买来的数据，就没风险了?

作者：潘永建 | 朱晓阳 | 邓梓珊

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。这些调查有些涉及行政程序，有些涉及刑事程序，涉及的客户业务不同，行业不同，规模不同，但调查的内容都指向了：企业从外部采购的数据。随着数据领域立法的完善，企业的数据合规意识越来越高，风险意识也越来越强，很多企业开始选择自己不直接收集、处理数据，而是向第三方数据供应商或者合作伙伴购买数据。那么，这么做是不是真的能够降低风险?实现风险隔离又需要注意哪些合规问题?本期合规评论，我们来为大家解读。

一. 数据的性质

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。例如，买卖个人的姓名和地址会构成行政违法甚至是侵犯公民个人信息犯罪，但买卖企业的名称和地址则通常不会构成违法行为，甚至可以成为合法的商业模式。因此，要避免外采数据的合规风险，首先需要对数据的性质进行甄别。

1. 个人信息

毋庸置疑，个人信息在全球几乎所有国家，都是受法律监管最严格、敏感程度最高的数据类型之一。而从法律责任及执法强度来看，中国的个人信息监管严格程度丝毫不弱于欧盟等主要境外法域。

对于采购数据的企业而言，最需要注意的是以下两个问题:

如您需要了解我们的出版物，
请联系:

Publication@llinkslaw.com

1) 数据是不是(含不含)个人信息?

在很多场景下，判断数据是不是构成或者包含个人信息并不像大部分企业想象得那么容易。在我们过往协助客户应对的政府调查中，执法部门对企业提出的 VIN 码(车架号)、医院的床位号、公司电脑的序列号等(常识不认为是个人信息的)信息不属于个人信息的主张提出了质疑。如果企业不能精确地对数据的个人信息属性进行识别，那就谈不上遵守个人信息的合规义务，被处罚了可能还是一头雾水。

此外，很多企业希望通过“匿名化数据”来避免个人信息风险，但殊不知其购买的“匿名化数据”充其量只能算是“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。很多企业没有充分评估所接受数据的匿名化程度，而将去标识化的个人信息作为非个人信息对待，反而放大了个人信息的风险敞口。

2) 个人信息的来源是否合规?

相较于有形的财产，数据的一大属性是其合规风险更容易随着数据的流转而被“继承”。虽然对于违法数据流转的责任继承通常也需要买受企业“明知违法”这一要件，但在数据的情形，“明知”常常会被推定。例如，在“侵犯公民个人信息罪”中，如果购买的个人信息敏感程度高(涉及行踪轨迹、通信内容、征信信息、财产信息等)，或者购买数量大(达到或超过 5000 条)，通常会推定企业应当明知数据的来源违法而没有尽到审慎义务，从而认定企业至少存在间接故意而入罪。

2. 非个人信息

即使企业能够确定采购的数据完全不涉及个人信息，是不是就没有任何风险了呢?非也。

即使我们先排除国家秘密、国家情报等对于大部分企业比较“遥远”(但也不是完全不可能接触到)的数据类型，其他非个人信息类的数据仍然存在让企业“踩坑”的可能。

举例而言，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，认定商业秘密侵权通常也要求企业“明知或应知”，但大量的情形下，企业会被推定“应当知道”。例如，如果企业接收的数据涉及同行业竞争对手的核心同类经营信息，那么司法实践中通常会推定企业“必然知晓”此类信息为商业秘密，从而认定接受数据的企业构成侵犯商业秘密。

除此之外，来源于特定“上游”的数据可能还会有额外的合规风险。例如某些供应商可能会采取第三方系统的方式获取数据，从而构成“非法侵入计算机信息系统罪” 或“非法获取计算机信息系统数据罪”，而如果企业明知或应知数据是该等供应商通过上述犯罪行为获取的数据而仍然接收，可能会构成收受赃物罪。

因此，企业有必要在接收数据前，对相关数据的内容和性质进行识别，确认其是否构成或包含特定类型的敏感数据(个人信息、商业秘密、重要数据/核心数据、国家秘密/国家情报)，从而履行相应的合规义务和风险缓释措施(具体见下文第三部分)。

二. 公司与供应商的法律关系

许多企业知道敏感数据不要拿，但是认为，如果企业选择由外部供应商来收集、处理数据，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。很多公司还会在与供应商的合同中写明“双方之间不构成任何合资、合伙、代理等法律关系”“公司不因供应商的行为而承担法律责任”等免责条款。那么，这么做真的有效吗?

答案是，未必。学习过民法的读者应当都对“委托代理”的法律概念并不陌生。根据《民法典》的规定，“代理人在代理权限内，以被代理人名义实施的民事法律行为，对被代理人发生效力”。而在数据安全领域，这一原则仍然适用。虽然数据领域多强调“数据处理者/控制者”和“受托处理者”的概念，而且对数据违法行为的处罚更多地是属于行政法(而非民法)领域，但其本质仍然适用委托代理法律关系，及其归责原则。相应地，如果受托处理者在收集、处理数据的过程中存在违法的行为，包括民事、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，即使数据的收集、处理完全由受托处理方来进行(数据也完全存储于受托处理方的 IT 环境)，委托方完全不接触数据，受托处理方违法收集或者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。

除了委托代理的法律关系外，数据的提供方和接受方还有可能会构成“共同处理者/控制者”，这一点即使是在数据采购的情形下也不例外。例如，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. 特定行业的考量

除了上文所述的通用风险因素外，特定行业的企业还需要考虑“专属”于其行业的数据采购风险。

举例而言:

1. 医药领域: 医药健康领域向来是强监管领域，数据保护也不例外。医药领域的企业容易接触到生理健康信息等敏感个人信息，因此如果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，即使对非个人信息而言，许多医药企业采购的涉及医院(尤其是公立医院)的数据(例如医院的科室信息、采购数据、统方数据)等在极端情况下可能会被认定为“国家秘密”，从而让企业陷入非法获取国家秘密罪的深渊。

2. 消费品：消费品行业企业通常需要大量的个人信息用于进行市场营销和用户分析。企业需要关注所采购的数据是基于个人画像还是群体画像产生的。相对而言，群体画像的合规风险会低于个体画像。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，该等个人信息较普通个人信息更为敏感，会面临更严格的审查和数据风险。

3. 半导体等先进制造业：制造业虽然通常不过多涉及个人信息，但也不是数据合规的“法外之地”。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. 有效实现风险隔离

了解了采购数据的风险，那么企业到底需要采取何种措施，才能降低风险、实现风险隔离呢？

1. 充分了解业务及数据相关情况

根据我们的过往经验，很多企业最大的数据合规风险，不是数据的性质，不是供应商的管理，也不是内控制度的不完善，而是，企业完全不了解自身的业务使用了哪些数据，如何使用这些数据，也不清楚相关数据在企业的内外部及相关的业务流程中是如何流转的。这导致无论是数据本身的风险、与供应商之间的法律关系、企业的数据合规风险等后续分析都无从谈起，企业处于风险之中却不自知。

因此，我们强烈建议企业对于自身的业务及数据情况进行完整、全面的梳理，最好是能够画出业务、数据流转的详细流程图，并标明涉及的数据类型以及相关内、外部主体。“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. 明确企业与相关方之间的法律关系

鉴于企业与供应商之间不同的法律关系将会给企业带来不同的法律风险，因此如有可能，企业可以主动选择以风险较小的方式来聘用供应商。

首先，尽量避免会被认定为“委托代理”或“共同处理”的法律关系。例如，如无必要，企业不应对个人信息处理的方式和目的进行决定，而应当把决定权交给供应商，由供应商充当“数据处理者/控制者”的角色，企业不给出数据处理的指示，也不接收供应商收集的原始数据，而仅仅接收供应商分析、处理后的数据结果，相当于买“数据报告”，如此可以最大程度避免原始数据中的瑕疵，或者为供应商的违法行为承担法律责任。

如果必须要达成“委托代理”或者“共同处理”的安排，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。虽然合同的约定并不能完全排除企业需要承担的法律责任，但在对数据合规和保护有明确合同约定和承诺的情形下，如果供应商仍然违法收集、处理数据并向企业提供，合同将是企业向执法机关进行抗辩、争取减轻或免除处罚的有力证据。

3. 对所接收数据及供应商进行审查

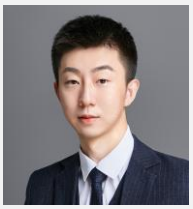
对于特定法律风险比较高的数据(例如敏感个人信息，或者商业秘密等数据)，企业仅通过协议约定的方式还不足以“自证清白”。在这些情形下，企业可能需要进一步“主动出击”，在接收数据前对供应商及提供的数据进行审查，包括对供应商的业务资质、业务模式及历史合规情况进行尽调，以及对数据的内容、来源、获取方式、处理目的、第三方权利等进行摸排，从而帮助企业充分评估与该供应商进行合作以及接收相关数据的风险。

4. 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。这一点在非个人信息领域也同样成立，完善的数据合规内控制度，反映的是企业否定数据违法行为、遵守数据保护法律法规的集体意志，有助于在执法和司法程序中证明相关违法结果的发生并非企业追求的结果，相反企业采取了相应措施来(试图)避免相关结果，以此争取减轻或免除处罚。

如您希望就相关问题进一步交流，请联系：

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

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