LINKS Law Offices 通力律师事务所

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

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

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

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

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

LONDON
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
master@llinkslaw.com

合规法律评述
2018 年 7 月

企业与第三方流转个人信息的典型场景与合规要点

Compliance Analysis on Flows of Personal Data between Companies and Third Parties(Summary)

作者：潘永建 | 李天航 | 洪馨

The flows of personal data between a company and third parties may result in additional responsibilities for the company that collects the personal data. This article will, by analyzing various case scenarios, discuss the legal risks caused by flows of personal data and the proposed compliance solutions.

A. Companies Provide Personal Data to Third Parties

I. General Situations

1. Typical Scenarios
2. Legal Risks

Flows of personal data without or exceeds consent or authorization of data subjects, or security incident occurs.

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

企业与第三方流转个人信息的典型场景与合规要点
Compliance Analysis on Flows of Personal Data between Companies and Third Parties(Summary)

3. Compliance Tips

(1) Obtain the consent or authorization of data subjects.

(2) Desensitization of personal data.

(3) Conduct due diligence on third parties.

(4) Regulate the use of personal data by third parties through a solid cooperation agreement.

II. Special Situations

1. Typical Scenarios
2. Legal Risks

New personal data controllers or new affiliated parties arise.

3. Compliance Tips

(1) In the event of a new personal data controller, the company shall inform data subjects about the situation and give them the choices.

(2) Before the company's control over personal data is officially handed over, the company shall back up all personal data.

(3) The third party shall continue to perform the obligations on the personal data which were previously undertaken by the company.

B. Companies Receive Personal Data from Third Parties

1. Typical Scenarios
2. Legal Risks

Such scenarios may be deemed as illegal collection, transfer, sale, or provision of others' information, and may involve civil liabilities, administrative liability or criminal liability.

3. Compliance Tips

(1) Companies shall conduct due diligence on third parties.

(2) Companies should, through a solid cooperation agreement, reduce the risk of receiving data.

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》系列双语指引的第九篇，通过案例式的场景分析，探讨企业在数据流转下的合规要点。

在数据时代，数据已经成为重要的生产因素而渗透到各行各业，并在各个领域流动。 个人数据未开始流动时，仅由收集数据的企业承担保护责任。数据一旦离开收集企业开始流动，产生多个利益相关方，易使

企业与第三方流转个人信息的典型场景与合规要点
Compliance Analysis on Flows of Personal Data between Companies and Third Parties(Summary)

企业失去对数据的控制并承担额外的法律责任。本文将通过案例式的场景分析，探讨企业在数据流转下的合规要点。

一. 企业向第三方提供个人信息

(一) 一般情形

1. 典型场景

场景一. 企业向第三方提供员工个人信息。比如，企业委托第三方旅行社帮员工个人预定差旅机票和住宿；或者，企业委托第三方人力资源公司协助发放员工的薪酬福利及提供其他员工管理服务等。

场景二. 企业向第三方提供客户/用户个人信息。比如，企业在网络平台上销售产品后，向物流企业提供客户的收货信息；又如，企业是网络平台方，第三方拟与企业建立合作关系，为企业用户提供一些衍生服务，需要大量抓取和使用企业用户的个人数据。

2. 法律风险

(1) 企业未取得数据主体的同意或授权，向第三方转移个人信息；或者，第三方未取得企业或数据主体的同意或授权，抓取和使用企业用户的信息。
(2) 企业向第三方转移的个人信息的范围超出了数据主体同意或授权的范围；或者，第三方对企业提供的个人信息的使用超出了企业和/或数据主体同意的范围。
(3) 企业将个人信息提供给第三方后，第三方发生个人信息泄漏等安全事故。

3. 合规要点

(1) 企业应通过完善的劳动协议/隐私政策或用户协议取得数据主体(包括企业员工、客户、用户等)的同意或授权。该等协议或政策应该明示:
  (i) 相关个人信息收集与使用的规则、目的、方式和范围;
  (ii) 个人信息可能被提供给第三方的目的、涉及的个人信息类型、接受个人信息的第三方类型，以及企业和第三方所承担的相应的法律责任；以及
  (iii) 提供给第三方的数据涉及个人敏感信息(包括身份证号码、电话号码、银行账号等)的，还应告知涉及的个人敏感信息的类型、数据接收方的身份和数据安全能力。

  同时应注意，企业应当采用显著的方式提请用户注意该等协议或政策，且企业不能替用户默认勾选，而应确保用户以主动点击“同意”选项等方式完成授权动作。

(2) 对个人信息进行脱敏处理(去标识化的方法之一)，即处理后使其成为无法识别特定个人且

不能复原的信息，是企业在未经数据主体同意或授权的情况下向第三方提供个人信息的合法途径。 但是，对数据进行脱敏，不可避免地会改变原始数据，可能无法实现商业目的。

(3) 企业应事先对第三方展开尽职调查，确保第三方具备足够的数据安全能力，且提供了足够的安全保护水平。

(4) 企业应通过完善的合作协议规范第三方对个人数据的使用。在该等协议中，企业同意向第三方提供的个人信息不得超出企业已征得个人信息主体同意或授权的范围；同时，企业应要求第三方严格按照企业的要求处理个人信息，通过合同条款规定第三方的责任和义务，包括:

(i) 第三方不得抓取未获得数据主体同意或授权的个人信息，也不得超出数据主体已经授权或同意的范围而使用数据;

(ii) 第三方应协助企业响应个人信息主体基于法律规定而有权提出的请求，比如，访问数据、更正数据、删除数据、注销账户等;

(iii) 第三方在处理个人信息过程中如果无法提供足够的安全保护水平或发生了安全事件，应及时采取相关措施，告知个人信息主体、通报企业并及时向有关主管部门报告；以及

(iv) 第三方在与企业的合作关系解除时，不得再保存企业提供的个人信息。

(5) 企业自身应准确记录和保存向第三方提供个人信息的情况，包括提供的日期、规模、目的，及数据接收方基本情况等。

(二) 特殊情形

1. 典型场景

场景三. 企业经营一家淘宝天猫店，存储并控制着大量的客户个人信息，后来企业决定将这家天猫店的经营权转移给另一家企业，因此需要将其存储的大量客户信息转移给该第三方。其结果是企业作为个人信息控制者转让个人信息的占有及使用权，第三方成为新的个人信息控制者。

场景四. 企业发生收购、兼并、重组等变更:

(1) 如果企业控制权发生了变更，但是企业的名称保持不变，那么个人信息控制者仍是企业自身，个人数据未发生流动;

(2) 如果一家企业被另一家企业吸收合并，或者两家企业合并成为一个新的企业，原有企业消失，则存续公司是新的个人信息控制者。

企业与第三方流转个人信息的典型场景与合规要点
Compliance Analysis on Flows of Personal Data between Companies and Third Parties(Summary)

2. 法律风险

除了与场景一、场景二共同的关于个人信息授权与使用的问题，当出现新的个人信息控制者时，企业应告知个人信息主体，并且给予个人信息主体相应的选择权。

另外，在企业发生收购、兼并、重组等变更时，还需要考虑企业/存续企业是否产生了新的关联方，如果是，需要明确企业/存续企业与关联方之间有关个人信息的共享是否符合企业/存续企业与个人信息主体的约定。

3. 合规要点

我们依据对法律法规的解读以及监管机构的执法尺度，认为企业宜采取以下最佳实践。

(1) 在出现新的个人数据控制者时，企业应向个人信息主体告知有关情况，并给予个人信息主体相应的选择权，让其选择继续使用企业(原个人信息控制者)的服务(如原企业仍留存)，或使用第三方(新个人信息控制者)的服务，或者删除个人信息控制者留存的其个人信息。

(2) 在企业对个人数据的控制权正式移交之前，企业应当对截至交接日的所有个人数据进行备份，由企业与第三方共同确认后对备份载体进行封存。如果后续因个人数据引发争议时，该封存的备份将可以作为争议事项涉及的数据范围的对照标准。

(3) 第三方应继续履行企业原有的对个人信息的责任和义务。如果第三方变更对个人信息的使用范围和/或目的，应该重新取得个人信息主体的明示同意。

二. 企业从第三方接收个人信息

1. 典型场景

场景五. 企业的销售部门为获得潜在客户的信息，聘用市场调查公司，以调查问卷的方式获得个人信息，包括姓名、联系方式、兴趣爱好等。市场调查公司把调查问卷提供给企业，企业根据市场调查公司收集到的个人信息的数量，按每人每条 x 元的价格计价，支付给市场调查公司服务费，且发票的开票名目为“个人信息费”。

场景六. 一家奶粉制造销售企业赞助一家儿童营养协会召开研讨会，面向新生儿妈妈们和孕妇们提供免费培训。协会留存了来访人员的个人信息，包括姓名、联系方式、婴幼儿的姓名和年龄等。奶粉企业的赞助协议明确要求，作为赞助的条件，协会需要将其留存的来访人员个人信息以原样通过电子邮件发送给企业，且对个人信息的收集数量有一定的要求。

企业与第三方流转个人信息的典型场景与合规要点
Compliance Analysis on Flows of Personal Data between Companies and Third Parties(Summary)

2. 法律风险

以上两个场景均可能被认定为非法收集、传输、买卖或提供他人信息的违法行为，并可能涉及以下法律责任:

(1) 民事责任: 《民法总则》已明确个人信息权，任何个人或组织不得侵犯个人信息。企业侵犯个人信息权的，应向相应信息主体承担民事侵权责任。

(2) 行政责任: 《网络安全法》明确禁止的行为包括窃取或者以其他非法方式获取个人信息，非法出售或者非法向他人提供个人信息。企业作为网络运营者从事以上行为，尚不构成犯罪的，可能遭受相应行政处罚。处罚种类包括由公安机关没收违法所得，并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。

(3) 刑事责任: 我国《刑法》禁止两类侵犯公民个人信息的行为，包括:
(i) 违反国家有关规定，向他人出售或者提供公民个人信息；以及
(ii) 窃取或者以其他方法非法获取公民个人信息。

值得注意的是，场景六其实是一种变相买卖个人信息的行为。赞助的目的必须合法合规，不得要求被赞助的非营利性机构协助企业实施违法行为。如果协会向个人信息主体明示相关信息收集与使用的用途，且得到个人信息主体的书面授权或同意，协会可向奶粉企业提供其收集的来访人员信息。 即便如此，作为非营利性组织，协会可否从事变相营利性行为值得警醒。

3. 合规要点

(1) 企业应对第三方开展尽职调查，内容包括但不限于以下方面:
(i) 要求第三方说明个人信息来源，确保个人信息来源的合法性；以及
(ii) 对第三方与个人信息主体的协议进行审查，确认个人信息主体有授权第三方收集、使用并向企业提供其个人信息，并确认个人信息主体授权或同意的范围足够覆盖企业从第三方获取和使用个人信息的范围。

(2) 企业应通过完善的合作协议减少接收数据的风险，要求第三方承诺或保证以下内容:
(i) 其提供的数据是通过合法途径收集的，是真实、合法、有效的;
(ii) 其提供该等数据的行为已经取得个人信息主体充分且完整的授权，足以支撑企业合法收集、使用、存储、处理该等个人信息；以及

企业不因使用、处理、复制、传输和/或以其他方式使用第三方提供给企业的个人信息而被要求承担任何的责任。

企业与第三方流转个人信息的典型场景与合规要点
Compliance Analysis on Flows of Personal Data between Companies and Third Parties(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

企业与第三方流转个人信息的典型场景与合规要点
Compliance Analysis on Flows of Personal Data between Companies and Third Parties(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 Hou 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 *Information Security Technology – Personal Information Security Specification* 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

企业与第三方流转个人信息的典型场景与合规要点
Compliance Analysis on Flows of Personal Data between Companies and Third Parties(Summary)

如需进一步信息，请联系:

作　者	
潘永建 电话:+86 21 3135 8701 david.pan@llinkslaw.com	

上　海	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**刘贇春** 电话: +86 21 3135 8678 bernie.liu@llinkslaw.com
佘　铭 电话: +86 21 3135 8770 selena.she@llinkslaw.com	**娄斐弘** 电话: +86 21 3135 8783 nicholas.lou@llinkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@llinkslaw.com	**孔焕志** 电话: +86 21 3135 8777 kenneth.kong@llinkslaw.com
吴　炜 电话: +86 21 6043 3711 david.wu@llinkslaw.com	**潘永建** 电话: +86 21 3135 8701 david.pan@llinkslaw.com
姜　琳 电话: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
北　京	
俞卫锋 电话: +86 10 8519 2266 david.yu@llinkslaw.com	**刘贇春** 电话: +86 10 8519 2266 bernie.liu@llinkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@llinkslaw.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@llinkslaw.com	**吕　红** 电话: +86 21 3135 8776 sandra.lu@llinkslaw.com
伦　敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	