

## 信息政策领导中心就《个人信息保护法（草案）》提出的意见

信息政策领导中心 (CIPL)<sup>1</sup> 非常荣幸能有此机会就《个人信息保护法（草案）》(“个信法”)向中华人民共和国全国人民代表大会常务委员会 (“人大常委”) 递交下述意见。

CIPL 曾于 2020 年 11 月就个信法的一审稿向人大常委提供过意见<sup>2</sup>。CIPL 继续支持这些意见，其中许多建议仍与个信法二审稿相关并适用。CIPL 强烈建议人大常委在进一步修订个信法时再次审议我们之前所提的意见，但我们对个信法二审稿的下述意见并不推翻我们此前对下文中所提问题的评论。我们之前就个信法一审稿所提的意见可在此处找到：<https://bit.ly/3exVWo8> (中文版) <https://bit.ly/2Sv2zir> (英文版)。CIPL 建议人大常委考虑我们先前所提的意见，尤其是以下几方面的意见：处理法律依据；儿童和敏感个人信息处理；明确第三方服务提供者与个人信息处理者<sup>3</sup>有关的角色；个人信息的跨境传输（包括符合亚太经合组织 (APEC) 隐私框架和 APEC 跨境隐私规则 (CBPR)；境外个人信息处理者在中国设立专门机构或指定代表；泄露通知规则；以及不合规惩罚。

我们希望个信法的立法能结合《网络安全法》和《数据安全法（草案）》，可以构建一个坚实的数据保护体系。我们注意到人大常委在首次公开征询意见后对个信法一审稿进行了诸多更新，对此我们非常认同。例如，我们认同人大常委明确了“目的限制”概念，确保以对个人权利影响最小的方式限制处理。此外，CIPL 认同人大常委已明确规定，如果个人撤回处理同意，此类撤回不应影响在撤回之前已经发生的处理活动。个信法的这些修订和补充将为寻求遵守该法律的国内和国际组织增加确定性，并确保国家互联网信息办公室 (“网信办”) 等执法部门在依据个信法进行数据保护执法活动时进一步明确的范围。

在本意见里，我们重申了以前的几项建议，我们认为这些建议对于确保有效的隐私法符合全球数据保护规范至关重要。CIPL 还对人大常委接下来有关个信法的工作提出了几个可以重点考量的新

---

<sup>1</sup>CIPL 是何威安律师事务所 (Hunton Andrews Kurth LLP) 的全球隐私和数据政策智库，由该律师事务所和 80 家在全球经济关键领域处于领导地位的成员公司提供资金支持。CIPL 致力于思想领导和发展最佳实践，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。CIPL 的工作可促进全球商业领导者、隐私和安全专业人士、监管部门和政策制定者之间富有建设性的互动。如需更多信息，请访问 CIPL 的网站 <http://www.informationpolicycentre.com/>。本提交材料中的任何内容均不得解释为代表 CIPL 的任何成员公司或何威安律师事务所 (Hunton Andrews Kurth) 的观点。

<sup>2</sup>请参阅 2020 年 11 月 18 日 CIPL 对中国《个人信息保护法（草案一审稿）》的意见，获取地址为 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/%E5%85%B3%E4%BA%8E%E4%B8%AD%E5%9B%BD%E3%80%8A%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95%E5%9F%BC%88%E8%8D%89%E6%A1%88%E5%9F%BC%89%E3%80%8B%E7%9A%84%E7%AB%8B%E6%B3%95%E5%BB%BA%E8%AE%AE - cipl%E6%8F%90%E4%BA%A4.pdf> (中文版) 和 [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_comments\\_on\\_chinas\\_draft\\_personal\\_information\\_protection\\_law\\_18\\_november\\_2020\\_-\\_english\\_.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_chinas_draft_personal_information_protection_law_18_november_2020_-_english_.pdf) (英文版)。

<sup>3</sup>在许多隐私法中，个信法中的“个人信息处理者”被称为“数据控制者”，而“第三方服务提供者”通常被称为“数据处理者”。CIPL 建议人大常委在个信法中采纳这些全球接受术语，以确保中国组织在全球数字经济中互动时保持国内（例如：个人信息安全规范（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) 提及“个人信息控制者”）和全球的一致性。

问题。CIPL 认为，通过采纳以下建议，中国可以更好地将自己定位为全球数字经济领导者，同时为数据主体维护高标准的数据保护、确保私人 and 公共部门数据得到适当保护<sup>4</sup>。

### 1. 进一步明确根据个信法什么情形下需获得个人同意

个信法的第 13 条规定了处理个人信息的若干法律依据，包括个人同意、合同必要性、遵守法定义务或责任、应对公共卫生紧急情况或在紧急情况下保护生命、健康或财产，新闻报道和法律 and 行政法规规定的其他情形。CIPL 认同在个信法二审稿中引入额外的法律依据，在合理范围内处理公开可获得的个人信息。

CIPL 也认同个信法二审稿指出，虽然本法的其他相关条款规定处理个人信息必须征得个人同意，但第 13(2) - 13(7) 条中规定的情况无需征得同意。如果人大常委在个信法其他需征求个人同意才可进行特定处理的条款中交叉引用这一说明，将会很有帮助。例如，根据个信法第 39 条，如果个人信息处理者向境外传输个人信息，除利用第 38 条列举的相关传输机制外，必须获得个人的单独同意。然而，如果向境外传输个人信息对于签订或履行合同是必要的，假设第 13(2) 条规定的情况适用于这种情形，从字面看上去可以在无需征得个人同意的情况下进行这种跨境传输。

建议：在个信法规定的其他需获得个人同意才可进行的特定处理活动之条款中交叉引用说明第 13(2)- 13(7) 条中所规定的不需要征得个人同意的情形，以明确只有在没有其他处理法律依据的情况下才需要获得该等个人同意。

### 2. 进一步明确撤回同意的影响

如上所述，CIPL 认同人大常委明确了如果个人撤回对其个人信息处理的同意，该类撤回不应影响在撤回之前已经发生的个人信息处理活动。CIPL 建议人大常委进一步明确，对于特定的依赖数据集完整性的正在进行的处理，例如在撤回同意之前已经开始的医学研究，撤回同意也不应影响此类正在进行的处理。

建议：明确撤回同意不影响依赖数据集完整性的正在进行的特定处理，且已获得个人最初同意（例如，为已经开始的医学研究处理数据）。

### 3. 增加合法利益处理依据

CIPL 认为，个信法将受益于增加合法利益类型处理依据，以确保在个人同意可能无法实行、不可行或无效的情况下，对于不完全符合其他现有的处理依据的常规和普通的个人信息处理在中国仍然可以进行。例如，处理网络 and 信息安全信息；发现、防止或调查欺诈或犯罪；处理员工数据；个性化在线内容；以及以实现社会公益和社会效益为目的。

---

<sup>4</sup>请注意，本次提交的意见是基于《个人信息保护法》的两种非官方翻译。因此，我们对某些问题的特定意图或细微差别的理解可能存在偏差。在某种程度上，如果任何特定意见确实存在偏差，请忽略此提交材料的相关部分内容。

合法利益或与其性质相似的处理依据正在成为许多现代隐私法的标志。例如《欧盟通用数据保护条例》（GDPR）、巴西《通用数据保护法》（LGPD）和最近修订的新加坡《个人数据保护法》（PDPA）都包含了有关处理的合法权益依据<sup>5</sup>。

在个信法中增加合法利益将要求个人信息处理者采取平衡原则或评估，以证明其或第三方具有处理个人信息的合法权益，且该等利益不会被数据主体的权利推翻。该等平衡评估还必须向隐私执法机关（如网信办）证明。通过适用此类平衡原则，组织机构可以确保适当的以风险为基础实施补救、控制的优先次序，并根据实际风险提供更有效的数据保护。

印度拟议的《个人数据保护法案》中有更为狭义、更不具灵活性的合法权益处理依据<sup>6</sup>。如果法律规定基于合理目的处理个人信息是必要的，在考虑多种因素的情况下（包括是否能够合理期待个人信息处理者可以获得个人的同意），“合理目的”依据允许在不征得同意的情况下处理个人信息。如果不在个信法中包含“合法权益依据”，这可能是一个可供考虑的替代方案，尽管不那么灵活，也缺乏保护性。

**建议：**鉴于“合法权益依据”越来越多地出现在全球数据保护的法律法规中，其可以确保许多未能被其他法律依据包含的处理操作形式仍然可以实现，CIPL 建议人大常委在下一个版本的个信法加入处理的合法权益依据。

#### 4. 采用一种基于风险的方法来确定一个组织是否在混合受众网站中处理未成年人的个人信息

个信法草案二审稿要求处理 14 岁以下未成年人个人信息的个人信息处理者获得未成年人的父母或监护人的同意。CIPL 建议人大常委采用一种基于风险的方法，让组织机构判断它们是否在混合受众网站里处理未成年人的个人信息。这种方法可以包括诸多考虑因素，例如，所提供的在线服务/产品的性质、服务的可获得性、服务对儿童的潜在吸引力以及儿童是否被类似或竞争的服务所吸引、网站/服务的注册过程是否反映了用户年龄在 14 岁以上的假设等<sup>7</sup>。这样就可以无需验证每一个用户的年龄（这可能会引起重大的数据保护和数据最小化问题）而在该等混合受众平台/网站上处理个人信息。当然，对于明确面向儿童的网站和平台，组织必须获得父母的同意，才能处理每个使用服务儿童的数据。

**建议：**使个人信息处理者能够根据若干因素做出情境判断，以确定他们是否在处理未成年人的个人信息，以满足第 15 条对混合受众网站和服务的要求。

#### 5. 修订数据跨境传输条款的某些方面

<sup>5</sup>请参阅 GDPR 第 6(1)(f) 条；巴西 LGPD 第 7(IX) 条；2020 年《新加坡个人数据保护法（修正案）》第 3 部分附表 1。

<sup>6</sup>请参阅 2019 年《印度个人数据保护法案》第 14 节。

<sup>7</sup>美国也采用了类似的方法。请参阅遵守《儿童在线隐私保护法 (COPPA)》：常见问题、面向儿童的网站和在线服务（包括混合受众网站和服务）的获取地址为 <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions>。关于这种方法如何作用的讨论，还请参阅 2018 年 3 月 6 日 CIPL 关于涉及儿童数据和同意的 GDPR 实施白皮书，获取地址为 [https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl\\_white\\_paper\\_-\\_gdpr\\_implementation\\_in\\_respect\\_of\\_childrens\\_data\\_and\\_consent.pdf](https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_gdpr_implementation_in_respect_of_childrens_data_and_consent.pdf)。

作为初步观点，CIPL认为，人大常委应恢复个信法第1条规定的保障个人信息有序、自由流动的的总体目标。中国是APEC成员经济体，帮助制定并签署APEC隐私框架和APEC跨境隐私规则体系。APEC隐私框架的核心目标之一是确保数据在亚太地区的自由流动，并推动“避免阻碍信息流动的有效隐私保护”<sup>8</sup>。CIPL理解某些形式的个人信息（例如涉及国家安全利益的高度敏感个人信息）在中国境外的国际传输可能会引起政府、公共利益和安全方面的问题。然而，实现负责任且安全的个人信息跨境传输对于成功且强劲的数字经济至关重要。此外，个信法还就个人信息的跨境传输建立了严格的保护措施，这将解决许多现有问题。因此，CIPL认为，人大常委仍应将个人信息的有序和自由流动需求作为个信法的总体目标。

个信法认识到基于业务需要个人信息可能需要传输到境外。只要满足特定条件，包括与境外接收方签订约束发送方和接收方权利和义务的合同，则允许进行该类传输。个信法二审稿规定，网信部门将为此类传输制定标准合同。CIPL建议，在制定任何示范合同时，网信部门应考虑全球相似的公司，包括东盟(ASEAN)《跨境数据流动示范合约条款》<sup>9</sup>，以及欧盟委员会即将发布的修订版《标准合约条款》。这样做将确保网信部门制作的任何传输示范合同接近现有的传输示范合同。CIPL认为，该等合同的设计应便于缔约各方根据传输情况以及实体之间的总体业务关系灵活地定制协议。

此外，CIPL希望重申此前对个信法一审稿所提的意见中就跨境数据传输提出的几项建议：

- 网信部门应明确组织机构进行个人信息跨境传输的安全评估涉及哪些内容；
- 建议人大常委明确所需的监督范围，以确保接收来自中国的个人信息的境外接收者符合个信法中列举的保护标准。网信部门可以通过制定指南来实现，即规定此类监督包括在与境外接受者订立示范合同之前进行尽职调查、在合同中界定传输目的、以及在接收者违反其合同义务时应采取适当行动。
- 建议人大常委将行为准则和公司规则添加到个信法中列出的现有传输机制中。
- 建议人大常委去除个信法中列出的其他传输要求之外还要征得个人单独同意的要求。CIPL此前曾向人大常委就为什么这种方法对组织来说有问题而且不符合数据保护全球规范提供了详尽的意见。
- 中国于2011年签署了APEC跨境隐私规则(CBPR)<sup>10</sup>，作为APEC经济体，中国有资格寻求积极参与该跨境传输认证。CIPL鼓励中国努力加入CBPR体系，并建议人大常委明确，如果

---

<sup>8</sup> 示例参见APEC隐私框架前言和序言第4段，获取地址为[https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-\(2015\)/217\\_ECSG\\_2015-APEC-Privacy-Framework.pdf](https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf)。

<sup>9</sup> ASEAN跨境数据流动示范合约条款，获取地址为[https://asean.org/storage/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows\\_Final.pdf](https://asean.org/storage/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf)。

<sup>10</sup> 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>。

中国加入该体系，为业务所需跨境数据传输而进行的个人信息保护认证可包括 APEC CBPR<sup>11</sup> 认证。

**建议：**恢复个信法第 1 条中规定的保障个人信息有序、自由流动的的总体目标；在制定个信法中的任何示范合同时，考虑其他管辖区中的现有示范合约条款，并阐明此类合同要求的监管范围，以确保个人数据的接收者符合个信法列举的标准；将行为准则和公司规则添加到个信法规定的现有传输机制列表中；除使用个信法规定所概述的跨境传输机制外，取消需要征得个人单独同意的要求；努力加入 APEC CBPR 体系，并明确在个信法规定的传输认证可能包括 APEC CBPR 和 PRP 认证。

## 6. 明确哪些类型的个人信息处理者需要设立外部独立机构，以监督处理和发布社会责任报告

个信法草案二审稿第 57 条要求向“巨大”数量用户提供“基础性互联网平台服务”并拥有“复杂”业务类型的个人信息处理者“(1) 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；(2) 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；以及(3) 定期发布个人信息保护社会责任报告，接受社会监督”。

虽然这些要求有助于加强组织机构的问责制，但 CIPL 建议人大常委明确触发这些要求的确切条件。哪些类型的互联网平台服务者受此类义务约束？多少用户构成“巨大”数量？“复杂”业务类型是什么样的？此外，人大常委还应进一步明确独立外部机构的角色及其职能，使各组织机构更清楚地了解为此目的建立任何团体的要求。

关于第二条停止为平台内严重违反法律和行政法规处理个人信息的产品/服务提供者提供服务这一要求，人大常委宜明确，这一义务如何适用于不了解其平台上开展的某些活动的平台服务者（例如，云服务提供者的情况）。在此类情况下，人大常委宜明确，这些平台服务者只有在确知平台用户违反法律的情况下才必须停止提供服务。

**建议：**明确触发个信法第 57 条要求的条件，以及这些要求如何适用于不了解其平台上某些活动的互联网平台服务者。

## 7. 从风险管理的角度来规范匿名化，而不是作为一种技术或最终状态

第 72(4) 条将“匿名化”定义为“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”。这一定义似乎强调数据的技术或最终状态，并指向一个要求没有任何重新识别理论可能性的标准。这是一个非常高的标准，因为没有什么是完全不可逆的，并且会对数据分析的使用产生激冷效应，这可能会影响企业和初创企业生态系统的竞争力和创新能力。

CIPL 认为，在考虑到个人信息处理者或任何其他可能使用的所有合理的个人识别手段后，如果未识别出个人，则数据应被排除在个信法的范围之外。这一更现实的标准鼓励各组织机构使用适合于身份认证风险的措施对数据进行匿名化，这可以通过适用于特定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去匿名化时（例如，内部问责措施和组织不重新识别数据的承诺；与第三方签订的不重新识别数据的有强制力的合同承诺；法律禁止任何第三方在未经授权的情况下重新识别身份），个人将得到有效保护。

<sup>11</sup>请注意，APEC CBPR 的配套认证以 APEC 处理者隐私识别 (PRP) 的形式存在。人大常委 还应将 PRP 纳入任何关于为境外数据传输而进行的个人信息保护认证可能包括 APEC CBPR 认证的说明。

正如 CIPL 对个信法一审稿所提出的最初意见中所阐述的那样，该修订后的标准将与个信法第 24 条相一致，该条款规定，如果个人信息处理者向第三方提供匿名信息，第三方不得使用技术或其他手段重新识别个人。根据匿名化的最初定义，这种风险不可能存在，因为数据将无法恢复到原始状态，也无法识别特定个人。因此，CIPL 认为上述提议的标准更符合个信法的其他部分。

建议：修改“匿名化”的定义，以反映结合程序、法律和行政保障措施的更现实的合理匿名化标准。

## 结论

CIPL 非常感谢有此机会就《个人信息保护法（草案）》二次审议稿向人大常委提供意见。除上述意见外，CIPL 强烈建议人大常委再次审议 CIPL 此前对个信法草案一审稿的意见，因为其中一些意见与当前的个信法草案二次审议稿仍然相关。该一审稿意见可在此处找到：<https://bit.ly/3exVWo8>（中文版）<https://bit.ly/2Sv2zir>（英文版）。我们期待今后有机会对个信法的制订提供看法和意见。

如果希望讨论本文件中的任何意见或需要其他信息，请联系 Sam Grogan，邮箱为 [sgrogan@huntonAK.com](mailto:sgrogan@huntonAK.com) 或 Dora Luo，邮箱为 [doraluo@huntonAK.com](mailto:doraluo@huntonAK.com)。