Llinks Client Alert — June 2025(Supplement)
Is Purchased Data Risk-Free?

Recently, several of our clients have undergone government enforcement or investigations, which all pointed to one thing: procuring data or data services from external sources. Contracting vendors to collect data, or data purchasing, is often intended to alleviate the data compliance obligations on data controllers. However, many overlook the significant risks involved in data procurement. In this client alert, we summarize key compliance points for purchased data.

I. Do you understand the data your company is procuring?

The sensitivity of data and the legal liabilities arising from data breaches are closely tied to the nature of the data. Based on our experience, we've identified the following common oversights by companies, which can lead to an unfavorable position during inspections:

1. **Misjudgment regarding personal information.** Companies often believe that information like VIN (Vehicle Identification Numbers), hospital bed numbers, or serial numbers of corporate devices does not constitute personal information. This assertion may not be accepted by enforcement departments, leading them to conclude that the company has not fulfilled its corresponding compliance obligations for personal information.
2. **Insufficient understanding of anonymization.** Many companies hope to avoid personal information risks by using "anonymized data". However, the "anonymized data" they purchase may, at best, only be "de-identified data". Legally speaking, de-identified personal information still qualifies as personal information. A misjudgment of the degree of anonymization can significantly amplify a company's personal information risk exposure.
3. **Knowledge about the source of personal information.** In practice, it's not uncommon for companies to commission vendors to collect personal information, as an attempt to absolve themselves of responsibility. However, when dealing with illegal personal information cases, this attempt to sever responsibility is ineffective, as enforcement agencies will presume the company has or should have knowledge about the legality of data, especially concerning criminal offenses involving the infringement of citizens' personal information.
4. **Infringement of trade secrets can also lead to a "presumption of knowledge".** One of our clients was recently investigated by the government because the data provided by their vendor was suspected of infringing a third party's trade secrets. Similar to personal information, proving trade secret infringement also requires the company to have "known" or "should have known".

II. In specific circumstances, companies may be held responsible for vendor actions

Many companies believe that once they engage an external vendor, as long as the company itself doesn't directly process the data, they are off the hook, even if the data is highly sensitive or unlawfully sourced. They also often include contractual clauses to explicitly disclaim such responsibilities. However, this approach may not always be effective.

1. **Companies may be responsible for the actions of their processors (vendors).** If the entrusted processor acts unlawfully while processing data, the data processor/controller may face civil, administrative, and even criminal liabilities. In such cases, even if data processing is entirely carried out by the vendor and data is stored solely within the vendor's IT environment, the legal consequences of unlawful data processing may still be borne by the commissioning party (the data purchaser).

2. **Data procurement may constitute "joint control".** For example, if Company A and Company B jointly decide to develop an APP for marketing activities and collectively determine the purpose and methods of collecting personal information, they will be considered joint controllers of personal information. This holds even if Company A ultimately performs all personal information collection and processing, and Company B only receives the results of Company A's data analysis. When joint control occurs, each joint data controller will be directly liable for any illegal acts committed by either party.

III. Common issues in specific industries

1. **Pharmaceutical industry:** Given the unique nature of sensitive personal information in the pharmaceutical sector, like physiological and health data, companies procuring data without sufficient scrutiny face a higher likelihood of being presumed "should have known" and thus higher personal information legal risks. Furthermore, hospital-related data (e.g., hospital department information, procurement data, prescription statistics) procured by many pharmaceutical companies may be classified as "state secrets".

2. **Retail:** Companies in the retail industry are more inclined to procure marketing and user analysis data. It's crucial to pay attention to whether the procured data is generated based on individual profiling or group profiling. Additionally, specific subsectors of retail may have even more particular personal information compliance issues. For instance, the luxury goods industry might possess personal information of high-net-worth individuals or those involved in political/military affairs, which could face stricter scrutiny and higher risks.

3. **Semiconductor and other advanced manufacturing industries:** Besides potentially involving important data/core data related to these industries, legal risks in the areas of export controls and trade sanctions shall not be overlooked. Moreover, because export controls focus on end-users and uses, companies not only need to be aware of data source risks from upstream but also need to strengthen risk management for data provided from the company to external parties.

IV. Risk isolation solutions and services

1. **Thoroughly understand your business and data processing.** As a legal team with many years of experience in corporate data compliance assessments, we can assist companies in systematically identifying data processing scenarios involved in their business operations, assessing data sensitivity, and recognizing compliance risks related to data-intensive business activities. Data inventory is not only the starting point for companies to evaluate risks associated with externally procured data but also the foundation for fulfilling virtually all other data compliance obligations.

2. **Adjustments to business and data processing models and procedures for identified compliance risks.** For example, we can advise on whether relevant data processing activities need to be outsourced to a third party, and how to design data collection and processing requirements for third parties to prevent the company from incurring legal liability due to the third party's actions.

3. **Review and refine contract clauses to clarify the legal relationship between the company and relevant parties.** Firstly, efforts should be made to avoid relationships that could be deemed as "principal-agent" or "joint control". If such arrangements are necessary, we recommend that companies clearly define the rights and obligations of all parties in agreements with vendors/partners. Specifically, vendors should be required to commit and guarantee the compliance of data sources and data processing, and to fulfill data protection obligations mandated by law and the company.

4. **Conduct due diligence on data and vendors.** For data with particularly high legal risks (e.g., sensitive personal information or trade secrets), simply relying on contractual agreements is insufficient for a company to "prove its innocence". We can assist with pre-acquisition due diligence for data procurement scenarios where companies are uncertain. This includes conducting due diligence on the vendor's business qualifications, business model, and historical compliance, as well as investigating the data's content, source, acquisition method, processing purpose, and third-party rights.

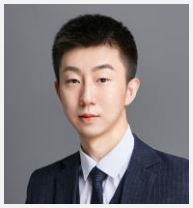
5. **Improve internal data compliance control systems.** Data compliance risks are often very abstract, and companies may expend 100% effort yet still be unable to fully avoid the risks associated with externally procured data. A robust internal control system can be a company's last "lifeline". For example, in the realm of personal information, the *Personal Information Protection Law* stipulates that in the face of infringement claims by personal information subjects, a company needs to prove it was not at fault to be exempt from liability. System documents such as data classification and grading systems, data access management systems, personal information protection impact assessments, records of personal information protection activities, and personal information protection compliance audits are the best evidence for a company to demonstrate its lack of fault.

6. Provide **specialized training** for employees on data compliance and personal information protection, and conduct **specific training and drills** for certain employees on how to respond to government investigations.

7. For executives with a need to avoid personal risk (e.g., general managers, company/department heads), we can review their scope of responsibilities and approval authorities and propose solutions to mitigate legal risks arising from the exercise of their duties and approval powers (e.g., approving and signing high-risk contracts and business dealings).

If you are in need of any of our legal services, please feel free to contact us:

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com



Nigel Zhu
+86 21 3135 8683
nigel.zhu@llinkslaw.com

Susan Deng
+86 21 6043 3793
susan.deng@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	18F, China Resources Tower 2666 Keyuan South Road, Nanshan District Shenzhen 518063 P.R.China T: +86 755 3391 7666 F: +86 755 3391 7668

HONG KONG	LONDON
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE United Kingdom T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD