任个人施加责任。我们认为，代表雇用他们的法人并以官方身份行事的自然人，除非他们是高级官员或董事，并且有故意或重大过失，并为了获得财务或类似利益而行事，否则不应对违法行为承担个人责任。因此类违法行为，对个人，特别是对内部数据隐私专家/个人信息保护专员追究刑事责任，将损害组织寻找负责处理个人数据的合格信息保护人员和类似工作人员的能力，从而破坏该法的宗旨。因

[16] *同上。*

此，我们建议澄清任何负责人或其他直接责任个人是指为财务或类似利益（而不仅仅是违反法律）而故意或造成严重过失的公司高级人员或董事，因为这也包括较低级别的违规行为和任何疏忽行为。

*建议：*澄清何种情形构成第 62 条所述的“情节严重”的违法行为。对于此类行为，澄清罚款何时为设定的货币金额或营收的百分比，以及所指营收与在中国的营收有关。澄清第 62 条规定的个人责任仅适用于因财务或类似利益而故意或造成重大过失的公司高级官员或董事。

第 63 条：个信法侵权对信用档案的影响

个信法第 63 条规定，有任何违反个信法的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

我们没有看到个信法违规和信用风险之间的联系。我们建议删除第 63 条，并在第 62 条及相关条款范围内处理任何侵权处罚。

*建议：*删除个信法第 63 条。

第 69 条：定义

第 69 条定义了“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或个人。与其他数据保护法律不同，个信法似乎只引用了个人信息处理者的义务，在一些其他国家的隐私法律中，这些信息处理者称为“数据控制者”。但是，还有其他行为者参与处理个人信息，包括第三方服务提供商。例如，云服务提供商、工资结算公司等。个信法没有详细说明这些实体的义务，也不清楚这些实体在何种程度上被个信法所涵盖。我们建议澄清第三方服务提供商在个信法中与个人信息处理者相关的角色。
此外，建议全国人大法工委在起草工作中将“个人信息处理者”一词替换为“个人信息控制者”。第三方服务提供商在其他司法管辖区通常称为“数据处理者”，我们建议在提及此类服务提供商时加入术语“个人信息处理者”。这些术语是全球公认的术语，随着中国组织在全球经济中的参与，这些术语的纳入不仅将确保在全球范围内的一致性，而且还将因个人信息安全规范所指的“个人信息控制者”而在国内范围内确保一致性。[17]

此外，第 69 条定义了“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。这是一个非常高的标准，因为没有什么是完全不可逆的。我们认为，全国人大应该在第 69 条中阐明，对于个人信息处理者或其他人使用所有可能手段都不能识别特定自然人的数据，该类数据应被排除在个信法的适用范围之外。这一更现实的标准鼓励各组织采用适合于识别风险的措施对数据进行匿名化，可以通过针对具体情况的适当风险评估程序进行评估。当这与程序、行政和法律保护相结合，防止匿名化（例如，内部问责措施和组织承诺不重新识别数据；与第三方强制执行的合同承诺不重新识别数据；以及法律禁止任何第三方未经授权重新识别数据）时，个人可得到有效保护。

[17]通常请参阅信息安全技术–个人信息安全规范，中华人民共和国国家标准，GB / T 35273-2020。

此外，该修订标准符合个信法第 24 条，该条规定，如果个人信息处理者向第三方提供匿名信息，则第三方不得使用技术或其他手段重新识别个人。根据匿名化的原先定义，这种风险是不可能的，因为数据无法恢复到原来的状态，也无法确定具体的个人。因此，我们认为上述提出的标准与个信法的其余部分更具有一致性。

*建议：*明确第三方服务提供商在个信法下的角色，推荐在个信法中使用更标准化和全球公认的术语，例如“个人信息控制者”（指个人信息处理者）和“个人信息处理者”（指第三方服务提供商）。修订匿名化的定义，以反映合理匿名化的更为现实的标准，外加程序、法律和行政的保障。

第 70 条：生效

虽然目前的草案对法律生效的确切日期、月份和年份没有说明，但我们建议说明各组织有充足的时间遵守个信法，并且从个信法通过之日起不少于两年。这与全球其他隐私法律一致，包括 GDPR 和巴西通用数据保护法(LGPD)。

*建议：*在第 70 条中详细阐明各组织自个信法通过日期起两年内须全面遵守该法律。

联系方式

我们非常感谢有此机会向全国人民代表大会常务委员会法律工作委员会就《个人信息保护法（草案）》提供我们的意见和建议。我们期待未来还有机会对相关立法草案提供意见。

如果法工委希望讨论本文中的任何意见或需要更多信息，请联系：

Markus Heyder(mheyder@huntonAK.com)或
Sam Grogan(sgrogan@huntonAK.com)或
Dora Luo(doraluo@huntonAK.com)。

信息政策领导中心（Centre for Information Policy Leadership）
何威安卓律师事务所（Hunton Andrews Kurth LLP）
联系地址：北京市朝阳区新源南路6号京城大厦2007室
电话： +86.10.8486.2715
传真： +86.10.8486.8565
网站：http://www.informationpolicycentre.com/