



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

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

作者: 潘永建 | 朱晓阳 | 邓梓珊

Employers in searching, hiring and managing employees will gather a huge amount of personal data. Simply because an employee is employed by the employer does not mean employees have surrendered rights to their personal data to the employer. This article analyzes the compliance issues in connection with employers' collection and use of employee personal data in the following typical scenarios.

1. Hiring and Interview
2. Background Check
3. Pre-employment Health Check
4. Induction
5. Drug or Alcohol Test
6. Disease Test
7. Internal Investigation
8. Sharing of Employee Personal Data
9. Employee Personal Data Cross-border Transfer
10. Surveillance in Workplace
11. Correction and Deletion of Employee Personal Data

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。

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

Compliance Tips

As a prerequisite for compliance, employees' consent always plays an important role in an employer's collection and use of their personal data. Employers shall in employee handbook or other policies specify its substantive and procedural rules of collection and use of employee personal data, and make employees sign such documentation. As for employee personal data collected, employers must employ sufficient policies and technical measures to ensure the personal data will not be leaked, modified or damaged.

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》系列双语指引的第十篇，对企业使用、收集员工信息的若干典型场景进行分析，并有针对性地提出合规建议。

企业在重视客户信息等“外部”个人信息的合规收集及使用的同时，应同等重视员工¹信息这类“内部”个人信息的合规性。作为雇主，企业在招聘、录用以及日常管理员工的过程中，需要收集、使用大量的员工信息，但企业是否因与员工建立了劳动关系而可对员工的个人信息为所欲为呢？

本文对企业使用、收集员工信息的若干具体场景进行分析，并有针对性地提出合规建议。

典型场景一：招聘与面试

企业内部规章制度通常赋予企业在与员工的劳动关系存续期间依法使用、使用员工个人信息的权利。在招聘与面试阶段，应聘者尚不是企业的员工，并不受到企业内部规章制度的约束。因此，企业必须要对应聘者的个人信息的收集进行明确说明并获得其同意。

在招聘阶段，企业往往会要求应聘者提供其个人简历，应聘者通常也会应要求或是主动提供。同时，在面试、谈话等招聘环节中，企业也会询问应聘者的有关个人信息。在此类情形下，应聘者在简历中或者面试中披露的个人信息应视为其主动同意并提供，企业相应的收集个人信息行为符合正当、合理及必要原则，但是企业应避免利用欺骗、诱导或者强迫的手段收集应聘者个人信息。此外，如果应聘者最终没有被企业录用，企业即无留存相关应聘者个人信息的必要，应当及时予以删除或进行匿名化处理。

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

实践中，企业在招聘阶段获得的应聘者信息可能来自于猎头等第三方机构。在间接获取个人信息的情形下，企业应要求该等第三方机构说明应聘者信息的来源，并对其来源的合法性进行确认。此外，企业应向第三方机构了解应聘者对于其个人信息处理的授权同意范围，包括使用目的以及应聘者是否同意信息转让、共享等。如果企业对应聘者的个人信息处理超出了应聘者的同意范围(如应聘者仅同意将简历提供给某公司，但某公司要将其个人信息提供给她关联公司或其他公司)，企业应重新告知应聘者并取得应聘者的同意。

典型场景二：背景调查

在招聘阶段，企业往往会自行或委托第三方专业机构对应聘者进行背景调查。无论是企业自身进行背景调查还是委托第三方进行背景调查，必须事先取得应聘者的同意(同意最好以书面的形式获得，例如在 offer 中向应聘者征得同意并要求其签名，或者通过书面形式告知并请应聘者签字确认)，且明确告知背景调查收集个人信息的目的、收集的范围、以及个人信息的存储、使用方式等。同时，在委托第三方进行背景调查的情形下，企业必须向应聘者明确告知第三方调查机构的名称等信息，必须确保选择具有健全内部制度以及保障信息安全的充分技术措施的第三方进行背景调查，与第三方明确背景调查涉及的个人信息范围，并且与第三方签订充分的保密协议，确保第三方不会违法收集、使用应聘者个人信息。

如果最终企业没有录用该应聘者，应及时将背景调查中获得的信息删除或进行匿名化处理。

典型场景三：录用前体检报告

在招聘过程中企业可能会要求员工进行某些健康或身体检查并提供相关体检。首先，任何体检都必须在征得应聘者同意的前提下才可进行(无论是由企业进行检查或由企业指定的医疗机构进行检查)。其次，因为健康或身体检查结果通常涉及到个人敏感信息，企业获取相关的检查报告应征得应聘者的同意(建议采取由应聘者自行获取体检报告后向企业提供的形式，而不是企业直接从有关体检机构的数据库中调取)。

若企业以体检结果作为员工雇佣的前提条件，企业应在 offer 或其他书面文件中提前明确告知。同时应明确若应聘者最终未被录用，企业应返还相关报告并将任何副本销毁。

典型场景四：录用及入职

在录用及入职阶段，企业通常会要求应聘者填写个人信息登记表，要求员工书面披露其个人信息。虽然企业在个人信息登记表中列明的信息可以视为明示告知了员工，员工的填写行为也可以视为其对企业收集其个人信息的同意，但企业的收集行为仍应符合个人信息收集最小化的要求。此外，根据劳动合同法，企

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

业有权了解的员工信息应限于“与劳动合同直接相关的基本情况”。据此，企业可以要求员工提供与劳动合同直接相关的信息，例如年龄、性别、学历、工作经验、过往从业经验等，如果是特殊行业，还可以要求员工提供疾病史、无犯罪记录、特殊技能证明等个人信息。但对于与劳动合同并不直接相关的员工个人信息，例如宗教信仰等信息，企业不应主动收集，但员工主动提供相关信息的，则不在此限。

典型场景五：药物或酒精测试

我国法律对于雇主是否能够对员工进行药物或酒精测试并没有明确的规定。相关实践更多的要结合劳动合同法、与员工的劳动合同以企业的相关规章制度来分析。实践中，建议企业事先以书面形式明确企业能够对员工进行药物/酒精测试的条件、情形以及进行测试的程序，向员工进行书面告知并且取得其同意(劳动合同或对相关规章等的签收等)。

在获得员工事先同意，且按照公司相关制度和程序进行药物或酒精测试的前提下，公司必须对测试结果严格保密，未经员工同意不得向任何第三方提供。在企业委托第三方进行相关药物或酒精测试的情形下，如同第2点中所述，企业必须向应聘者明确告知第三方测试机构的名称等信息，必须确保选择具有健全内部制度以及充分技术措施的第三方进行相关测试，并且与第三方签订充分的保密协议，确保第三方不会违法收集、使用应聘者个人信息。

典型场景六：疾病检测

除了常规的药物、酒精测试以外，一些企业可能会对员工进行例如乙肝、艾滋等疾病检测。首先需要明确的是，除非是法律规定某些疾病不得从事的岗位(例如乙肝携带者不得从事某些食品和保育工作)，企业不应员工进行相关疾病测试。对于按照法律规定确有必要进行测试的，由于乙肝、艾滋等疾病的疾病信息属于员工的个人敏感信息，企业应在取得员工明确同意后进行测试，同时对相关疾病测试结果的获取也必须取得员工的明确同意。对于企业获得的疾病测试结果，必须采取技术措施严格保密，且必须在超过有正当理由的存储时限后(例如员工离职或员工的相关疾病与其岗位不再相关)及时删除。

典型场景七：内部调查

在企业因员工涉嫌违规违法而对其进行内部调查的情形下，企业对员工相关信息的收集也应符合法律的规定。企业并非国家有权机关，因此在内部调查中员工对其隐私及个人信息的权利并不因企业对其调查而减损。企业在调查前获取之前未掌握的员工信息(如员工个人电脑中的信息、个人的银行账号、交易信息、行踪轨迹等)应取得员工的明确同意，企业在调查中聘请的第三方机构亦应遵守这一规则。若员工拒不同

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

意提供相关个人信息，企业可以向公安、检察机关报案等，引入国家公权力进行调查。

典型场景八：员工信息的共享

企业在运营过程中有可能会需要将员工信息提供给第三方处理。例如，将工资支付等企业职能外包给第三方的情形下，企业需要将员工的个人信息以及工资信息等提交给第三方服务机构。自此情形下，根据《信息安全技术-个人信息安全规范》(GB/T 35273-2017)的要求，企业在向第三方提供员工信息前应进行安全评估，并采取能够有效保护员工的措施。在向第三方转让前，必须向员工告知共享、转让其信息的目的、信息接收方的身份并征得员工的同意。如果转让的员工信息属于敏感信息，还应当特别向员工告知涉及的敏感信息类型、信息接收方的身份和数据安全能力，并必须征得相关员工的同意。

典型场景九：员工信息的跨境传输

实践中，一些外资公司将员工信息存储于母公司的全球人事管理系统中，而该类系统的服务器通常位于境外。此外，也有外资企业将部分员工信息传输到境外服务商进行数据处理。上述情形均涉及到员工个人信息的跨境传输问题。按照《个人信息和重要数据出境安全评估办法(征求意见稿)》规定，“个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。”因此，企业如涉及员工信息出境的情况，宜在劳动合同、公司制度等文件中予以明确并取得员工的同意。对于共享给第三方的信息，企业必须准确记录和保存员工信息转让和共享的情况(包括共享/转让的日期、规模、目的以数据接收方的基本情况等)。

为帮助企业建立员工信息跨境传输出境的内控流程，我们附上简要的预审批程序表，供企业参考。

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

个人数据传输问卷调查

潜在供应商的名称:	部门:
部门联系方式:	预期完成日期:
简要描述供应商拟提供的服务:	

一般规则:

个人数据不得从欧洲经济区,瑞士或任何国家传输到“第三国”(欧洲经济区之外的国家),除非接收国的法律能确保数据得到充足的保护。如果一个国家不能从法律上确保充分的数据保护标准,则个人数据传输必须根据欧盟委员会批准的合同条款(标准条款)或其他替代措施(如果数据接收国为美国,则按照安全港协议)进行。根据上述事实,除了从合同条款来确保供应商将采取技术性和组织性措施之外,还可能需要单独的数据传输协议来保护我方的个人数据。

一、确定涉及个人数据的类别 <i>提示: 如果涉及的是 2、3 或 4 类个人数据,我们将考虑加入违约通知和赔偿条款,要求供应商在合作结束时自动销毁或归还数据档案,将保障措施延伸到任何分包商,以及审计/监督条款</i>	<u>第 1 类:</u> 姓名, 与业务相关的联系信息(例如工作电话号码, 公司地址和电子邮件地址); <u>第 2 类:</u> 工作和薪水信息, 如薪酬数据等; 奖金和奖励; 关于福利的基本信息; 退休金; 绩效; 遵守EHS政策, 程序, 标准和准则以及相关调查情况; 培训、个人发展记录以及遵守公司政策, 程序, 标准和准则以及相关调查情况; <u>第 3 类:</u> 家庭住址; 家庭和任何个人电话号码和电子邮件地址; 工作和教育背景; 差旅费用; 肖像; <u>第 4 类或个人敏感数据:</u> 根据当地的法律法规,可能被视为敏感数据的个人资料包括政府颁发的身份信息; 种族或族裔、宗教信仰; 身体或心理健康或残疾状况; 性取向; 个人银行或支付卡信息; 工会成员资格; 犯罪历史和任何为已证实的罪行而受到的惩罚。
二、确定供应商传输或访问数据涉及的国家	1. 数据现在是否存储在位于[XX 数据中心]的[实体名称]服务器内吗? 是/否

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

提示：传输形式可以是上传数据,通过电子邮件发送给供应商,或是将数据发送到供应商的服务器或云计算环境,或是允许供应商通过[实体名称]网络框架下的入口访问个人数据。	2. 数据现在是否存储于第三方服务器（例如 XX, XXX, XXXX...）？ 是/否 如是，列明第三方名称： _____ 如否，则目前数据储存位置或地区？ _____ 3. 数据将会被传输至哪个(些)国家？ _____ 4. 若数据将被传输至云计算环境，则该云计算及其备份服务器位于哪个/些国家？ _____ _____
三、确定传输涉及的[实体名称]关联公司	数据在被传输到第三方供应商之前是否是从非[实体总部所在国家/地区]的[实体名称]关联公司转移到[实体的总部]的？ 是/否 或 数据是否会从非[实体总部所在国家/地区]的[实体名称]关联公司直接转移至第三方供应商？ 是/否
四、如果供应商是一家美国公司,确定它是否经安全港认证,并考虑相关合同目的是否与安全港声明中涵盖的目的相符 提示：为了验证安全港状态,以及经安全港认证的公司列表,安全港覆盖的当前状况和范围已在商务	供应商是否是经认证的安全港？ 是/否 若是,则合同目的是否与供应商安全港声明中所涵盖的目的相符？ 是/否

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

部 网 站 https://safeharbor.export.gov/list.aspx 上公布	
五、确定是否有其他公司可以访问我方的个人数据	供应商是否会使用分包商来协助其提供服务,使得该等分包商有可能访问我方个人数据? 是/否
六、确定是否有 IT 安全团队的参与,以便其能够得知供应商 IT 安全标准是否充分	1. 是否有 IT 安全团队成员的参与? 是/否 IT 联系人的姓名: _____ 2. 询问 IT 安全评估调查问卷是否需要提供给供应商。
七、确定供应商是否在寻求第三方直接营销权利	注意: 不得将我们的员工信息提供给第三方用于直接营销目的。

典型场景十: 工作场所监控

在日常运营管理中,出于监督管理的需要,企业可能会对员工的行为进行监控。例如,企业可能通过摄像头获得员工的影像,通过考勤机采集员工指纹,或者通过 APP 的定位功能收集员工的位置信息等,而此类信息往往涉及到员工的敏感信息(行踪轨迹、生物识别信息等)。为合规之目的,企业首先应当保证上述监控措施,以及其所采集的员工信息具有正当目的,且为企业经营所必须(例如,对于非外勤人员,应无采集位置信息的必要),杜绝在非工作时间、非工作场所收集、监控任何员工信息(例如,不应在更衣间、休息室等场所安装监控,也不应在工作结束后继续监控收集相关员工的位置信息)。其次,对于采集的信息的种类、目的、收集方式及保护措施等必须以书面形式事先告知员工,并且取得员工的书面同意。

此外,企业通常对其邮件、电话、其他信息系统等进行监控。考虑到员工经常会在企业系统中存储或传输个人信息,公司宜制定关于系统监控的完善规章制度,并在该等规章制度或其他员工书面确认的文件中明确告知员工公司对公司设备、邮件、系统等采取的监控措施和形式,并明确告知公司能获取系统中的所有信息。

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

典型场景十一：员工信息的修改与删除

企业应通过规章制度等确保员工能够访问企业收集的其个人信息。同时，企业应确保收集的员工信息的准确性，在员工发现其个人信息有错误或不完整，而向企业要求更正的，企业应对信息进行更正或补充。

员工信息的删除与消费者个人信息的删除有所区别。就商业环境下的消费者个人信息而言，如果消费者撤回同意，企业将无权继续处理相应的个人信息。而在员工信息的情况下，如果企业收集的员工信息是其基于劳动关系必须要了解的劳动者信息，原则上员工无权撤回对相关个人信息的同意，也无权要求企业删除。当然，如果企业超过了必要限度收集了员工信息，或者违法或者违反劳动合同、规章制度的规定收集、处理、转让了员工信息，员工仍有权利要求企业删除。

此外，在员工与企业间的劳动关系终止或解除时，企业即丧失收集、存储、处理员工信息的基础，应当及时删除员工信息或进行匿名化处理。当然，在员工离职后仍对企业负有履行保密或竞业禁止义务的情形下，企业仍有权保留上述义务期限内与该等义务履行相关的离职员工的个人信息。

合规建议

综上，我们建议企业结合自身实际情况，在合适的书面文件中(劳动合同、员工手册、公司章程等)明确对于员工信息收集、使用的制度，并让员工签署或签收相应文件。同时，在制定上述规章制度的过程中，也要注意按照劳动合同法等的规定，通过正当程序形成合规政策。

对于已经合法合规收集的员工信息，企业必须采取必要的制度和技术措施，对相关信息保密，并确保员工信息不会被泄露、损毁或篡改。对于公司已收集的员工信息的查阅或处理，企业必须通过明确的规章制度，确定公司哪些人员，在何种情形下，有权查阅或处理哪些员工信息，同时在实践中严格按照相关规章制度，对相关人员授予合适的查阅、处理员工信息的权限。

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(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

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(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

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(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 selenashe@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。

企业收集、使用员工个人信息的典型场景与合规要点

Scenario Analysis on Employers' Collection and Use of Employee Personal Data(Summary)

¹ 因企业招聘环节与后续涉及员工的环节一脉相承，且招聘环节同样涉及大量的个人信息收集，为本文之目的，“员工”也包括招聘阶段的“应聘者”。