

中华人民共和国个人信息保护法(草案)

(二次审议稿)

目 录

第一章 总 则

第二章 个人信息处理规则

第一节 一般规定

第二节 敏感个人信息的处理规则

第三节 国家机关处理个人信息的特别规定

第三章 个人信息跨境提供的规则

第四章 个人在个人信息处理活动中的权利

第五章 个人信息处理者的义务

第六章 履行个人信息保护职责的部门

第七章 法律责任

第八章 附 则

第一章 总 则

第一条 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。

第二条 自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

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。

第五条 处理个人信息应当采用合法、正当的方式，遵循诚信原则，不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条 处理个人信息应当具有明确、合理的目的，并应当限于实现处理目的所必要的最小范围、采取对个人权益影响最小

的方式，不得进行与处理目的无关的个人信息处理。

第七条 处理个人信息应当遵循公开、透明的原则，公开个人信息处理规则，明示处理的目的、方式和范围。

第八条 处理个人信息应当保证个人信息的质量，避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条 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。

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。

第十一条 国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关行业组织、社会公众共同参与个人信息保护的良好环境。

第十二条 国家积极参与个人信息保护国际规则的制定，促进个人信息保护方面的国际交流与合作，推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等的互认。

第二章 个人信息处理规则

第一节 一般规定

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。

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。

第十五条 个人信息处理者处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意。

第十六条 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。个人信息处理者应当提供便捷的撤回同意的方式。

个人撤回同意，不影响撤回前基于个人同意已进行的个人信

息处理活动的效力。

第十七条 个人信息处理者不得以个人不同意处理其个人信息或者撤回其对个人信息处理的同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。

第十八条 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；

（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。

第十九条 个人信息处理者处理个人信息，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款规定的事项。

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及时告知。

第二十条 个人信息的保存期限应当为实现处理目的所必要的最短时间。法律、行政法规对个人信息的保存期限另有规定的，从其规定。

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人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。

第二十二条 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、期限、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；委托合同不生效、无效、被撤销或者终止的，受托方应当将个人信息返还个人信息处理者或者予以删除，不得保留。

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。

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。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，应当依照本法规定重新取得个人同意。

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。

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，应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。

第二十六条 个人信息处理者不得公开其处理的个人信息，取得个人单独同意的除外。

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。

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。

第二节 敏感个人信息的处理规则

第二十九条 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。

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。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。

第三十一条 个人信息处理者处理敏感个人信息的，除本法第十八条第一款规定的事项外，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。

第三十二条 法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的，从其规定。

第三节 国家机关处理个人信息的特别规定

第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。

第三十四条 国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。

第三十五条 国家机关为履行法定职责处理个人信息，应当依照本法规定向个人告知并取得其同意；法律、行政法规规定应当保密，或者告知、取得同意将妨碍国家机关履行法定职责的除外。

第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行风险评估。风险评估可以要求有关部门提供支持协助。

第三十七条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息，适用本法关于国家机关处理个人信息的规定。

第三章 个人信息跨境提供的规则

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。

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。

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。

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。

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的处理活动的，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。

第四十三条 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对等采取措施。

第四章 个人在个人信息处理活动中的权利

第四十四条 个人对其个人信息的处理享有知情权、决定权，有权限制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。

第四十五条 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。

第四十六条 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的，个人信息处理者应当对其个人信息予以核实，并及时更正、补充。

第四十七条 有下列情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除：

（一）处理目的已实现或者为实现处理目的不再必要；

（二）个人信息处理者停止提供产品或者服务，或者保存期限已届满；

（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除存储和采取必要的安全保护措施之外的处理。

第四十八条 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。

第四十九条 自然人死亡的，本章规定的个人在个人信息处理活动中的权利，由其近亲属行使。

第五十条 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。

第五章 个人信息处理者的义务

第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人的影响、可能存在的安全风险等，采取必要措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露或者被窃取、篡改、删除：

(一) 制定内部管理制度和操作规程；

(二) 对个人信息实行分类管理；

(三) 采取相应的加密、去标识化等安全技术措施；

(四) 合理确定个人信息处理的操作权限，并定期对从业人

员进行安全教育和培训；

(五) 制定并组织实施个人信息安全事件应急预案；

(六) 法律、行政法规规定的其他措施。

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。

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。

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；

(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。

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；

(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。

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）对严重违法法律、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，接受社会监督。

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。

第六章 履行个人信息保护职责的部门

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。

第六十条 履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

- (二) 接受、处理与个人信息保护有关的投诉、举报；
- (三) 调查、处理违法个人信息处理活动；
- (四) 法律、行政法规规定的其他职责。

第六十一条 国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作：

- (一) 制定个人信息保护具体规则、标准；
- (二) 针对敏感个人信息以及人脸识别、人工智能等新技术、新应用，制定专门的个人信息保护规则、标准；
- (三) 支持研究开发安全、方便的电子身份认证技术；
- (四) 推进个人信息保护社会化服务体系建设，支持有关机构开展个人信息保护评估、认证服务。

第六十二条 履行个人信息保护职责的部门履行个人信息保护职责，可以采取下列措施：

- (一) 询问有关当事人，调查与个人信息处理活动有关的情况；
- (二) 查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料；
- (三) 实施现场检查，对涉嫌违法个人信息处理活动进行调查；
- (四) 检查与个人信息处理活动有关的设备、物品；对有证据证明是违法个人信息处理活动的设备、物品，向本部门主要负责人书面报告并经批准，可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责，当事人应当予以协助、配合，不得拒绝、阻挠。

第六十三条 履行个人信息保护职责的部门在履行职责中，发现个人信息处理活动存在较大风险或者发生个人信息安全事件的，可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈，或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施，进行整改，消除隐患。

第六十四条 任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 法律责任

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，给予警告，没收违法所得；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。

第六十六条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第六十七条 国家机关不履行本法规定的个人信息保护义务的，由其上级机关或者履行个人信息保护职责的部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

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。

第六十九条 个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、履行个人信息保护职责的部门和国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十条 违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第八章 附 则

第七十一条 自然人因个人或者家庭事务处理个人信息的，不适用本法。

法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。

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。

第七十三条 本法自 年 月 日起施行。