



《网络安全法》 概览

管理咨询
毕马威中国
—
2017年2月

目录

《网络安全法》立法历程	4
《网络安全法》带来的挑战	5
《网络安全法》版本对比	6
《网络安全法》关键点及解读	7
毕马威中国的网络安全服务	15

《网络安全法》立法历程

在《网络安全法》立法前，在国家层面已有一些专题性的信息安全法律法规、规章条例，如《计算机病毒防治管理办法》、《信息安全等级保护管理办法》等。随着我国对网络安全的重视程度不断提高，《网络安全法》也应运而生。在历时一年多的立法过程后，《网络安全法》于2016年11月由全国人大表决通过，并将于2017年6月正式生效。



《网络安全法》带来的挑战



《网络安全法》的重要元素

1

个人信息保护

- 强调个人信息及隐私的保护
- 规范个人信息的收集和使用
- 企业的关注点应从单纯的“数据安全”延展至影响范围更广的“个人隐私保护”

2

网络运营者的安全要求

- 明确网络运营者的定义及安全要求
- 大部分大型金融机构都可能成为“网络运营者”

3

关键信息基础设施

- 对关键信息基础设施的保护提出了较高的要求
- 明确尚未正式明确关键信息基础设施的范围

4

个人信息和业务数据传输至境外的限制

- 外资企业及组织机构通常需要传输至海外
- 《网络安全法》要求敏感数据应存储在本地

5

处罚规定

- 明确处罚措施，包括暂停业务活动
- 严重的违法行为将导致停业整顿或吊销执照
- 处罚金额最高可至100万元

《网络安全法》版本对比



《网络安全法》草稿与终稿的重要修改

《网络安全法》在定稿前经过多次讨论与修改。在草稿与最终稿之间，可以发现有以下值得关注的修改内容：

条目	最终稿	关键修改
第三十一条	国家对 <u>公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施</u> ，在网络安全等级保护制度的基础上，实行重点保护……	明确了哪些行业和领域需要“重点保护”其关键信息基础设施。
第四十三条	……发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。 <u>网络运营者应当采取措施予以删除或者更正。</u>	增加了公民对个人信息的保护权利，且新增了网络运营者及时更正个人信息的义务。
四十六条	任何个人和组织 <u>应当对其使用网络的行为负责</u> ，不得设立用于实施诈骗，传授犯罪方法……的网站、通讯群组。	强调了个人及组织是“使用网络的行为”的责任主体。
第七十六条（五）	个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于 <u>自然人的</u> 姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。	本条将个人信息保护的适用范围从“公民”扩大至“自然人”。
第六十三条	违反本法第二十七条规定，从事危害网络安全的活动……情节较重的，处五日以上十五日以下拘留，可以并处 <u>十万元以上一百万元以下</u> 罚款。	本条将违反《网络安全法》的最高处罚金额提升至人民币一百万元。

《网络安全法》关键点



《网络安全法》关键点

《网络安全法》共七章七十九条，明确了多方面的网络安全要求，包括维护国家网络空间主权、保护关键信息基础设施与重要数据、保护个人隐私信息、明确各方网络安全义务等。纵观《网络安全法》，毕马威认为企业及相关组织机构应重点关注以下关键内容：



个人信息保护

《网络安全法》明确了对于个人信息收集、使用及保护的要求。



关键信息基础设施

“关键信息基础设施”的保护要求在《网络安全法》中反复提及。



网络运营者

“网络运营者”：网络的所有者、管理者和网络服务提供者。《网络安全法》明确了网络运营者的多项安全职责。



敏感信息保存

《网络安全法》要求在境内运营收集或产生的个人信息/重要数据，应在境内存储。



安全产品认证

网络关键设备和网络安全专用产品应在安全认证合格后，方能销售或提供。



法律责任

对于违反《网络安全法》的企业及组织机构，最高处罚金额可达100万元人民币。

关键点解读 – 个人信息保护

个人信息的收集	第二十二条	网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意.....
	第四十一条	网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则.....
	第四十四条	任何个人和组织不得窃取或者以其他非法方式获取个人信息.....



毕马威解读：

- 上述条目强调必须在“用户知晓并同意收集目的和使用范围”后，方能收集个人信息。
- 实际情况中，公民在多种场合均需提供个人信息，包括教育、医疗、公共交通、线上线下交易等。这些法律条款从源头上规范了企业及相关机构对个人信息的获取途径、获取方式。

个人信息的收集	第四十一条	网络运营者.....应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。
	第四十二条	网络运营者不得泄露、篡改、毁损其收集的个人信息.....
	第四十三条	个人发现网络运营者违反法律.....，有权要求网络运营者删除其个人信息.....
	第四十五条	依法负有网络安全监督管理职责的部门.....必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密.....



毕马威解读：

- 上述条目明确了对个人信息保护的要求，尤其是针对个人信息的泄露、损毁与丢失等情况；同时也明确了个人对个人信息进行更正或删除的权利。
- 结合目前层出不穷的电信诈骗、个人信息泄露等事件，《网络安全法》无疑对持有个人信息的组织机构提出了更高的安全防护要求。
- 如何准确识别企业自身所持有的个人信息、如何从技术手段与管理流程对个人信息进行有效防护、如何识别潜在的信息泄露风险点，都已成为企业对个人隐私信息保护的重中之重。

关键点解读 – 网络运营者

“网络运营者”的定义

《网络安全法》第七十六条：网络运营者，是指网络的所有者、管理者和网络服务提供者。

在此定义下，“网络运营者”所适用的范围将大为扩展。通过网络提供服务、开展业务活动的企业及机构，都可能被视为“网络运营者”。

网络运营者除传统的电信运营商、互联网企业外，还可能包括：

- 银行、保险、证券基金等收集公民个人信息，同时又提供线上服务的金融机构；
- 网络安全服务和安全产品的提供者；
- 拥有网站并提供网络服务的企业等。

总体安全 要求	第十条	建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。
	第二十一条	国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改……



毕马威解读：

上述条目从总体层面明确了网络运营者在网络安全方面的要求。其中第二十一条从不同的角度对网络运营者提出了安全要求：

- **安全管理：**网络运营者需在组织内部明确网络安全的责任，并通过完善的规章制度、操作流程为网络安全提供制度保障；
- **技术层面：**网络运营者应采取各种事前预防、事中响应、事后跟进的技术手段，应对网络攻击，降低网络安全的风险。值得注意的是，网络日志的保存期限已明确要求不低于六个月；
- **数据安全方面：**网络运营者需对重要数据进行备份、加密，以此来保障数据的可用性、保密性。

如何根据自身实际情况建立有效的安全管理体系、如何在技术层面选择合理的技术解决方案、如何加强自身的数据保护能力，都将成为网络运营者所重点关注的问题。

关键点解读 – 网络运营者（续）

具体网络安全要求

第二十二条

网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

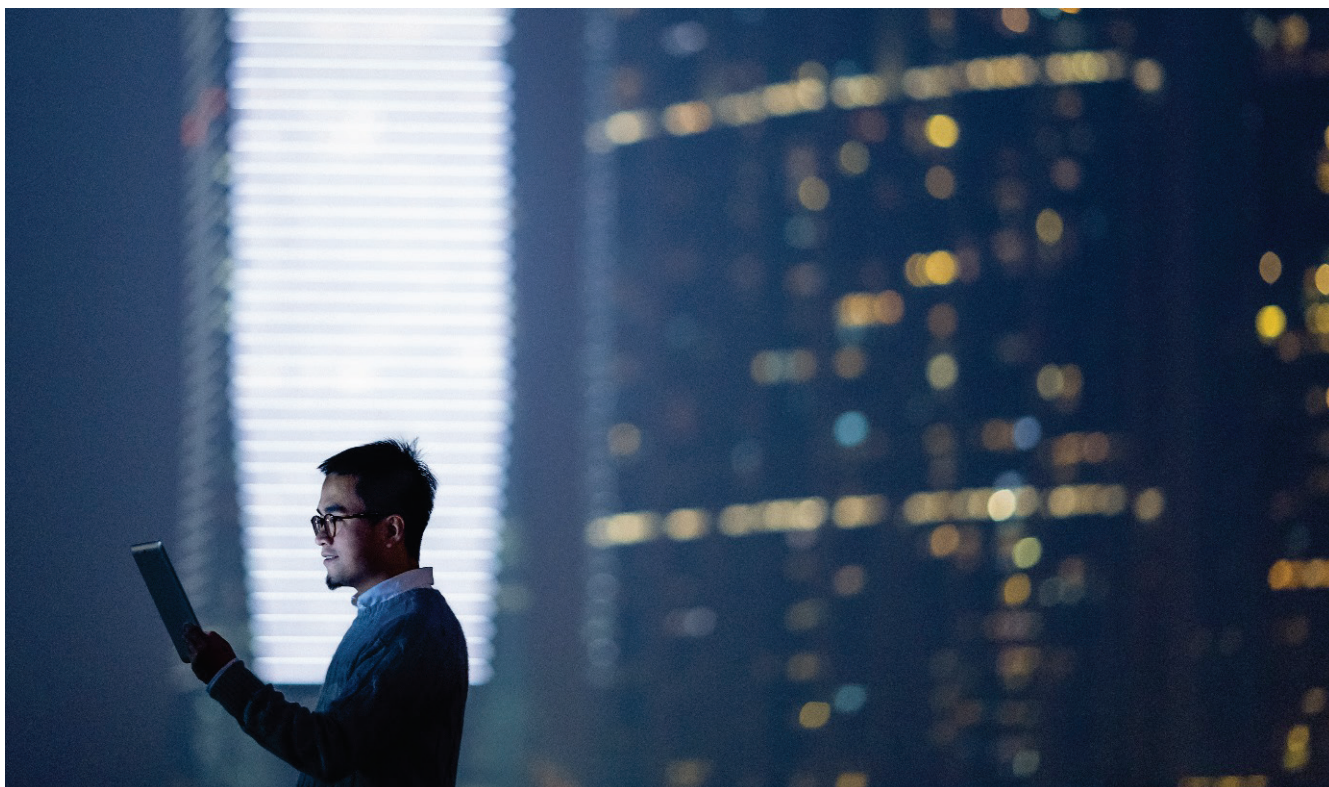
网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。



毕马威解读：

本条目适用于网络安全产品厂商、安全服务提供商及其他通过网络提供相关服务的组织机构。对于此类网络运营者，应及时对产品/服务中所出现的安全缺陷进行响应，并提供必要的安全维护，保障安全产品/服务的正常运行。

目前部分网络安全产品/服务提供方对于自身产品的漏洞缺乏有效、及时的响应，后续维保服务也难以保证，此类情况必然会对产品/服务的使用者带来额外的网络安全风险。本条目无疑对网络安全产品及服务提出了更高的要求。



关键点解读 – 关键信息基础设施

关键信息基础设施的运行安全	第三十一条	国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。
	第三十八条	关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。



毕马威解读：

《网络安全法》提到：关键信息基础设施的具体范围和安全保护办法由国务院制定。但目前尚未正式明确关键信息基础设施的范围。企业可从多角度进行初步评估，例如：用户规模、信息泄露风险、潜在影响、数据中心规模、其他维度等。

若企业符合关键信息基础设施运营的条件，则应根据《网络安全法》第三十八条的要求定期对自身的网络安全风险进行全面评估。



关键点解读 – 敏感信息保存

具体网络安全要求

第三十七条

关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。



毕马威解读：

《网络安全法》中，上述条目对于敏感信息的保护提出了新的要求。

- **潜在影响**：部分企业需要将数据传输至位于境外的总部/合作方/供应商。对于此类企业，一旦符合“关键信息基础设施”运营者的条件，其向境外传输数据的内容、方式方法均需进行重新评估；
- **如何应对**：对于存储于境外的个人信息/重要数据，最直接有效的应对方式是将相关数据转移至境内存储，实际案例可参考Apple、Airbnb等跨国企业对中国用户数据的处理方式；对于原存储于境内，但需要向境外发送的，则需视实际情况对外发送数据的内容与方式进行相应的调整，以满足法律的要求；
- **落地实施**：虽然目前尚未有明确的规章制度来支撑本条目的落地执行，但网信部门及其他监管主体将陆续出台相应的政策，明确详细的境内存储数据要求。



关键点解读 – 安全产品认证

具体网络安全要求

第二十三条

网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第三十五条

关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。



毕马威解读：

上述条目明确要求关键网络安全设备/产品/服务的提供方需通过认证或检测后方能开展销售活动；而上述安全产品的使用方也需根据实际情况通过安全审查。

上述安全审查/评估的目的是从安全的角度出发，为《网络安全法》中所提到的个人信息安全与关键信息基础设施的安全运营提供支持，实现“用户的信息用户自己说了算，用户的系统用户自己说了算”。

对于网络安全设备/产品/服务的提供者，需要积极响应国家安全审查，避免因无法通过国家安全认证、检测而影响安全业务的开展。



关键点解读 – 法律责任

具体网络安全要求

第六十四条

网络运营者、网络产品或者服务的提供者违反本法...，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款...情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

第六十六条

关键信息基础设施的运营者违反本法...，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。



毕马威解读：

上述条目明确规定了对网络运营者、网络产品或者服务的提供者，以及关键信息基础设施运营者的处罚措施，包括暂停业务、停业整顿、吊销相关许可证等，最高处罚金额可达人民币100万元。

网络运营者、网络产品或者服务的提供者，以及关键信息基础设施运营者必须严格遵守网络安全法的相关规定，避免对企业造成损失。



毕马威中国的网络安全服务

毕马威在网络安全咨询服务方面深耕多年，对中国的网络安全现状、监管机构法律法规及规范要求有着深刻理解。

毕马威根据客户的需求提供不同类型的咨询服务。在网络安全方面，毕马威在网络安全管理方面主要提供以下四类服务：





联系

石浩然

合伙人

电话：+852 2143 8799

henry.shek@kpmg.com

赫荣科

总监

电话：+86 (755) 2547 1129

jason.rk.he@kpmg.com

王鑫

副总监

电话：+86 (21) 2212 3651

shane.wang@kpmg.com

邹治國

副总监

电话：+852 2685 7521

matrix.chau@kpmg.com

张令琪

总监

电话：+86 (21) 2212 3637

richard.zhang@kpmg.com

李昊扬

副总监

电话：+852 2978 8233

alvin.li@kpmg.com

肖腾飞

副总监

电话：+86 (10) 8508 5456

frank.xiao@kpmg.com

kpmg.com/cn

所载资料仅供一般参考用，并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的资料，但本所不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

© 2017毕马威企业咨询(中国)有限公司 — 中国外商独资企业，是与瑞士实体 — 毕马威国际合作组织(“毕马威国际”)相关联的独立成员所网络中的成员。版权所有，不得转载。

毕马威的名称和标识均属于毕马威国际的商标或注册商标。