KPMG 上海睿威律师事务所

个人信息保护法（草案）概览

毕马威网络安全

—

2020年11月10日

引言

2020年10月21日，中国人大网公布《中华人民共和国个人信息保护法（草案）》（下称“个保法草案”）全文，并对其公开征求意见。

作为国内首部关于个人信息保护的专门法律，个保法草案的出台势必对组织和个人处理个人信息的各项活动产生重大影响。个保法草案着眼“个人信息处理活动”，厘清适用范围、个人信息及敏感个人信息定义、个人信息处理合法性基础、告知与同意基本要求等，明确了个人信息处理者的各项义务，也提出了国家机关处理个人信息的特别规定。

本文期望从一般商业组织的合规遵从视角出发，总结个保法草案中建议予以关注的个人信息保护工作要点，共同探索在数字化经济时代企业落实个人信息保护工作、变挑战为机遇的有效路径。

目录

概览

> “制定个人信息保护法是进一步加强个人信息保护法制保障的客观要求，是维护网络空间良好生态的现实需要，也是促进数字经济健康发展的重要举措。”
>
> —全国人大法工委

适用范围
- 在中国境内处理个人信息的活动
- 符合条件的在中国境外处理境内自然人个人信息的活动

个人信息处理者
- 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
- “特殊”的处理者：共同处理，委托和受托处理，第三方等

个人信息处理的合法基础
- 取得个人的同意；或
- 合同订立或履行、法定职责或义务履行、应对突发或紧急情况、为公共利益实施新闻报道、舆论监督等行为，法律、行政法规规定的其他情形

个人信息处理者的合规义务
- 组织人员、制度流程、技术防护等
- 受理和处理个人行使权利的申请
- 事前风险评估和事后定期审计

个人信息跨境提供
- 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，应当将在境内收集和产生的个人信息存储在境内
- 事前风险评估和单独同意

法律责任
- 责令整改，没收违法所得，针对组织和人员的罚款，记入信用档案，赔偿损失等
- 罚款上限五千万元以下或上一年度营业额百分之五以下

适用范围和保护对象

适用范围

个保法草案中关于适用范围的约定与中华人民共和国网络安全法（下称“网络安全法”）、中华人民共和国数据安全法（草案）相较均有所不同，在域外适用方面对欧盟通用数据保护条例（European Union General Data Protection Regulation，下称“EU GDPR”）有所借鉴。总体的界定思路尊重“个人信息”本身的数据属性，以“个人信息处理活动”发生地点为核心，弱化了“个人信息处理者”的地域属性，约定“在中华人民共和国境内处理自然人个人信息的活动”，或者符合条件的“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”均适用于本法。*（个保法草案第三条）*

个人信息和敏感个人信息

与民法典、网络安全法相较，个保法草案对“个人信息”定义进行了微调，采取了跟近似EU GDPR的界定标准，即“与已识别或者可识别的自然人有关的各种信息”，并明确匿名化处理后的信息不属于“个人信息”。*（个保法草案第四条）*

个保法草案在“第二章 个人信息处理规则 第二节 敏感个人信息的处理规则”单独约定关于“敏感个人信息”（此前多称“个人敏感信息”），定义“ 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”属于敏感个人信息。与“个人信息”的定义调整类似，“敏感个人信息”亦进行了细微调整，包括从“危害”调整至“严重危害”，弱化对“名誉”的侵害，参照EU GDPR，直接列举类似“种族”、“民族”等信息为“敏感个人信息”。*（个保法草案第二十九条）*

值得注意的是，除了传统个人信息保护法案中通常需要明确的个人信息和敏感个人信息概念外，个保法草案中在“第五章 个人信息处理者的义务”中，也提出“对个人信息实行分级分类管理”的要求，但未明确统一的分级分类标准。实操中应考虑结合各行业实际情况和数据安全分级分类标准，对个人信息作进一步分级分类识别和管理。*（个保法草案第五十条）*

适用范围和保护对象

个人信息处理者

个保法草案在国内体系里面首次提出了“个人信息处理者”的概念，作为承载个人信息保护义务的首要主体。从实质上，个保法草案中约定的“个人信息处理者”更加类似于此前GB/T 35273—2020 及EU GDPR中提及的“个人信息控制者”（Data Controller），具有对个人信息处理活动的自主决定权。（个保法草案第六十九条）

值得注意的的是，实操中组织可能因处理行为的不同，而同时扮演不同类型的个人信息处理者，如共同处理、委托（和受托）处理、甚至包括泛指的“第三方”。特殊类型的个人信息处理者在相应的场景下承担特定的保护义务，如：

- 共同处理：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；*（个保法草案第二十一条）*
- 委托（和受托）处理：委托方承担监督义务，受托方应按约定处理并在在合同履行完毕或者委托关系解除后，将个人信息返还或者予以删除，未经委托方同意不得转委托；*（个保法草案第二十二条）*
- “第三方”：考虑到个人信息处理活动全周期的复杂性和可能的场景，个保法草案中也设置了关于个人信息处理活动中涉及的“第三方”权利义务的兜底约定。 “第三方”作为个人信息的接收方，应当在限定范围内处理个人信息，且不得利用技术等手段基于获取的匿名化信息重新识别个人身份。*（个保法草案第二十四条）*

中华人民共和国境外的个人信息处理者，应当在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。*（个保法草案第五十二条）*

个人信息处理的合法性基础

合法基础

在网络安全法第四十一条的基础上，个保法草案一定程度上扩大了处理个人信息的合法性基础。除了“取得个人的同意”外，如个人信息的处理活动符合下列情形之一的，也可作为处理个人信息的合法基础：*（个保法草案第十三条）*

- 为订立或者履行个人作为一方当事人的合同所必需；
- 为履行法定职责或者法定义务所必需；
- 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；
- 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；
- 法律、行政法规规定的其他情形。

基本原则

草案重申了个人信息保护工作的多项基本原则，充分借鉴了国际上个人信息保护相关法律法规和较佳实践的，包括：合法正当、公开透明、目的明确、最小必要、准确完整、安全可靠等。*（个保法草案第五条、第六条、第七条、第八条和第九条）*

告知与同意

在合法性基础上，个保法草案进一步讨论了关于不同场景个人信息处理的告知与同意要求。通常情况下，处理个人信息应当按照规定恰当地予以告知并获取个人的同意。个人对其个人信息的处理享有知情权、决定权，有权撤回同意或要求补充、更正其个人信息。*（个保法草案第十四条、第十六条、第十七条、第十八条、第四十四条）*

此外，个保法草案中对例外场景进行了进一步明确，比如：

个人信息处理的合法性基础

免除告知

- 第十九条进行了笼统约定，“有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条规定的事项”。

特殊告知：

- 紧急情况：第十九条“紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，个人信息处理者应当在紧急情况消除后予以告知。”
- 合并分立：第二十三条“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。”

特殊同意：

- 儿童个人信息处理：第十五条“个人信息处理者知道或者应当知道其处理的个人信息为不满十四周岁未成年人个人信息的，应当取得其监护人的同意。”

单独同意：

- 向第三方提供其处理的个人信息：第二十四条　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。
- 公开其处理的个人信息：第二十六条　个人信息处理者不得公开其处理的个人信息；取得个人单独同意或者法律、行政法规另有规定的除外。
- 处理敏感个人信息：第三十条、第三十一条　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。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。还应当向个人告知处理敏感个人信息的必要性以及对个人的影响。
- 向境外提供其处理的个人信息：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。

关于告知与同意的详细操作指引，建议可重点参考个人信息安全规范 GB/T 35273-2020以及个人信息告知同意指南（征求意见稿）。

个人信息处理者的保护义务

个保法草案从组织架构、制度流程、技术防护等方面对个人信息安全管理工作提出了明确要求。在总体个人信息保护框架体系中，着重强调了以下方面的内容：

- ❑ **个人信息保护负责人的任命**；*（个保法草案第五十一条）*
- ❑ 个人信息处理人员安全教育和培训；*（个保法草案第五十条）*
- ❑ 个人信息整体内部管理制度和操作规程的制定和落实；*（个保法草案第五十条）*
- ❑ 个人信息分级分类管理；*（个保法草案第五十条）*
- ❑ 个人信息操作权限管理；*（个保法草案第五十条）*
- ❑ 个人信息保存时限管理；*（个保法草案第二十条）*
- ❑ **个人行使权利的申请受理和处理机制**；*（个保法草案第四十九条）*
- ❑ 个人信息处理第三方安全管理；*（个保法草案第二十二条、二十四条）*
- ❑ 个人信息事件应急响应和通知；*（个保法草案第五十五条）*
- ❑ 个人信息安全技术防护（如加密、去标识化等）；*（个保法草案第五十条）*
- ❑ **个人信息处理活动事前风险评估**；以及*（个保法草案第五十四条）*
- ❑ 个人信息保护定期审计等。*（个保法草案第五十三条）*

实操中建议系统化考虑各项个人信息保护工作的建设和落地，详细要求可重点参考系列配套国标，包括但不限于个人信息安全工程指南（征求意见稿），个人信息安全影响评估指南（征求意见稿），个人信息去标识化指南 GB/T 37964-2019，个人信息安全规范 GB/T 35273-2020等等。

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并公开其姓名、联系方式等，同时报送履行个人信息保护职责的部门。*（个保法草案第五十一条）*

个人可行使的权利主要包括如查阅复制、更正补充、撤回删除、解释说明等。*（个保法草案第四十五条、第四十六条、第四十七条、第四十八条、第四十九条）*

关于个人信息处理活动事前风险评估的要求，适用于处理敏感个人信息、个人信息跨境提供、利用个人信息进行自动化决策、个人信息对“外”提供等多个场景，与此前仍在公开征求意见的个人信息安全影响评估国家标准列举的典型评估场景有所重合，具体评估亦可进行借鉴和参照。此类处理情况记录和风险评估报告应当至少保存三年。*（个保法草案第五十四条）*

与数据战略密切相关的几点要求

个人信息跨境提供

个保法草案设置独立章节“第三章 个人信息跨境提供的规则”，约定个人信息跨境提供的前提条件和管控方式。除网络安全法中已提及的关键信息基础设施运营者，个保法草案进一步将个人信息本地化存储的适用范围扩大至“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”，预计将对涉及大量公民信息处理的服务行业，如网上购物、酒店服务等产生重大影响。目前，个保法草案中暂未对“规定数量”进行约定和明确。*（个保法草案第三十八条、第三十九条和第四十条）*

另外，个人信息跨境属于个保法草案中提及的少数需要“单独同意”场景之一，并需进行事前风险评估。*（个保法草案第三十九条和第五十四条）*

公共场所人像采集和识别

针对目前公共场所应用大量图像采集和识别技术的情况，个保法草案中明确约定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，应设置显著的提示标识，且信息只能用于维护公共安全的目的。一般情况下不得公开或者向他人提供，但取得个人单独同意或者法律、行政法规另有规定的除外。*（个保法草案第二十七条）*

与数据战略密切相关的几点要求

处理公开的个人信息

个保法草案对处理已合法公开的个人信息提出了更高的要求。处理活动原则上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，应当依规向个人告知并取得其同意。如果个人信息被公开时的用途不明确的，则应当合理、谨慎地处理；利用已公开的个人信息从事对个人有重大影响的活动，仍应当依规向个人告知并取得其同意。 *（个保法草案第二十八条）*

自动化决策

个保法草案定义“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。 *（个保法草案第六十九条）*

个人信息安全规范 GB/T 35273-2020中已初步明确了关于使用信息系统自动决策机制的相关要求。此前个人信息安全规范GB/T 35273-2020中主要强调了个人信息处理者应向个人提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核。本次个保法草案中补充提出了在个人认为自动化决策对其权益造成重大影响的，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。此外，要求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。 *（个保法草案第二十五条）*

利用个人信息进行自动化决策同样须在事前进行风险评估并对处理情况予以记录。 *（个保法草案第五十四条）*

合规和法律责任

主管部门

个保法草案明确了中央层面由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。同时，国务院各有关部门将依照个人信息保护法和有关法律、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。而地方层面应按照国家有关规定确定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。*（个保法草案第五十六条、第五十七条、第五十八条）*

履行个人信息保护职责应建立有效机制，接收和处理对违法个人信息处理活动的投诉和举报。*（个保法草案第六十一条）*

履行个人信息保护职责的部门依法履行职责时，个人信息处理者应当予以协助、配合，不得拒绝、阻挠。*（个保法草案第五十九条、第六十条）*

法律责任

与网络安全法略有不同的是，目前个保法草案中并未详细约定具体违反某些特定条款的相关责任，而是笼统的阐述了可能的违反后果，包括责令整改，没收违法所得，针对组织和人员的罚款，记入信用档案，赔偿损失等。其中，值得关注的是，关于情节严重的违法行为的罚款金额较此前网络安全法有大幅提升，为五千万元以下或者上一年度营业额百分之五以下罚款，而关于“营业额”的范围，后续期待在落地层面能有进一步的解释和明确。*（个保法草案第六十二条、第六十三条和第六十五条）*

此外，参照EU GDPR，在涉及赔偿责任条款中，个保法草案中亦提及个人信息处理者能够证明自己没有过错的，可以减轻或者免除责任。*（个保法草案第六十五条）*

与个人信息保护相关的法律法规、国家标准清单（节选）

2020

- 中华人民共和国民法典（2021年1月1日生效）
- 中华人民共和国数据安全法（草案）
- 中华人民共和国个人信息保护法（草案）
- 信息安全技术 个人信息安全规范 GB/T 35273-2020
- 信息安全技术 网络数据处理安全规范（征求意见稿）
- 信息安全技术 个人信息告知同意指南（征求意见稿）
- 移动互联网应用（App）收集个人信息基本规范（征求意见稿）
- 移动互联网应用程序（App）个人信息安全防范指引（TC260-PG-20203A）（征求意见稿）
- 移动互联网应用程序（App）收集使用个人信息自评估指南（TC260-PG-20202A）

2019

- 最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释
- 关于开展App违法违规收集使用个人信息专项治理的公告
- App违法违规收集使用个人信息自评估指南
- App违法违规收集使用个人信息行为认定方法
- 儿童个人信息网络保护规定
- 数据安全管理办法（征求意见稿）
- 个人信息出境安全评估办法（征求意见稿）
- 互联网个人信息安全保护指南
- 信息安全技术 个人信息去标识化指南 GB/T 37964-2019
- 信息安全技术 个人信息安全工程指南（征求意见稿）
- 移动互联网应用基本业务功能必要信息规范（TC260-PG-20191A）

2018

- 中华人民共和国电子商务法
- 信息安全技术 个人信息安全影响评估指南（征求意见稿）

2017

- 中华人民共和国网络安全法
- 最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释
- 个人信息和重要数据出境安全评估办法（征求意见稿）
- 信息安全技术 数据出境安全评估指南（征求意见稿）

2017以前

- 中华人民共和国消费者权益保护法
- 中华人民共和国刑法修正案（七）
- 中华人民共和国刑法修正案（九）
- 关于加强网络信息保护的决定
- 电信和互联网用户个人信息保护规定

下一步行动建议

从整体的立法进程而言，个人信息保护法已于2018年被列入十三届全国人大常委会立法规划。2019年经第十三届全国人民代表大会常务委员会第四十四次委员长会议通过，制定《个人信息保护法》被明确列入全国人大常委会2020年度立法工作计划。个保法草案的正式发布表明相关立法进度正在按计划有序进行，后续应持续保持高度关注并及时调整策略。

从上述梳理分享的国内与个人信息保护相关的法律法规及国家标准推进情况，我们也不难发现目前关于个人信息保护工作的开展并非无从下手、无据可依。相反的，目前相对庞杂的合规体系对企业如何在过渡期有效管控个人信息保护风险，特别是在数字化转型和大数据等新技术应用过程中如何同步考虑个人信息保护从而业务发展和部署保驾护航，提出了更高的要求。

从把控企业整体合规风险，确保个人信息安全的角度出发，我们建议立即行动，变被动为主动，从以下方面入手，开展个人信息保护工作：

01

现状摸排，快速诊断

进行现状评估，匹配数字化转型和数据战略，制定总体规划和实施路线图。

02

突出重点，短期速赢

对高风险领域快速整改，通常包括治理和运营模式的搭建，法律文件修订，应急管理和权利请求响应机制搭建、培训教育落实等。

03

由点及面，分步推进

逐步在不同业务单元推进系统化个人信息保护和管理，利用技术支撑管控流程自动化。

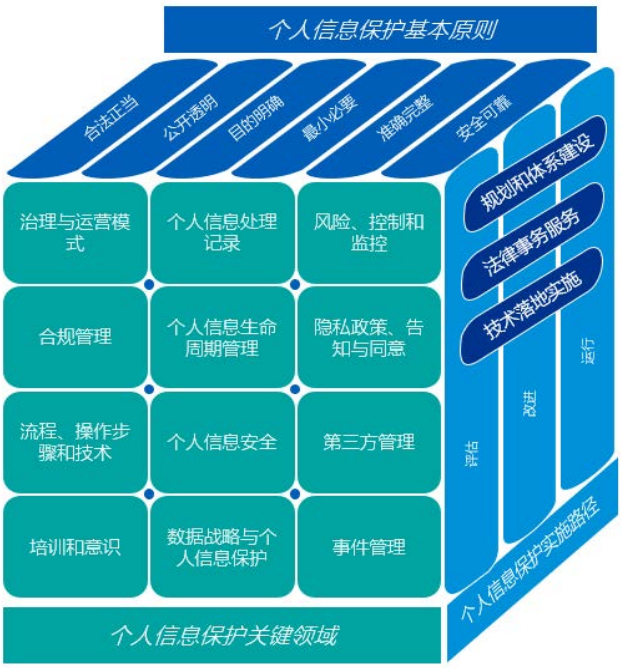
04

良性循环，持续改进

对整体管理体系和流程及技术工具进行优化，以确保符合内外部环境的变化和需求。

毕马威个人信息保护管理框架和服务

毕马威个人信息保护管理框架和服务致力于解决客户真正的业务和技术威胁，协助企业逐步实现和提升。毕马威的个人信息管理成熟度模型除对标各行业通用的个人信息保护要求外，还可根据企业适用的行业特定的个人信息保护要求，如个人金融信息保护技术规范JR/T0171-2020，金融数据安全数据安全分级指南JR/T 0197—2020等进行定制，协助企业快速进行现状评估和目标规划，细化个人信息保护各个组件的建设和改进行动方案，有序全面地推进个人信息保护工作的建设和落地。



全球化的网络安全和法律服务专业团队

丰富的个人信息保护评估、规划、落地实施经验

良好的网络安全生态圈互动与协作关系


Shift
Pg Dn
End

联系我们

石浩然
毕马威中国
网络与信息安全咨询
服务合伙人
电话：+852 2143 8799
henry.shek@kpmg.com

张令琪
毕马威中国
网络与信息安全咨询
服务合伙人
电话：+86 (21) 2212 3637
richard.zhang@kpmg.com

张倪海
毕马威中国
网络与信息安全咨询
总监
电话：+852 2847 5062
brian.cheung@kpmg.com

黄芃芃
毕马威中国
网络与信息安全咨询
总监
电话：+86 (21) 2212 2355
quin.huang@kpmg.com

郝长伟
毕马威中国
网络与信息安全咨询
总监
电话：+86 (10) 8508 5498
danny.hao@kpmg.com

吴永胜
上海睿威律师事务所
数据和知识产权保护
服务合伙人
电话：+86 (21) 5203 1587
rocky.wu@kpmglegal.com.cn