

《个人信息保护法（草案）》 十大核心亮点

◆丹青/文

近日，《中华人民共和国个人信息保护法（草案）》公布并公开征求社会公众意见。该草案确立了“告知-同意”为核心的个人信息处理一系列原则，明确国家机关对个人信息的保护义务，全面加强个人信息的法律保护。草案共八章七十条内容，本文梳理了草案的十大核心亮点内容，以供参考。

亮点一：明确我国个人信息及相关概念的定义

草案明确规定了个人信息、敏感个人信息、个人信息的处理、个人信息处理者以及自动化决策、去标识化、匿名化等相关概念的定义。（草案第四条、第二十九条、第六十九条）

亮点二：明确了本法的适用范围，突出强调必要的域外适用

草案基于数据流动性的实际情



况和有关国家、地区的现行做法，在坚持“属地管辖”原则的同时，突出强调三种情况下必要的域外适用效力，包括以向境内自然人提供产品或者服务为目的；为分析、评估境内自然人的行为；法律、行政法规规定的其他情形。同时，对相关情况下境外主体提出明确的合规

要求。（草案第三条、第五十二条、第六十八条）

亮点三：确立个人信息处理应当遵循的五大基本原则

1. 处理个人信息应当采用合法、正当的方式，遵循诚信原则；
2. 处理个人信息应当具有明

确、合理的目的,限于实现处理目的的最小范围;

3.处理个人信息应当遵循公开、透明的原则,明示其处理规则;

4.处理个人信息应当确保信息准确,并及时更新;

5.个人信息处理者应采取必要措施保障所处理个人信息的安全。(草案第五条至第九条)

亮点四:确立了以“告知-同意”为核心的个人信息处理规则体系

1.草案明确了“告知-同意”是个人信息处理的首要原则,即“个人在充分知情的前提下,自愿、明确做出的意思表示”。

2.草案规定了个人信息处理者在处理个人信息前应当向个人告知的四类事项,强调告知方式的显著明示和语言的清晰易懂,同时规定了基于保密要求的不需告知情形和紧急情况下的事后告知。

3.草案强调重要事项发生变更后,应当重新取得个人同意,包括个人信息的处理目的、处理方式、信息种类、个人信息处理者因控制权变动发生个人信息转移等。

4.草案明确个人有权撤回对个人信息处理的同意,且个人信息处理者不得以个人不同意为由拒绝提供产品或者服务。

5.草案基于实际情况,规定了五种基于个人同意以外合法处理个人信息的情形,包括订立/履行合同所必需、履行法定职责或义务所必需、应对公共卫生事件和紧急避险

所必需、公共报道和舆论监督所合理必需、其他情形。

6.草案对个人信息的共同处理、委托处理、向第三方提供等实际情况提出了针对性要求,并对匿名化信息识别、自动化决策、公共场所的身份识别、处理已公开的个人信息等社会关切热点问题做出了明确回应。(草案第十三条至第二十八条)

亮点五:对敏感个人信息处理提出增强性要求

1.草案设立专节对处理敏感个人信息作出增强性的规定,强调只有在具有特定的目的和充分的必要性的情形下方可处理敏感个人信息,并且应当取得个人的单独同意或者书面同意。

2.草案强调处理敏感个人信息的告知,除个人信息的一般告知事项,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。

3.草案强调针对敏感个人信息的法律适用,应当以“从严适用”为原则。(草案第二十九条至第三十二条)

亮点六:对国家机关处理个人信息提出特别规定

1.草案设立专节规定国家机关处理个人信息的规则,在保障国家机关依法履行职责的同时,要求国家机关处理个人信息应当依照法律、行政法规规定的权限和程序进行,不得超出履行法定职责所必需的范围和限度。

2.草案要求国家机关处理的个人信息应当在境内存储,确需向境外提供的应当进行风险评估。(草案第三十三条至第三十七条)

亮点七:完善个人信息跨境流动规则,强调国际数据规则“对等”原则

1.草案明确了个人信息处理者



向境外提供个人信息的,至少要符合四类合规规则中的其中一条,包括通过国家网信部门的安全评估、个人信息保护认证、合同约定并达到本法要求、其他条件。

2.草案明确了个人信息处理者在个人信息出境前应当向个人告知的事项,包括接收方的身份、联系方式、处理目的、处理方式以及维权方式等,并取得个人的单独同意。

3.对关键信息基础设施运营者、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、国际司法和行政执法协助、国际条约规定等情形下的个人信息出境提出针对性要求。

4.明确赋予国家网信部门对境外从事危害我国个人信息权益、国家安全和公共利益的个人信息处理活动采取限制或禁止措施的权力,以充分保护我国境内主体的合法权益。

5.强调“对等原则”,明确强调国家有权针对我国的歧视性措施的国家 and 地区采取相应措施。(草案第三十八条至四十三条)

亮点八:明确个人信息处理活动中个人权利和处理者义务

1.草案与《民法典》第1034~1039条规定相衔接,明确在个人信息处理活动中个人的各项权利,包括知情权、决定权、查询权、更正权、删除权和规则说明权等,并要求个人信息处理者建立个人行使权利的申请受理和处理机制。



2.草案明确个人信息处理者的个人信息合规管理义务,包括制定内部管理制度和操作规程、对个人信息进行分级分类管理、采取相应的安全技术措施、合理确定个人信息处理的操作权限和定期人员安全教育培训、制定并组织个人信息安全事件应急预案、定期对其个人信息活动进行合规审计等。

3.草案对个人信息达到国家网信部门规定数量的个人信息处理者,和境外个人信息处理提出针对性合规要求,包括确定个人信息保护负责人等。

4.草案明确个人信息处理者应当进行事前风险评估的个人信息处理活动,包括处理敏感个人信息、自动化决策、委托处理和向第三方提供、信息公开、个人信息出境等,并规定了风险评估的内容事项。

5.草案强调个人信息处理者的个人信息泄露通知和补救义务,明确了泄露通知对象(主管部门和个人)和事项(事件原因、信息种类、事件危害、补救措施等)。(草案第四十四条至第五十五条)

亮点九:健全个人信息保护的体制机制

1.草案明确了国家网信部门负责个人信息保护工作的统筹协调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;地方的个人信息保护和监督管理职责按照国家有关规定确定。

2.草案明确上述部门应当履行的个人信息保护职责,包括开展相关宣传教育、接受和处理有关投诉举报、调查和处理违法事件等。

3.草案明确了履行个人信息保护职责的部门可以采取的措施和相应条件、程序,包括询问、查阅和复制资料、现场检查、查封和扣押、约谈和要求整改等。(草案第五十六至六十一条)

亮点十:加强了对个人信息违法的惩治力度

1.草案明确了对于违反本法规定处理个人信息、或未按照规定采取必要安全保护措施的,情节严重的可以处以五千万以下或上一年度营业额百分之五以下的罚款,并可责令其暂停相关业务、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。

2.草案明确个人信息处理者的个人信息处理活动侵害个人信息权益的,应当按照个人因此受到的损失或者个人信息处理者因此获得利益承担赔偿责任。(草案第六十二条至第六十七条) 