



合规法律评述
2018 年 7 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

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

作者：潘永建 | 李天航 | 邓梓珊

The CSL raises specific requirements on processing (collection, use, storage and sharing, hereinafter collectively referred to as “processing”) of personal information. A compliant privacy policy conveys the company’ good faith in processing personal information lawfully.

I. Key Points for Compliance

Privacy policy shall comply with relevant laws, regulations and ministry rules. Relevant provisions concerning personal information protection are found in a variety of laws and regulations. After the implementation of the CSL, the governmental authorities have taken actions to review the privacy policies of famous enterprises. This article sets out the key points of compliance regarding privacy policy based on applicable legal requirements and necessary formality elements as follows:

.....
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。

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

i. Contents

1. Explicitly state the type, scope and item of personal information collected and explain the purpose and methods of such collection.
2. Where personal information will be transmitted abroad, specify the purpose of such transmission, scope and types of the data transmitted, the country or region where the recipient is located.
3. Where commercial information will be distributed to personal information subjects, it shall be clarified.
4. Explicitly provide the technical measures and other necessary measures to ensure information security.
5. Delete the personal information collected in violation of applicable laws and regulations or relevant mutual agreement; correct the errors in the personal information collected or stored.
6. State remedial actions in case of an information incident where information has been or could be leaked or lost, as well as the means to inform users and report to the relevant authorities.
7. Provisions regarding consent by the information subject. Such provisions shall be drafted considering the channels and means through which users access the privacy policy and they shall ensure a complete review by users of such policy through technical means.

ii. Formality

1. Be concise and user-friendly.
2. Use enhanced notice.
3. User-oriented.

I. Best Practices

Elements of 7 Sections of a Best-practice Privacy Policy and Examples:

General Provisions
Collection of Personal Information
Use, Storage and Transfer of Personal Information
Disclosure of Personal Information

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

Security Measures for Personal Information
Rights of Users over Personal Information
Others

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从6月1日起陆续推出《<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。

本篇为《<网络安全法>实务30问》系列双语指引的第八篇，简析隐私政策的合规要点与最佳实践，以期对相关人士提供参考。

《网络安全法》对于个人信息的收集、使用、保存、对外提供等一系列处理行为(以下简称“处理”)提出了明确要求。《网络安全法》第22条第3款规定,“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41条第1款规定,“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,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。”不仅是《网络安全法》,诸多法律法规规章都对个人信息的处理作出了规定。隐私政策是目前企业对个人信息处理向信息主体进行“明示”的常用方式之一,其合法合规为企业处理收集的个人信息提供了保障。本文将对隐私政策合规要点和最佳实践进行分析,供企业参考。

一、 企业隐私政策的合规要点

隐私政策应当符合法律法规规章等对个人信息处理的要求。目前,中国尚未有一部关于个人信息保护的综合性法律,有关个人信息保护的内容散见于不同的法律、法规、规章中。在《网络安全法》施行之后,2017年7月至9月,中央网信办、工信部、公安部、国家标准委四部门联合开展“个人信息保护提升行动”,其中“隐私条款专项工作”对新浪微博、淘宝、京东商城、支付宝、高德地图、百度地图、滴滴、航旅纵横、携程网等10款网络产品和服务的隐私条款进行评审,并公布了评审结果。本文以相关法律要求为基础,结合“隐私条款专项工作”的评审结果,针对隐私政策的格式要件,对合规要点总结如下:

(一) 企业隐私政策的主要内容

1. 明示收集个人信息的类型、范围和具体项目,说明具体的使用方式和用途。前述内容应当遵循合法、正当、必要的原则,并与实际情况相符。
2. 向境外提供个人信息的,应当在隐私政策中说明数据出境的目的、范围、类型以及接收方所在的国家或地区。
3. 拟向个人信息主体发送商业性信息的,包括但不限于向其固定电话、移动电话或者个人

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

电子邮箱发送商业性电子信息，以及向其住宅、交通工具等发送广告，或者以电子信息方式向发送广告的，应当在隐私政策中说明。

4. 明示为确保信息安全而采取的技术措施和其他必要措施。
5. 根据用户要求删除违反法律、行政法规或者双方约定收集、使用的个人信息，更正收集、存储的有错误的个人信息。
6. 明确在发生或者可能发生信息泄露、丢失的情况时，采取的补救措施，以及企业将按照规定及时告知用户并向有关主管部门报告的做法。
7. 个人信息主体同意的条款。该条款宜结合用户获取隐私政策的途径、方式以及确保完整阅读的技术实现路径实施。

(二) 企业隐私政策的呈现形式

1. 尽量简洁、用户友好，可使用图表帮助说明。“隐私政策专项工作”评审结果提出，鼓励企业制定简洁、易懂的隐私政策，帮助用户迅速找到关键信息。
2. 用户安装、注册、第一次使用前采取增强式告知，提示关于个人信息收集的核心内容。增强式告知不是隐私政策的全部内容，但浓缩了隐私政策的核心，突出用户最关心的信息，例如收集的个人信息范围、使用目的和使用主体等。2017 年“隐私条款专项工作”结束后，京东、支付宝等在其更新后的隐私政策使用了增强式告知，并且展现形式可扩展收缩，点击目录可以跳转到具体条款，易于用户获取和阅读关键信息。
3. 以用户为中心，提供“一站式”撤回和关闭授权，在线访问、更正、删除用户个人信息，在线注销账户等功能。主动区分核心功能和附加功能提供用户选择。

二、 最佳实践

(一) 隐私政策要素

由于法律规定原则性较强，对个人信息保护的具体要求需要企业根据自身情况予以细化落实。在法律强制性要求的基础上，本文结合推荐性国家标准《信息安全技术 个人信息保护规范》(GB/T 35273—2017)，将隐私政策的最佳实践版本总结如下：

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

概述部分	
1.	隐私政策的适用产品或服务范围, 适用的用户类型, 生效及更新的时间。
2.	说明企业保护用户个人信息、尊重用户个人隐私的意愿, 列明企业主动遵循的国内和/或国外的法规政策、安全协议和已取得的相关认证。
3.	信息主体若使用或继续使用相关产品或服务的, 意味着同意隐私政策的内容。
个人信息的收集情况	
1.	明确列举收集的个人信息类型, 如不使用“我们收集您的身份相关信息”, 而明确写明“我们收集您的姓名、电话号码、地址信息”。避免使用概括性语言, 但可以酌情使用“包括但不限于”此类字眼。
2.	详尽地说明收集个人信息的目的, 尽可能包含企业运营发展过程中可能预想到的使用目的, 但必须遵循合法、正当、必要的原则。
3.	使用自动工具(例如 Cookie、脚本等)收集个人信息的, 应说明使用自动工具收集个人信息的目的, 并向用户说明限制自动工具进行数据收集的方法。
4.	提供服务过程中涉及第三方平台的, 需要对第三方是否收集、共享个人信息作出明确说明。
个人信息的使用、存储及传输情况	
1.	对个人信息的使用进行详细说明, 如“用于提供个性化服务”“用于支持和改进向用户提供的服务”等。
2.	明确哪些类型的个人信息将用于提供基本的服务; 哪些将用于提供额外服务(如个性化、升级服务)。
3.	说明个人信息的传输情况, 包括是否与关联方或第三方共享、转让个人信息以及共享、转让的细节。
4.	说明个人信息在使用过程中涉及的地理区域, 如个人信息存储和备份的服务器所在区域, 传输过程中涉及的地域范围。
5.	如果因业务需求、政府和司法监管要求存在跨境信息传输情况, 需详细说明需要进行跨境传输的数据类型, 以及跨境传输遵守的标准、协议和法律机制(合同等)。
6.	根据实际需求, 注明不同类别个人信息预计的保留时间, 需要删除或销毁的截止日期, 确保符合“最少够用”原则。
个人信息的披露情况	
1.	说明是否需要对外披露个人信息, 并详细描述需要披露的个人信息类型、披露个人信息的原因、对接收方的约束和管理准则、个人信息披露过程中的安全措施、披露的个人信息是否对用户带来高危风险等。
2.	说明何种情况下个人信息控制者会不经过用户同意披露数据, 如响应执法机关和政府机构的要求、进行个人信息安全审计、保护用户免受遭受欺诈和严重人身伤害等。
个人信息安全措施	
	详细说明企业对于个人信息进行的安全保护措施, 包括各类加密措施、授权机制、审计机制、信息安全事件的处置等。同时, 可在此提醒用户保护好个人信息安全并提供具体说明, 起到一定的划分责任效果。

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

用户对个人信息享有的权利	
1.	明确用户的访问、更正、删除、获取个人信息，隐私偏好设置的权利，以及取消订阅服务、不再使用服务的撤回同意方式、注销账号的渠道。
2.	处理个人信息主体询问、投诉的渠道和机制，以及外部纠纷解决机构及联络方式等。
其他	
1.	涉及未成年人、老年人、残疾人等特殊人群的注意事项。如涉及收集未成年人个人信息的，应明确获得其监护人的知情同意。
2.	说明隐私政策的修订、更新机制。隐私政策发生重大变化时需及时更新并及时通知用户。

(二) 其他注意事项

1. 如隐私政策与会员/用户注册协议配合使用，企业应将注册协议的阅读与同意作为会员/用户注册的必经程序。基于此，企业的特殊需求可通过注册协议得以明确并起到约束用户的效果。
2. 如隐私政策单独使用的，隐私政策则成为获取个人信息主体同意的唯一渠道。在此情形下，企业宜采取技术措施确保个人信息主体在个人信息被收集前阅读了隐私政策，如通过弹窗等形式展示隐私政策，将隐私政策的阅读与同意作为浏览网页、使用服务的必经环节等。

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

《<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

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

	Products and Services
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（GBT）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 (GBT)
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

企业隐私政策的合规要点与最佳实践

Key Points for Compliance and Best Practices of Privacy Policy(Summary)

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。