通力合规评论 —— 2025 年 6 月(增)
买来的数据，就没风险了？

近日，我们多家客户被政府执法部门要求接受调查或配合调查，调查的内容都指向了：企业从外部采购数据/数据服务。委托供应商采集数据，或直接采购数据，本是为了给企业减负，但此类采购活动实则暗藏风险。本期合规评论，我们为大家梳理相关注意要点。

一. 你是否清楚公司到底采购了何种数据？

数据的敏感程度，以及违反相关数据保护义务所需承担的法律责任，与数据的性质密切相关。结合我们的经验，我们发现企业通常会有以下疏漏，可能导致应对检查中的不利地位：

1. **对个人信息发生误判。**企业通常认为 VIN 码(车架号)、医院的床位号、公司电脑的序列号等信息不属于个人信息，该主张可能不被执法部门所接受，导致执法部门认为企业未经到个人信息相应的合规义务。
2. **对匿名化不够了解。**很多企业希望通过“匿名化数据”来避免个人信息风险，但可能购买的“匿名化数据”充其量只能算 A 是“去标识化数据”，而去标识化后的个人信息在法律意义上仍然属于个人信息。对匿名化程度的误判会放大个人信息的风险敞口。
3. **“明知”个人信息来源违法。**实践中，不乏有企业为了切割责任，委托供应商从非法渠道采集个人信息的情况是。但在处理个人信息违法案件时，这种责任切割是无法奏效的，因为执法部门会推定企业是否“明知”,尤其是涉及侵犯公民个人信息的刑事犯罪，企业可能被认定存在间接故意而入罪。
4. **侵犯商业秘密，也会“推定明知或应知”。**笔者最近有一个客户受到政府调查，是因为供应商提供的数据涉嫌侵犯第三方的商业秘密。与个人信息类似，认定商业秘密侵权也要求企业“明知或应知”。

二. 特定情况下，公司需要为供应商的行为担责

许多企业认为委托了外部供应商后，只要企业自身不接触数据，哪怕相关数据本身涉及高敏感性数据，甚至来源违法，公司也不会因此承担责任，甚至设置合同条款明确责任分割。但这么做未必有效。

1. **业需要为受托者(供应商)的行为担责。**如果受托处理者在处理数据的过程中存在违法的行为，民事、行政、刑事的法律后果都有可能由数据处理者/控制者来承担。所以，在此情形下，即使数据处理完全由供应商进行，数据也完全存储于供应商的 IT 环境，违法处理数据的法律后果仍然有可能由委托方(数据买受方)来承担。

2. **数据采购可能构成“共同处理/控制”。**举例而言，A 公司和 B 公司共同决定开发一款 APP 来进行市场营销活动，并且一致决定了收集个人信息的目的和方式。那么即使最终个人信息的收集、处理活动仅由 A 公司进行，B 公司只接收 A 公司进行数据分析后的结果，A、B 公司仍然会被认为是个人信息的共同处理者。在构成共同处理者的前提下，每一共同处理者都是直接的行为人，从而需要为任何一方的数据违法行为承担直接的法律责任。

三. 特定行业的常见问题

1. **医药领域**：考虑到生理健康信息等敏感个人信息的特殊性，对于采购数据疏于审查而被推定“应知”而承担个人信息违法风险的可能性更高；此外，许多医药企业采购的涉及医院的数据(例如医院的科室信息、采购数据、统方数据)可能会被认定为“国家秘密”。

2. **消费品**：消费品行业通常需要采购市场营销和用户分析数据，需关注所采购的数据是基于个人画像还是群体画像产生的。此外，特定消费品行业会有更为特殊的个人信息合规问题。例如，奢侈品行业可能会掌握高净值人士、涉政/涉军人士的个人信息，该等个人信息可能面临更严格的审查，风险较高。

3. **半导体等先进制造业**：除了可能涉及相关行业的重要数据/核心数据外，出口管制及贸易制裁领域的法律风险也不容忽视，而且由于出口管制关注终端用户和用途，企业不仅需要关注上游的数据来源风险，还需要加强对于数据从企业向外部提供的风险管控。

四. 风险隔离方案及服务

1. **充分了解业务及数据相关情况**。作为有多年企业数据合规体检经验的律师团队，我们能够协助企业系统化梳理业务过程中涉及的数据处理场景，识别数据的敏感程度，以及涉数据业务的合规风险。“摸清家底”不仅是企业评估外部采购数据相关风险的起点，也几乎是企业履行其他一切数据合规义务的基础。

2. **针对识别出的合规风险，提出业务及数据处理模式和流程的调整方案**。例如，是否需要将相关数据处理活动外包给第三方；如何设计针对第三方提出的数据收集、处理要求，避免公司因为第三方的行为承担法律责任。

3. **审阅完善合同条款，明确企业与相关方之间的法律关系。**首先，应尽量避免会被认定为“委托代理”或“共同处理”的法律关系；如果必须要有此安排，那么建议企业在与供应商/合作伙伴的协议中明确约定各方之间的权利义务，尤其应要求供应商对数据来源和数据处理的合规性做出承诺和保证，以及履行法律和企业要求的数据保护义务。

4. **对所接收数据及供应商进行审查。**对于特定法律风险比较高的数据(例如敏感个人信息，或者商业秘密等数据)，企业仅通过协议约定的方式还不足以“自证清白”。我们可以针对企业把握不准

的数据采购场景，协助进行事前审查，包括对供应商的业务资质、业务模式及历史合规情况进行尽调，以及对数据的内容、来源、获取方式、处理目的、第三方权利等进行摸排。

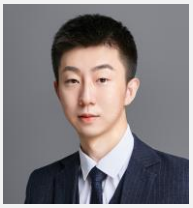
5. **完善数据合规内控制度。**数据合规的风险往往十分抽象，企业可能用尽100%的努力也无法完全避免外部采购数据所带来的风险。而完善的内控制度可以成为企业最后的“救命稻草”。例如，在个人信息领域，《个人信息保护法》规定面对个人信息主体的侵权主张，企业需要证明自身没有过错才能免责，而诸如数据分类分级制度、数据权限管理制度、个人信息保护影响评估、个人信息保护活动记录、个人信息保护合规审计等制度文件则是企业证明自身没有过错的最好证明。

6. 对员工进行数据合规、个人信息保护方面的**专项培训**，对特定员工进行应对政府调查的**专项培训和演练。**

7. 针对有降低个人风险需求的高管(如总经理、企业/部门负责人)，梳理其职责范围及审批权限，提出降低其因履行职责和审批权限而带来的法律风险(如对具有风险的合同和业务进行审批和签字)的方案。

如有需要，请随时与我们取得联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@llinkslaw.com

邓梓珊
+86 21 6043 3793
susan.deng@llinkslaw.com

往期文章：

AI 也有“署名权”了？简评《人工智能生成合成内容标识办法》
美国对华限制政策新发展——人工智能篇/生物医药篇
简评《生成式人工智能服务管理办法(征求意见稿)》七大问题
隐私计算技术对数据开发利用的突破与限制
AI 不是你想买，想买就能买——从出境合规视角看中美人工智能技术监管
算法推荐 深度合成 生成式 AI？傻傻分不清楚
利好 AIGC 行业？——AIGC 著作权第一案评析

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: **master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	**伦敦**	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野