Legal Insight | 法律洞察

10 December 2019
201903/003

Inside this issue:

Data Protection Clauses in Labor Relations

With the promulgation of Cyber Security Law, GB/T 35273—2017 *Personal Information Security specification*, as well as other laws, regulations and national standards, the protection of personal data has become a focus of current compliance and employment management for many Chinese companies, which cannot be ignored.

Due to the specificity of labor relations, sometime employers may encounter special circumstances in the collection and processing of personal data of employees, in comparison with "personal data controller"/"data processor" with the ordinary meaning under the *Personal Information Security Specification*.

Taking a virtual enterprise A as an example (regardless of the industry or the size of the company), we will discuss the application of the normative system of personal information and data protection in labor relations, as well as preventive measures to reduce the risk of non-compliance.

As the subject of information, employees would be collected a large amount of personal information during employer's management.[1] According to Article 8 of *Labor Contract Law of the People's Republic of China*, an employer shall have the right to ask about basic information of the employee in direct relation to the labor contract, and the employee shall answer truthfully. Therefore, collection of employee's information directly relevant to labour contract would be consistent with Article 5.4(g), i.e. indispensable to the signing and performance of contract required by personal information subject, under "the exception of consent" in *Personal Information Security specification*, and thus could be obtained without special consent of employees.

The boundary between employers' right of information and the protection employees' personal information lies in whether the personal information collected is directly relevant to the labour contract. There is no authoritative legal definition of this concept, but some simple explanation in local regulations. For example, in Article 8 of *Regulations of Shanghai Municipality on the Labour Contract*, The employer shall, when recruiting an employee, has the right to know his/her health conditions, knowledge, skills, working experience, and other information concerned, and the employee shall make statements according to facts. In Article 11 of *Labour Contract Regulations of Jiangsu Province*, employees shall declare truthfully their employment status, health status, non-competition information which relates directly to their labour contract pursuant to the requirements of their employer, and pro-

vide certification of their resident identity, academic qualification, work experience, professional skills, etc. truthfully. In Article 10 of *Labour Contract Regulations of Jilin Province*, employers could learn about employees' health status, academic qualification, work experience which relates directly to their labour contract, and check over the proof of the previous labour contract termination.

In original meaning of the above-mentioned terms of *Labour Contract Law of the People's Republic of China*, the information directly related to labour contract, i.e. information could be collected without the consent, usually includes health status, academic qualification, work experience and other information which is used to establish the labour relation and sign the labour contract. Among them, the health status of employees deserves special attention. The health status information of the employee without previous consent is limited to the information necessary for the employee's work, such as to check whether the employees in food and beverage industry have invisible infectious diseases. If it is not necessary, the employers have to acquire the consent from employees, otherwise they might be accused of discrimination if they ask for such information.

In principle, for other information other than those mentioned above, employers have to obtain consent from employees. We will discuss it as follows:

1. Hiring

It is normal for large enterprises to collect resumes from job hunters and large recruitment organizations (especially online recruitment platform, referred to as Platform B). As to these personal information, it can be understood that the potential employer A obtains personal information indirectly from B. According to Article 5.3 of *Personal Information Security Regulations*, company A shall require personal information provider B to explain the source of personal information and confirm the legality of such source; Company A shall be aware of the scope of the authorization agreement or privacy statement, including the purpose, whether the subject consent to transfer, share or public disclose of the personal information that B has obtained. If a business activity exceeds the scope of the consent, the explicit consent shall be obtained from information subject within a reasonable period or before processing the personal information.

As can be seen that Company A's obligation here is not to obtain the consent of the resume owner, but to perform the basic due diligence obligations of Platform B, including the source of personal information and the scope of consent. For example, if Company A is a multinational company that needs to transfer information in the resumes to its foreign headquarters, and there is usually no cross-border transmission content in privacy statement or authorization statement, potential employer A has to ask for explicit consent from job seekers for such transfer.

2. Daily Operation

Company A usually impose certain supervisions on employees, such as the instalment of a camera in the office, setup of a fingerprint access system to check attendance, check of the content of the computer and mobile phone which belongs to the company but are distributed to employees , tracking field employees by using the APP with positioning function, etc. In the cases before the enactment of *Cybersecurity* Law, the courts tend to think that collecting such information in the workplace and during working hours is related to the performance of the labor contract. However, many sensitive information. [2] would be collected during this process, such as fingerprint and track. Article 5.5 of *Personal Information Security Regulations* requires that the express consent for the collection of sensitive information subject to voluntary, specific and clear willingness of the fully informed subject. Therefore, the current understanding of the issue is still controversial and should be specifically analyzed according to the specific circumstances of the enterprise. With the enactment and implementation of data protection regulations, the attitude of administrative authorities and judicial practice towards this issue remains to be verified.

When inspecting employees' computers, mobile phones, mails or lockers belonging to company, the provisions of Articles 41 and 42 of the *Cybersecurity Law* and Article 4 of *Personal Information Security specification* shall be strictly observed: for legitimate, justified, necessary and clear purpose to process personal information and meet the minimum collection and transparency requirements. This requires to state clearly in the labor contract or employee handbook that storage devices such as computers/mobile phones are company property and are

not allowed to be used for personal purposes or to store personal information. Personal information should be cleaned up when the company checks or requests property return. When Company A retrieves the computer, mobile phone, mail or locker belonging to it and finds personal information stored by employee, it should first notify the employee to clean it up; if the employee refuses, it can delete it on behalf of this employee, and should not continue to store or process the information. It also cannot use such information for other purposes or leak it to any third parties.

In the daily operation and management, the personal information may also be delegated, shared, or transferred, such as outsourcing wages payment to a third-party Company C.

Under this circumstance, Company A should conduct personal information security assessment before providing employee information to Company C to ensure that C has sufficient ability to secure data.. [3] Company C should guarantee not to store personal information when the entrustment relationship is lifted. Company C shall bear responsibility and obligations and accept audit according to the relevant contracts, while Company A should accurately record and supervise Company C's process of information.

If such outsource is understood to "sharing or transferring", the employee should also be informed of the purpose of such share and the identification of recipient, and the consent of the employee shall be obtained in advance. If the transferred information is sensitive information, the employee should also be informed of the type of sensitive information involved, the identity of the recipient, and the data security capabilities, and the consent of the relevant employee must be obtained.

3. Transfer of personal information during merger, acquisition and restructure

In the process of merger or reorganization of a company, for the purpose of coordinating due diligence, Company A may need to disclose the personal information of its employees according to requirements of the acquirer. Based on *Chinese Cybersecurity Law* and *Personal Information Security Regulations*, what Company A is required to inform employees is the scope and extent of the disclosed personal information, the recipient, the scope of use for such personal information, etc. At the same time, Company A should also supervise whether the use of such information by the recipient is within the scope of the agreed purposes. When Company A actively acquires other companies, it should be noted that whether the purpose of using personal information is changed after acquisition. If yes, Company A should regain the consent from the subject of personal information.

Corporate Liability

Chinese Cybersecurity Law provides punishment for the conduct which violates personal information. Chapter Six clearly regulates that for network operators and the providers of Internet products or services, who seriously infringe upon any right in personal information that is legally protected, their business license would be likely to be revoked. *Personal Information Security specification* reiterates that it should be clear that legal representative or person in charge shall be comprehensively responsible for the personal information security. *Amendment (IX) to the Criminal Law* released in 2015 expands the subject of illegally selling or providing personal information of citizens to any natural person, and at the same time, in the event that personal information of citizens provided to others is obtained during performing duties or providing of services, the sentence shall be heavier within the stipulated range of the preceding Paragraph. When a corporation is the perpetrator, it shall be fined, and the person in charge and other directly responsible personnel in this company might also be punished personally.

In addition, from *(2016) Gan 0102 criminal case No. 605*, it can be seen that a component of the crime of infringement of personal information by the company is the subjective intention. When the court determines whether the conduct of an employee reflects the company's intention, the existence of relevant regulation and measures to prevent such employee crime is a very important consideration. Company A should enact some policies and regulations to strengthen the construction of personal information protection, explicitly prohibits employees from selling, providing, stealing or obtaining others' personal information, and arranges relevant training for employees in order to improve their compliance awareness. After the training, employees should be required to sign written commitments to minimize the

risk of punishment for the company due to employee infringement.

Conclusion

Therefore, in the daily management, employers should pay close attention to the regulations about data protection and the collection of personal information. As a prerequisite for compliance, employee's consent and legal basis for data processing play key roles in the employer's collection and use of their personal data. Employers should have substantial and procedural regulations about the collection and use of employee's personal information in its employee code of conduct or other polices, and asks employees to sign on these documents with democratic process. In any case, Company A must "record" all aspects of processing personal data and keep all relevant records to prove that it has fulfilled the basic principles and the requirements of personal data processing. Apart from the fact that employees enjoyed the rights as the subject of the personal information, they are also responsible for the implement of *Cybersecurity Law* on behalf of the employers. As to the employees who have the authorization to access the personal information collected by employers, the company should pay more attention to prevention and supervision in terms of regulations and technology, such as drafting detailed regulations for employees who take the specific responsibility to protect such information, and supervising the employees to follow them.

With the enactment of *GB/T 35273—20XX Information Security Technology Personal Information Security specification (2019.2, 2019.6, 2019.10)*, *Administration of Data Security (2019.5)* and *Assessment of Export of Personal Information*, partial opinions in this article may have to be updated.

---

[1] GB/T 35273-2017 *Personal Information Security specification* 3.1 Personal Information

Various electronically or otherwise recorded information that can identify a particular natural person or reflect the activity of a particular natural person, either alone or in combination with other information.

Note 1: Personal Information includes name, data of birth, ID number, personal biometric information, address communication records and content, account passwords, property information, credit information, whereabouts and other accommodation information, health information, transaction information, etc.

[2] GB/T 35273-2017 *Personal Information Security Specification* 3.2 Personal Sensitive Information

Once disclosed, illegally provided, or abused, the information would easily harm individual reputation and body health or lead to discrimination treatment.

Note 1: personal sensitive information includes ID Number, individual biological information, bank account, correspondence record and content, financial information, credit information, track, accommodation information, health information, trade information, child information under 14 years old.

[3] GB/T 35273-2017 *Personal Information Security specification* 8.1, 8.2

劳动关系中的数据保护条款

随着《网络安全法》、《GB/T 35273--2017个人信息安全规范》等法律法规、国标指引的出台和生效，个人信息和数据保护已经成为每一家中国境内企业在管理中无法避开的领域和不能忽视的问题，更成为诸多成熟企业当下合规的重点。

因劳动关系的特殊性，用人单位不同于《网络安全法》下一般意义上的“网络运营者”或者《个人信息安全规范》中一般意义上的“个人信息控制者”或者“个人信息处理者”，在收集处理员工个人信息时面临一些特殊情况。

我们以虚拟的企业A为例（不考虑特定的行业或规模大小），探讨个人信息和数据保护的规范体系在劳动关系中的应用，以及减少用人单位合规风险的预防措施。

员工作为信息主体，企业A在管理中会收集大量员工的个人信息[1]。依据我国《劳动合同法》第八条规定，用人单位有权了解劳动者与劳动合同直接相关的基本情况，劳动者应当如实说明。因此，收集员工**与劳动合同直接相关的信息**，可以被认定为《个人信息安全规范》第5.4条“征得授权同意的例外”第g)项**根据个人信息主体要求签订和履行合同所必需的**，从而不需要获得雇员的特别授权同意。

由此可以看出用人单位A的管理知情权与雇员的个人信息保护的界限在于所收集的个人信息是否“与劳动合同直接相关”。对于此概念，法律上没有统一的定义。而各地的地方性规定中则有简单的涉及。例如，上海市《劳动合同条例》第八条：用人单位在招用劳动者时，有权了解劳动者健康状况、知识技能和工作经历等情况，劳动者应当如实说明。江苏省《劳动合同条例》第十一条：劳动者应当按照用人单位的要求，如实说明与劳动合同直接相关的就业现状、健康状况、竞业限制等情况，如实提供自己的居民身份、学历、工作经历、职业技能等证明。吉林省《劳动合同条例》第十条：用人单位可以了解劳动者健康状况、知识技能和工作经历等与劳动合同直接相关的基本情况，查验解除或者终止劳动合同证明。

从上述条款以及《劳动合同法》的本意来看，“与劳动合同直接相关的信息”，即豁免授权同意的信息，通常包含为建立劳动关系以及签订劳动合同所必须的劳动者健康状况、知识技能和工作经历等。其中，劳动者的健康状况值得特别注意。用人单位豁免授权同意的健康状况信息仅限于雇员工作所必须的信息，例如需要了解餐饮行业工作者是否患有隐形的传染病。若非为工作所必须，用人单位无法豁免授权同意，若询问，甚至有就业歧视之嫌。

对于用人单位收集的其他信息，原则上都需要获得劳动者的同意。我们按如下情况分类讨论：

1. 招聘录用阶段：

如今通过猎头和大型招聘机构（尤其是互联网招聘平台，假设平台B）收集简历，已经是成熟企业的常用模式。对于这些个人信息，可以理解为潜在的用人单位A从B处间接获取个人信息。根据《个人信息安全规范》第5.3条，**公司A应要求个人信息提供方B说明个人信息来源，并对其个人信息来源的合法性进行确认；应了解个人信息提供方B已获得的个人信息处理的授权同意范围，包括使用目**

的，个人信息主体是否授权同意转让、共享、公开披露等。如企业A开展业务需进行的个人信息处理活动超出该授权同意范围，应在获取个人信息后的合理期限内或处理个人信息前，征得个人信息主体的明示同意。

由此可见企业A在此处的义务不是征得简历所有人的同意，而是对信息来源方B平台尽到基本的尽职调查义务，包括个人信息来源和授权同意范围的审查等。如A公司是一家跨国公司，需要将简历信息传输到国外总部，而国内招聘平台B的《隐私声明》或授权声明中通常不包含跨境传输内容，因此需要潜在用人单位A向求职者单独就该部分征求其明示同意。

2. 在企业的日常管理中：

企业A通常对员工进行一定的监督检查，如在办公场所设置摄像头，设置指纹门禁考勤制度，检查属于公司财产但配给员工使用的电脑、手机存储内容，对于外勤人员使用定位APP获取行踪路线等。通过检索案例发现，在《网络安全法》颁布之前的司法实践中，法院倾向于认为在工作场所、工作时间收集雇员的此类信息与履行劳动合同相关，是“履行合同所必需的”。但鉴于在这类情况中收集的很多信息，如指纹、行踪轨迹属于个人敏感信息[2]，《个人信息安全规范》第5.5条“收集个人敏感信息时的明示同意”指信息主体应在**“完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示”**。因此目前对该问题的认识尚存争议，应当根据企业具体情况具体分析。随着数据保护法规的出台和贯彻，未来监管部门和司法实践对这一问题的态度还有待考证。

在检查属于公司财产的员工电脑、手机、邮件或储物柜时，应严格遵守《网络安全法》第四十一条和第四十二条的规定，以及《个人信息安全规范》第4条的相关原则：具有合法、正当、必要、明确的个人信息处理目的，满足最少够用、公开透明的原则。其中包括在《劳动合同》或者《员工手册》中写明：*电脑/手机等存储设备属于公司财产，不允许用作私人用途或存储个人信息，在公司检查或要求返还时，应清理个人信息。如若电脑/手机等存储设备收回后仍存有个人信息，则视为放弃相关权利，由用人单位予以删除，用人单位对此不承担任何责任。*

企业A在收回属于公司财产的电脑、手机、邮件或储物柜时，如若发现员工存储的个人信息，应当先通知员工自行清理；若员工拒绝，可以代员工清理删除，不应继续存储、处理，更不能用作其他用途或泄露给第三方。

在企业的日常管理中，还可能会出现信息委托处理、共享或转让的情况，如将工资支付外包给第三方企业C等。

在此情形下，企业A在向C公司提供员工信息前应进行个人信息安全影响评估，确保C公司具备足够的数据安全能力及足够的安全保护水平[3]。促使C公司做出保证，在委托关系解除时不再保存个人信息。通过合同等方式确定C公司的责任和义务，并对其进行审计。A 公司还应准确记录和保存C公司处理员工信息的情况。

如果该等外包授权被理解为“共享或转让”还应向员工告知共享、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，且必须征得相关员工的同意。

3. 在企业收购、兼并、重组时的个人信息转让

在企业被收购兼并或重组过程中，出于配合尽职调查等目的，A公司可能需要根据收购方的要求披露其员工的个人信息。根据《网络安全法》和《个人信息安全规范》，需要A公司向员工告知相

关情况，包括被披露的个人信息范围和程度，接收信息的对象，以及其个人信息的使用范围等。同时A公司还应监督个人信息获取方在约定目的范围内合法合规使用其员工的个人信息。

如果A公司主动收购兼并其他企业，则应注意，如果变更了个人信息使用目的，则A公司应重新获取个人信息主体的同意。

企业责任

《网络安全法》对于侵犯个人信息的行为给出了相关的处罚措施，第六章“法律责任”中明确规定侵害个人信息的网络运营者、网络产品或者服务的提供者，严重者可被“吊销营业执照”。《个人信息安全规范》强调了“应明确其法定代表人或主要负责人对个人信息安全负全面领导责任”。2015年颁布的《 刑法修正案（九）》将出售或者提供个人信息的责任主体范围扩大至任何自然人，同时将“履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人”的情形修订为从重处罚的情节。单位作为犯罪主体时，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各款的规定处罚。

另外，从（2016）甘0102刑初605号案例可以看出，公司侵犯个人信息罪的一个构成要件是公司具有犯罪的主观意图。当法院判断公司员工的犯罪行为是否反映了公司的意愿时，公司是否有制度和措施来防止员工犯罪是非常重要的考量因素。公司应通过发布各种公司政策或规章制度，加强个人信息保护的合规建设，明确禁止员工出售、提供、窃取或以其他方式违法违规获取他人的个人信息，并对员工进行相应的培训，以提高员工的合规意识。在培训结束后，员工应被要求签署相关的书面承诺书，以尽可能减少因员工侵犯个人信息而导致公司被处罚的风险。

结语

因此用人单位在日常管理中，应重视数据保护和个人信息收集的相关规定。作为合规的先决条件，数据处理的合法依据与员工的事先同意在用人单位收集和使用其员工个人数据方面发挥重要作用。用人单位应在员工手册或其他政策中规定其收集和使用员工个人数据的实质性和程序性规则，并使员工经民主决策程序签署此类文件，将数据处理的合法依据充分告知员工，以保证满足处理个人数据透明性原则的要求。在无论何种情况下，公司须对处理个人数据的各个环节做好“记录”并且保存所有相关记录，以证明其履行了个人数据处理的基本原则和要求。除上述员工作为个人信息主体享有保护的权利外，员工作为用人单位落实《网络安全法》相关规定的执行者也负有相应责任。对于有权限获取公司收集的个人信息的员工，公司应当从制度和技术层面进行防范和监督，为承担特定义务的员工制定具体的数据保护合规条款，并监督其遵守。

随着《GB/T 35273--20XX 信息安全技术 个人信息安全规范（征求意见稿）》（2019.02, 2019.06, 2019.10），《数据安全管理办法（征求意见稿）》（2019.5）和《个人信息出境安全评估办法（征求意见稿）》（2019.6）的发布，本文的部分观点可能有待更新。

---

[1] 《GB/T 35273-2017 个人信息安全规范》3.1 个人信息
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特定自然人身份或者反映特定自然人活动情况的各种信息。
注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

[2] 《GB/T 35273-2017 个人信息安全规范》3.2 个人敏感信息
一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。
注1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

[3] 《GB/T 35273-2017 个人信息安全规范》第8.1、8.2条。

Datenschutzklausel in Arbeitsbeziehungen

Mit der Verabschiedung und dem Inkrafttreten des *Cybersicherheitsgesetzes,* der *GB/T 35273--2017-Spezifikation für die Sicherheit personenbezogener Daten,* sowie weiterer Gesetze, Vorschriften und nationalen Normen, wurde der Schutz personenbezogener Daten zu einem Verwaltungsbereich für jedes Unternehmen in China, das weder umgangen, noch ignoriert werden kann und ist somit zum Schwerpunkt der aktuellen Compliance vieler etablierter Unternehmen geworden.
Aufgrund des besonderen Charakters der Arbeitsbeziehungen, unterscheidet sich die Bedeutung von Arbeitgebern sowohl vom allgemeinen Begriff des "Netzbetreibers" gemäß dem *Cybersicherheitsgesetz*, als auch von dem allgemeinen Verständnis eines "Verantwortlichen/Daten Controllers" oder des "Daten Verarbeiters", wie sie in der *Spezifikation für die Sicherheit personenbezogener Daten* definiert werden. Manchmal kann es vorkommen, dass Arbeitgeber bei der Sammlung und Verarbeitung personenbezogener Daten von Arbeitnehmern auf besondere Umstände stoßen.

Nehmen wir als Beispiel ein virtuelles Unternehmen A (unabhängig von der Branche oder der Größe des Unternehmens), um die Anwendung des normativen Systems des persönlichen Informations- und Datenschutzes in den Arbeitsbeziehungen zu untersuchen, sowie vorbeugende Maßnahmen, die das Risiko der Nichteinhaltung von Vorschriften durch den Arbeitgeber verringern können.

Arbeitnehmer sind die Hauptbetroffenen der gesammelten Informationen [1] und die Verwaltung des Unternehmens A sammelt eine große Anzahl dieser persönlichen Daten. Nach dem Artikel 8 des *Arbeitsvertragsgesetzes der VR China* hat ein Arbeitgeber das Recht, die grundlegenden Informationen des Arbeitnehmers in direktem Zusammenhang mit dem Arbeitsvertrag zu erfragen und der Arbeitnehmer hat wahrheitsgemäß darauf zu antworten. Daher kann die Sammlung personenbezogener Daten, die in direktem Zusammenhang mit dem Arbeitsvertrag des Arbeitnehmers erfasst worden sind, als „Ausnahme von der Genehmigung des Betroffenen“ betrachtet werden. Dies geht aus Artikel 5.4 der *Spezifikation für die Sicherheit personenbezogener Daten* hervor: (g) Informationen, die auf den Angaben der Betroffenen beruhen und erforderlich sind, um einen Arbeitsvertrag zu unterzeichnen und auszuführen“. Somit ist keine besondere Genehmigung des Arbeitnehmers erforderlich, um die Informationen zu erheben.

Es zeigt sich, dass die Grenze zwischen dem Verwaltungsrecht des Unternehmens A und dem Schutz persönlicher Daten der Arbeitnehmer darin besteht, dass die gesammelten Daten „in direktem Zusammenhang mit dem Arbeitsvertrag“ stehen müssen. Es gibt diesbezüglich jedoch keine einheitliche Definition im Gesetz. In örtlichen Vorschriften gibt es allerdings viele kleinere Hinweise. Gemäß Artikel 8 der *Arbeitsvertragsbestimmungen von Shanghai* hat das Unternehmen „bei der Einstellung das Recht, den gesundheitlichen Zustand, Kenntnisse, Fähigkeiten, Arbeitserfahrungen und sonstige Informationen über den Arbeitnehmer zu erfahren und der Arbeitnehmer hat diesbezüglich Angaben gemäß den Tatsachen zu machen“. Gemäß Artikel 11 der *Arbeitsvertragsbestimmungen der Provinz Jiangsu* „müssen die Arbeitnehmer wahrheitsgemäß ihren Beschäftigungsstatus, ihren Gesundheitszustand und Informationen zum Wettbewerbsverbot, die sich direkt auf ihren Arbeitsvertrag beziehen, gemäß den Anforderungen ihres Arbeitgebers angeben und ihre Ausweisdokumente, sowie akademische Qualifikation, Berufserfahrung, berufliche Fähigkeiten usw. bereitstellen.“ Gemäß Artikel 10 der *Arbeitsvertragsbestimmungen der Provinz Jilin*, kann der Arbeitgeber nach den grundlegenden Informationen wie Gesundheitszustand, Kenntnissen und Fähigkeiten sowie Arbeitserfahrungen des Arbeitgebers, die in direktem Zusammenhang mit dem Arbeitsvertrag stehen, fragen und auch eine eventuelle Kündigung des Arbeitsvertrags überprüfen.

Nach den oben genannten Bestimmungen und der ursprünglichen Intention des *Arbeitsvertragsgesetzes*, hinsichtlich Informationen, die „in direktem Zusammenhang mit dem Arbeitsvertrag stehen“, sind Informationen, die von der gesonderten Genehmigung des Arbeitnehmers ausgenommen sind, zu verstehen und umfassen in der Regel den Gesundheitszustand, die Kenntnisse und die Berufserfah-

rung des Arbeitnehmers, die für den Aufbau der Arbeitsbeziehungen und Unterzeichnung des Arbeitsvertrags erforderlich sind. Unter diesen Kriterien ist der Gesundheitszustand gesondert zu betrachten. Die Informationen über den Gesundheitszustand sind nur insoweit anzugeben wie sie für die tatsächliche Arbeitstätigkeit relevant sind. Demnach ist es für ein Unternehmen, dass in der Lebensmittelindustrie tätig ist, von großer Bedeutung zu wissen, ob der Arbeitnehmer rezessive Infektionskrankheiten hat. Wenn es für die Arbeitstätigkeit nicht relevant ist, so darf der Arbeitgeber diese Informationen nicht ohne eine Genehmigung anfordern. Sollte es dennoch erfragt werden, könnte dadurch sogar das Risiko einer Diskriminierung gegenüber dem Arbeitnehmer entstehen.

Für andere vom Arbeitgeber erhobene Informationen, ist grundsätzlich die Einwilligung des Arbeitnehmers erforderlich. Wir kategorisieren die Diskussionen wie folgt:

1. Rekrutierungsphase

Das Sammeln von Lebensläufen über Headhunting-Agenturen und große Personalagenturen (insbesondere die Internet-Rekrutierungsplattform, in diesem Fall: Plattform B) ist heute eine gängige Methode für etablierte Unternehmen. Es ist möglich, dass das potenzielle Unternehmen A persönliche Daten indirekt von B bezieht. Gemäß Artikel 5.3 der *Spezifikation für die Sicherheit personenbezogener Daten* muss Unternehmen A den Anbieter B auffordern, die Quelle der personenbezogenen Daten anzugeben und die Rechtmäßigkeit dieser Quelle zu bestätigen; Unternehmen A muss zur Kenntnis nehmen, wie weit der Umfang der Autorisierung von Anbieter B für die Verarbeitung der erhaltenen personenbezogenen Daten einschließlich des Verwendungszwecks beträgt , und ob der Betroffene der persönlichen Informationen B dazu ermächtigt hat, seine persönlichen Informationen und dergleichen zu übertragen, weiterzugeben oder öffentlich zugänglich zu machen. Wenn die für die Geschäftsabwicklung des Unternehmens A erforderlichen Verarbeitungen personenbezogener Daten den Umfang der Genehmigung überschreiten, muss die ausdrückliche Zustimmung des Betroffenen der personenbezogenen Daten innerhalb einer angemessenen Frist nach Erhalt der personenbezogenen Daten oder vor Verarbeitung dieser Daten eingeholt werden.

Das Unternehmen A ist hier also nicht verpflichtet, die Zustimmung des Arbeitnehmers einzuholen, sondern eine grundlegende Due-Diligence-Prüfung gegenüber dem Anbieter B durchzufüllen, einschließlich der Überprüfung der Quelle der persönlichen Daten und des Umfangs der Genehmigung. Wenn Unternehmen A ein multinationales Unternehmen ist und persönliche Daten eines Arbeitnehmers an seinen ausländischen Hauptsitz übergeben will, muss das Unternehmen A die ausdrückliche Zustimmung des Arbeitnehmers für diese Aktion einholen, da die von der inländischen Personalbeschaffungsplattform B bereitgestellten Datenschutz- oder Genehmigungserklärung in der Regel keine Inhalte für grenzüberschreitende Übertragungen enthält.

2. Alltägliche Geschäftsführung des Unternehmens

Unternehmen A führt normalerweise eine bestimmte Überwachung und Inspektion der Arbeitnehmer durch, z. B. das Einrichten von Kameras in einem Büro, das Einrichten eines Fingerabdruck-Zutrittskontrollsystems und das Überprüfen des Speicherinhalts auf Computern und Mobiltelefonen, die zum Eigentum des Unternehmens gehören, aber an Arbeitnehmer verteilt werden. Für den Außendienstarbeitnehmer verwendet Unternehmen A normalerweise eine Ortungs-App, um den genauen Aufenthaltsort des Arbeitsnehmers zu ermitteln. Bei der Untersuchung der Fälle wurde festgestellt, dass die Gerichte in der Rechtspraxis vor der Verkündung des *Cybersicherheitsgesetzes* der Ansicht sind, dass das Sammeln solcher Informationen am Arbeitsplatz und während der Arbeitszeit im Zusammenhang mit der Erfüllung des Arbeitsvertrags steht und "für die Erfüllung des Vertrages erforderlich" ist. Die unter diesen Umständen gesammelten Informationen, wie Fingerabdrücke und Aufenthaltsorte fallen angesichts der Tatsache unter besonders sensible persönliche Daten[2]. Gemäß Artikel 5.5 der *Spezifikation für die Sicherheit personenbezogener Daten* heißt es, dass „bei der Erfassung sensibler personenbezogener Daten eine ausdrückliche Einwilligung erforderlich“ ist, was voraussetzt, dass „der Betroffene seinen freiwilligen, klaren und eindeutigen Willen äußert, der auf einer vollständig informierten Basis geäußert wird“. Daher ist das derzeitige Verständnis dieser Thematik immer noch umstritten und sollte speziell auf die spezifischen Umstände des Unternehmens hin analysiert werden. Angesichts der Einführung und Umsetzung der Datenschutzbestimmungen muss die Haltung der künfti-

gen Verwaltungsleitung und der Rechtspraxis zu diesem Thema noch überprüft werden.

Bei der Überprüfung von Computern, Mobiltelefonen, Postfächern oder Schließfächern von Arbeitnehmern, die Eigentum des Unternehmens sind, sind die einschlägigen Grundsätze der Artikel 41 und 42 des *Cybersicherheitsgesetzes* und des Artikels 4 der *Spezifikation für die Sicherheit personenbezogener Daten* strikt zu beachten: Der Zweck der Verarbeitung personenbezogener Daten muss legitim, geeignet, notwendig und eindeutig sein, sowie den Mindestanforderungen des Grundsatzes entsprechen und transparent sein. Folgende Inhalte sollen im *Arbeitsvertrag* oder im *Arbeitnehmerhandbuch* angeben werden: Speichergeräte wie Computer/Mobiltelefone sind Eigentum des Unternehmens und dürfen nicht für persönliche Zwecke oder zum Speichern persönlicher Informationen verwendet werden. Persönliche Daten müssen entfernt werden, wenn das Unternehmen eine Überprüfung oder eine Rückgabe anfordert. Wenn persönliche Daten auf den Speichermedien wie dem Computer/ Mobiltelefon gespeichert sind, nachdem diese von dem Unternehmen zurückgefordert wurden, wird davon ausgegangen, dass der Arbeitnehmer auf seine entsprechenden Rechte verzichtet und das Unternehmen die Informationen löschen kann, ohne dafür Verantwortung zu tragen.

Wenn Unternehmen A den Computer, das Mobiltelefon, die E-Mail oder das Schließfach zurückerhält und dabei persönliche Informationen findet, die vom Arbeitnehmer gespeichert wurden, sollte es den Arbeitnehmer benachrichtigen, die verbliebenen Informationen zu entfernen. Wenn der Arbeitnehmer dies ablehnt, kann das Unternehmen A im Namen des Arbeitnehmers die Informationen entfernen. Und die relevanten persönlichen Daten dürfen nicht gespeichert, verarbeitet, an einen Dritten weitergegeben oder für andere Zwecke verwendet werden.

In der täglichen Geschäftsführung des Unternehmens kann es auch Umstände geben, in denen Informationen an andere delegiert werden, um sie zu verarbeiten, weiterzugeben oder zu übertragen, wie z. B. das Auslagern von Löhnen an Drittunternehmen C. In einem solchen Fall muss Unternehmen A eine Bewertung der Auswirkungen auf die Sicherheit personenbezogener Daten durchführen, bevor die Informationen der Arbeitnehmer A an Unternehmen C weitergegeben werden, und sicherstellen, dass das Unternehmen C über ausreichende Datensicherheitsfunktionen und ein ausreichendes Sicherheitsniveau verfügt[3]. Unternehmen A soll Unternehmen C auffordern, zu gewährleisten, dass bei Aufhebung der Geschäftsbeziehung zu C keine personenbezogenen Daten gespeichert werden. Die Pflichten und Rechte des Unternehmens C sollten zuvor vertraglich klar geregelt werden, um eine Überprüfung seines Verhaltens zu ermöglichen. Unternehmen A sollte auch den Status der von Unternehmen C verarbeiteten Arbeitnehmerinformationen genau aufzeichnen und aufbewahren.

Wenn solche Auslagerungen als "geteilt oder übertragen" verstanden werden, sollte der Arbeitnehmer auch über den Zweck des Teilens, beziehungsweise der Übertragung seiner persönlichen Informationen, als auch über die Identität des Empfängers dieser Daten informiert werden und zusätzlich seine Genehmigung eingeholt werden. Wenn die Informationen zu den sensiblen Informationen gehört, sollte der Arbeitnehmer auch über die Art der sensiblen Informationen, die Identität und die Datensicherheitsfunktionen des Empfängers verständigt werden.

3. Übertragung persönlicher Informationen während Unternehmensakquisitionen, Fusionen und Umstrukturierungen

Während einer Akquisition, Fusion oder einer Umstrukturierung des Unternehmens zum Zwecke der Koordinierung der Due-Diligence usw. muss Unternehmen A möglicherweise die persönlichen Daten seiner Arbeitnehmer gemäß den Anforderungen des Erwerbers offenlegen. Gemäß dem *Cybersicherheitsgesetz* und der *Spezifikation für die Sicherheit personenbezogener Daten* ist Unternehmen A verpflichtet, den Arbeitnehmer sowohl über den Umfang der offengelegten Daten, die Identität des Empfängers, als auch den tatsächlichen Umfang der Verwendung ihrer personenbezogenen Daten zu informieren. Gleichzeitig beaufsichtigt Unternehmen A auch den Empfänger, der die personenbezogenen Daten erhalten hat, dass dieser die empfangenen Daten im Rahmen der vereinbarten Zwecke rechtmäßig verwendet.

Wenn Unternehmen A andere Unternehmen aufkauft oder zusammenführt, wird darauf hingewiesen, dass Unternehmen A die Zustimmung des Betroffenen in Bezug auf seine persönlichen Daten erneut einholen muss, wenn der Zweck der Verwendung geändert wird.

Unternehmensverantwortung

Das *Cybersicherheitsgesetz* sieht entsprechende Strafen für Verstöße gegen das Schutzrecht personenbezogener Daten vor. Dem Verarbeiter von Daten oder dem Anbieter, der „das gesetzlich geschützte Recht auf personenbezogene Daten verletzt“, kann seine "Geschäftslizenz abberufen" werden, welche im sechsten Kapitel „Rechtliche Verantwortlichkeiten“ eindeutig festgelegt ist. In der *Spezifikation für die Sicherheit personenbezogener Daten* wird betont, dass „die Gesamtverantwortung des gesetzlichen Vertreters oder der hauptverantwortlichen Person für die Sicherheit persönlicher Informationen klar sein muss“. Die im Jahr 2015 verkündete *Änderung des Strafrechts (IX)* enthält zum einen eine Erweiterung des Geltungsbereichs des Verantwortlichen, welcher die personenbezogenen Daten an eine natürliche Person weitergibt, und zum anderen soll gleichzeitig eine härtere Bestrafung erfolgen, wenn „persönliche Informationen von Bürgern verkauft oder zur Verfügung gestellt werden, die sie im Zuge der Erfüllung von Pflichten oder der Erbringung von Dienstleistungen für andere erhalten haben“. Das Unternehmen wird zu einer Geldstrafe verhängt, wenn es sich strafbar gemacht hat und die verantwortliche Person, welche sowohl die direkte als auch die indirekte Verantwortung trägt, wird gemäß den einschlägigen Bestimmungen bestraft.

Aus dem Fall von (2016) Gan 0102 Xing Chu Nr. 605 geht außerdem hervor, dass ein wesentlicher Bestandteil der Straftat eines Unternehmens die subjektive Absicht ist, wenn das Unternehmen die personenbezogenen Daten verletzt. Wenn das Gericht beurteilt, ist es ein sehr wichtiger Faktor, ob das kriminelle Verhalten eines Arbeitnehmers den Wünschen des Unternehmens entspricht, ob das Unternehmen über Systeme und Maßnahmen zur Verhinderung von Straftaten verfügt, die von Arbeitnehmern begangen werden. Unternehmen A soll die Compliance-Konstruktion des Schutzes personenbezogener Daten stärken, indem es verschiedene Unternehmensrichtlinien oder -regeln und Vorschriften erlässt, welche Arbeitnehmern das eindeutige Verkaufen, Anbieten, Stehlen oder anderweitig rechtswidriges Handeln bezüglich des Umgangs mit personenbezogenen Daten untersagt und Arbeitnehmern Trainings zur Verbesserung ihres Compliance-Bewusstseins anbietet. Am Ende des Trainings müssen die Arbeitnehmer entsprechende schriftliche Verpflichtungen unterzeichnen, um das Risiko von Strafen für das Unternehmen aufgrund von Verstößen der Arbeitnehmer gegen personenbezogene Daten zu minimieren.

Schlussfolgerung

Daher sollten Unternehmen bei der täglichen Verwaltung die einschlägigen Bestimmungen zum Datenschutz und für die Erhebung personenbezogener Daten beachten. Als Voraussetzung für die Einhaltung spielen die Rechtsgrundlage für die Datenverarbeitung und die vorherige Einwilligung des Arbeitnehmers eine wichtige Rolle bei der Erhebung und Nutzung personenbezogener Daten. Der Arbeitgeber sollte in Arbeitnehmerhandbüchern oder anderen Unternehmensrichtlinien, inhaltliche und verfahrenstechnische Regeln für die Erhebung und Verwendung personenbezogener Daten von Arbeitnehmern festlegen und den Arbeitnehmer veranlassen, solche Dokumente zu unterzeichnen. Außerdem sollte der Arbeitgeber die Arbeitnehmer in vollem Umfang über die Rechtsgrundlage für die Datenverarbeitung informieren, um der Anforderung nach der Transparenz in Verarbeitung der personenbezogenen Daten gewachsen zu sein. Der Arbeitgeber sollte unter allen Umständen jedes Glied des Datenverarbeitungsprozesses protokollieren und alle relevanten Protokolle bewahren, damit wird bewiesen, dass er die Grundprinzipien der Verarbeitung der personenbezogenen Daten einhält und der Anforderung nach der Rechenschaftslegung nachkommt. Der Arbeitgeber ist neben dem Arbeitnehmer als Hauptbetroffener von Datenschutzrechten, auch für die Umsetzung der einschlägigen Bestimmungen des *Cybersicherheitsgesetzes* verantwortlich. Für Arbeitnehmer, die Zugang zu personenbezogenen Daten haben, die vom Unternehmen gesammelt wurden, muss das Unternehmen die Einhaltung von Bestimmungen zum Datenschutz durch diese Arbeitnehmer auf institutioneller und technischer Ebene verhindern, sowie deren Einhaltung überwachen.

Mit der Veröffentlichung der *GB/T 35273--20XX Informationssicherheitstechnologie -Spezifikation für die Sicherheit personenbezogener Daten* (Entwurf für einen Kommentar) (Februar, Juni, Oktober 2019), *Verwaltungsmaßnahmen zur Datensicherheit* (Entwurf für einen Kommentar) (Mai 2019) und *Maßnahmen zur Sicherheitsbewertung für Grenzüberschreitende Übermittlung personenbezogener Daten* (Entwurf für einen Kommentar) (Juni 2019), müssen einige Inhalte in diesem Artikel möglicherweise aktualisiert werden.

Your Contacts

ZHANG Yuhua
LL.M. (Nanjing / Göttingen)

Attorney-at-law (China)
Associate

Cyber Security & Data protection
E-Commerce

+86 21 5010 7526
zhangyuhua@cn.luther-lawfirm.com

Languages: German, English, Chinese

QIN Anqi
LL.M. (Nanjing University)

Attorney-at-law (China)
Senior Associate

Employment Law
Litigation & Arbitration

+86 21 5010 6018
qinanqi@cn.luther-lawfirm.com

Languages: English, Chinese