



合规法律评述
2018 年 6 月

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编: 200120
电话: +86 21 3135 8666
传真: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编: 100005
电话: +86 10 8519 2266
传真: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话: +852 2969 5300
传真: +852 2997 3385

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

《网络安全法》体系下企业的责任与义务概览

Summary of Companies' Responsibilities and Obligations Under the CSL

作者: 潘永建 | 李天航

With a view to marking the first anniversary of the implementation of the China's Cybersecurity Law (the "CSL"), and to enabling companies to have a better understanding of their responsibilities and obligations under the CSL, Llinks Cybersecurity and Data Service Team will, starting from June 1st, 2018, publish a series of concise articles titled "30 Questions About the CSL". In this series, we aim to articulate companies' responsibilities and obligations under the CSL by interpreting applicable laws and regulations, as well as precedent cases. As the first episode of the series, this article serves as a framework introduction of companies' responsibilities and obligations under the CSL, while all other articles will offer insights into various key compliance aspects under the CSL.

Companies' responsibilities and obligations regarding cybersecurity and data compliance can be divided into four aspects: network operation security, critical information infrastructure protection, network information protection and compliance, and compliance of data cross-border transfer.

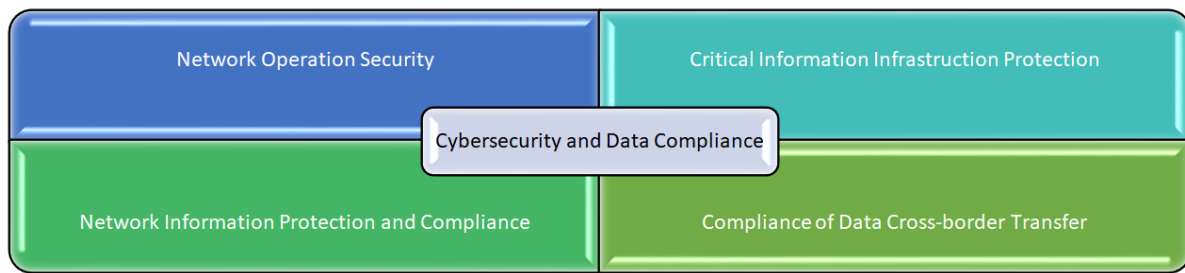
如您需要了解我们的出版物,
请与下列人员联系:

郭建良: (86 21) 3135 8756
Publication@llinkslaw.com

通力律师事务所
www.llinkslaw.com

免责声明: 本出版物仅代表作者个人观点, 不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

《网络安全法》体系下企业的责任与义务概览 Summary of Companies' Responsibilities and Obligations Under the CSL



I. Network Operation Security

This section contains obligations of companies regarding graded network security protection, network products and services procurement, real-name verification requirements, preparing emergency plans, publishing network public security information and network security.

II. Protection of Critical Information Infrastructure¹

Critical Information Infrastructure Operators (“CIIO”) have unique responsibilities and obligations in five aspects of construction, graded network security protection, network products and services procurement, data storage localization and security evaluation.

III. Network Information Protection and Compliance

Companies' responsibilities and liabilities in this area are divided into online information protection and compliance, and personal information protection.

IV. Data Cross-border Transfer²

This section introduces requirements on security assessment, data subject consent, mandatory assessment by competent authorities and circumstances where the data shall not be transferred outside the RPC in the data cross-border transfer.

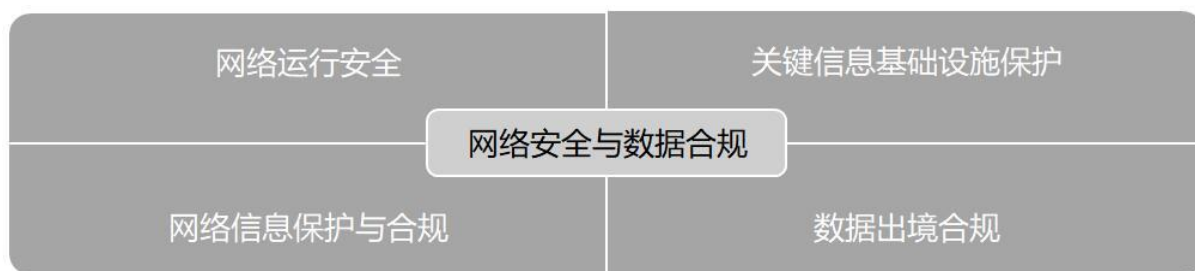
In addition, companies shall pay close attention to obligations imposed in other CSL-related areas, such as network architecture compliance, permits and filings for value-added telecommunication business and obligations of service providers of internet group messaging services.

2018年6月1日是中国《网络安全法》正式生效实施一周年之日。为帮助企业清晰理解网安法下企业的责任与义务，通力律师事务所网络安全与数据服务团队今日起将陆续推出《<网络安全法>实务30问》系列双语指引，通过对法律规定的解读，结合典型实践案例，深度剖析企业的责任与义务，助力企业合规经营，有效防范风险。

《网络安全法》体系下企业的责任与义务概览 Summary of Companies' Responsibilities and Obligations Under the CSL

本篇为《<网络安全法>实务 30 问》的第一篇，将对《网络安全法》框架下企业的责任和义务进行总括式阐述。具体各合规要点将在后续系列指引中分别进行详细分析。

《网络安全法》下企业的网络安全与数据合规责任义务大体分为四大方面：网络运行安全、关键信息基础设施保护、网络信息保护与合规、数据出境合规。



一、网络运行安全

1. 落实网络安全等级保护义务，保障企业网路运行安全。尽管法律没有强制性要求，出于技术能力等因素考虑，企业宜聘请有资质的专业评测机构协助实施。
2. 网络产品、服务以及网络关键设备和网络安全专用产品应当符合国家标准的强制性要求。
3. 落实网络实名制要求。为用户办理网络接入、域名注册服务，固定电话、移动电话等入网手续，或者提供信息发布、即时通讯等服务时，应当要求用户提供真实身份并核实，否则不得为其提供服务。
4. 制定应急预案。根据预案及时处置安全风险并按照规定向有关主管部门报告。
5. 不得擅自发布网络公共安全信息。开展安全认证、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息应当遵守国家规定。
6. 禁止危害网络安全以及帮助他人危害网络安全。

二、关键信息基础设施保护³

对于公共通信和信息服务等 7 个重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据

《网络安全法》体系下企业的责任与义务概览

Summary of Companies' Responsibilities and Obligations Under the CSL

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，国家在网络安全等级保护制度的基础上实行重点保护。关键信息基础设施运营者(下称“关基单位”或“CIIO”)的五个方面的特殊责任与义务为：

1. 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施规划、建设、使用“三同步”。
2. 在网络安全等级保护基础上，在责任主体界定、从业人员教育培训、容灾备份、应急预案等方面履行特别保护义务。
3. 采购网络产品和服务履行国家安全审查义务，并与提供者签订安全保密协议。
4. 重要数据和个人信息境内存储，出境应当安全评估。
5. 建立健全安全评测制度，定期检测评估。

三、网络信息保护与合规

这一领域的义务包括网上信息保护与合规与个人信息保护。

(一) 网上信息保护与合规

1. 管理用户发布信息的义务。发现法律、行政法规禁止发布或者传输的信息，应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。
2. 电子信息发送服务提供者和应用软件下载服务提供者，管理用户发送的电子信息、提供的应用软件的义务。发现设置恶意程序，含有法律、行政法规禁止发布或者传输的信息，应当立即停止传输，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。
3. 建立网络信息安全投诉、举报制度的义务。公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

(二) 个人信息保护

1. 收集、使用个人信息应当遵循合法、正当、必要的原则。公开收集、使用规则，明示收集、使用目的、方式和范围，并经被收集者同意。
2. 处理个人信息应当遵守法律法规和双方约定。不得泄露、篡改、毁损；未经被收集者

《网络安全法》体系下企业的责任与义务概览 Summary of Companies' Responsibilities and Obligations Under the CSL

同意，不得向他人提供，脱敏信息除外。

3. 建立健全用户信息保护制度。采取技术措施和其他必要措施，确保收集的个人信息安全。
4. 将收集的个人信息向境外提供的，应当明确告知个人信息主体并获得同意，并进行安全评估。
5. 应个人信息主体要求删除或者更正个人信息。

四、 数据出境合规⁴

1. 在中华人民共和国境内收集的个人信息和重要数据向境外提供的应当进行安全评估。
2. 对个人信息向境外提供的，应当告知个人信息主体并获得同意。
3. 在数据出境前应当进行自评估，且每年对数据出境情况进行一次评估。
4. 符合条件的应当提请主管部门评估。

类型	条件	要求
数据对应的对象规模	含有或累计含有 50 万人以上的个人信息	符合条件之一即需要申报安全评估
数据对应的容量规模	数据量超过 1000GB	
数据对应的相关领域	核设施、化学生物、国防军工、人口健康等领域数据	
数据对应的环境信息	大型工程活动、海洋环境以及敏感地理信息数据	
关键信息基础设施的安全技术与实体内容	关键信息基础设施的系统漏洞、安全防护等网络安全信息 关键信息基础设施运营者向境外提供个人信息和重要数据	

5. 存在以下情况之一的，数据不得出境：
 - (1) 个人信息出境未经个人信息主体同意，或可能侵害个人利益；
 - (2) 数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；
 - (3) 其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。
 - (4) 不符合国家法律、行政法规、部门规章等有关规定的，不具备合法性不得出境。

另外，企业在经营中还须注意与《网络安全法》相关领域的义务，如：网络构架合规、增值电信业务许可与备案、互联网群组信息服务提供者义务等。

《网络安全法》体系下企业的责任与义务概览
Summary of Companies' Responsibilities and Obligations Under the CSL

《<网络安全法>实务 30 问》系列双语指引问题清单 Schedule of “30 Questions About CSL”	
1	《网络安全法》体系下企业的责任与义务概览 Summary of Companies' Responsibilities and Liabilities under the CSL
2	企业如何落实网络安全等级保护义务 How Should Companies Implement the Graded Network Security Protection System
3	企业正确应对国家机关调取数据的实务分析 How Should Companies Properly Respond to Authorities' Requirement for Data Access?
4	企业使用微信企业号的合规要点 Key Compliance Issues in Using Enterprise WeChat
5	浅析网络运营者的刑事责任 Criminal Liabilities of Network Operators
6	VPN 使用与跨境联网的合规要点 Key Compliance Issues in Use of VPN and Cross-border Connectivity
7	互联网信息服务提供者责任义务辨析 Analysis on The Responsibilities and Obligations of Internet Information Services Providers
8	隐私政策的合规要点与最佳实践 Key Compliance Issues and Best Practices for Privacy Policies
9	企业与第三方关于个人信息保护责任划分 Division of Responsibilities Between Companies and Third Parties Regarding Personal Information Protection
10	员工信息收集、使用合规要点 Key Compliance Issues in Collection and Use of Employee Information
11	数据出境比你想象的常见——数据出境情形分析 Data Cross-border Transfer Happens More Than You Imagine – Analysis of Data Cross-border Transfer Scenarios
12	个人信息安全事件的妥善应对 Proper Response to Personal Information Security Incidents
13	个人信息和重要数据本地化存储的实务分析 Practical Analysis on Local Storage of Personal Information and Important Data
14	网络安全事件应对-兼论网络安全应急预案的必要性 Network Security Emergency Response and Discussion on Necessity of Network Security Emergency Plans
15	网络关键设备、网络安全专用产品、网络产品及服务涉及的网络安全审查制度 Network Security Review on Key Network Equipment, Specialized Network Products and Network Products and Services

《网络安全法》体系下企业的责任与义务概览
Summary of Companies' Responsibilities and Obligations Under the CSL

16	网络安全负责人的设立及职责辨析 Analysis on Network Security Officer and Its Duties and Responsibilities
17	个人信息使用合规分析 Compliance Analysis on Use of Personal Information
18	企业与员工关于个人信息保护的责任划分 Division of Responsibilities Between Companies and Employees Regarding Personal Information Protection
19	企业应当如何落实网络信息实名制要求 How Should Companies Implement Network Information Real-Name Requirements
20	中国法下的个人信息概念与范围辨析 Analysis on Definition and Scope of Personal Information Under PRC Law
21	客户信息收集、使用合规要点 Key Compliance Issues in Collection and Use of Customer Information
22	电商等行业使用个人信息的合规要点 Key Compliance Issues for Use of Personal Information in E-Commerce [etc.]
23	《信息安全技术 个人信息安全规范》作为推荐性国家标准（GB/T）的实践价值分析 Practical Value Analysis on <i>Information Security Technology – Personal Information Security Specification</i> as a Recommended National Standard (GB/T)
24	收购兼并中涉及数据尽职调查要点分析 Key Issues of Data Due Diligence in M&A
25	浅析企业的个人信息保护义务 Brief Analysis on Companies' Obligations of Personal Information Protection
26	关键信息基础设施的界定 Definition of Key Information Infrastructures
27	关键信息基础设施运营者的责任与义务 The Responsibilities and Obligations of Key Information Infrastructure Operators
28	重要数据的界定 Identification of Important Data
29	如何进行数据出境？——数据出境的基本流程 How to Transfer Data Abroad? – The Basic Process of Data Cross-border Transfer.
30	数据出境评估 Assessment for Data Cross-border Transfer

《网络安全法》体系下企业的责任与义务概览 Summary of Companies' Responsibilities and Obligations Under the CSL

如需进一步信息，请联系：

作 者	
潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com	
上 海	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	刘贇春 电话: +86 21 3135 8678 bernie.liu@linkslaw.com
余 铭 电话: +86 21 3135 8770 selena.she@linkslaw.com	娄斐弘 电话: +86 21 3135 8783 nicholas.lou@linkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@linkslaw.com	孔焕志 电话: +86 21 3135 8777 kenneth.kong@linkslaw.com
吴 炜 电话: +86 21 6043 3711 david.wu@linkslaw.com	潘永建 电话: +86 21 3135 8701 david.pan@linkslaw.com
姜 琳 电话: +86 21 6043 3710 elyn.jiang@linkslaw.com	
北 京	
俞卫锋 电话: +86 10 8519 2266 david.yu@linkslaw.com	刘贇春 电话: +86 10 8519 2266 bernie.liu@linkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@linkslaw.com	
香 港(与张慧雯律师事务所有限法律责任合伙联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@linkslaw.com	吕 红 电话: +86 21 3135 8776 sandra.lu@linkslaw.com
伦 敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@linkslaw.com	

© 《<网络安全法>实务 30 问》系列双语指引独家授权威科先行网络安全与数据合规模块在线发布

免责声明：本出版物仅代表作者本人观点，不代表通力律师事务所的法律意见或建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

《网络安全法》体系下企业的责任与义务概览 Summary of Companies' Responsibilities and Obligations Under the CSL

¹ As of the date of this Article, the *Measures on Protection of Critical Information Infrastructure* are still seeking public comments. The comments in this Article on critical information infrastructure operators' responsibilities and liabilities are based on the current published version of the exposure draft.

² As of the date of this Article, the *Assessment Measures on Cross-border Transfer of Personal Information and Important Data* are still seeking public comments. The comments in this Article on the responsibilities and liabilities associated with data cross-border transfer are based on the current published version of the exposure draft.

³ 截至本文写作之日，《关键信息基础设施保护条例》仍在征求意见阶段，本文此处基于公开的征求意见稿对关基单位责任义务作出阐释。

⁴ 截至本文写作之日，《个人信息和重要数据出境安全评估办法》仍在征求意见阶段，本文此处基于公开的征求意见稿对数据出境责任义务作出阐释。