并购交易实务之－从合规和资产视角看数据（上）

作者：傅鹏 唐江山 赵卿梦 俞沁

随着数据合规法律体系的建设与完善，数据领域执法活动的持续活跃，以及数据事项相关审查认证的逐项落地，越来越多的并购交易法律尽职调查工作中，专门就数据合规领域开启专项尽职调查；或者至少就数据合规领域的问题，在法律尽职调查中设立专章，进行专项分析。与此同时，数据作为一项重要资产和生产要素的价值越来越彰显，甚至是不少交易中的交易驱动因素之一。本系列文章将从合规和资产角度，审视并购交易中数据相关的尽职调查、合规风险处理、数据资产移交等问题。

作为本系列的首篇，我们将首先探讨数据合规尽调的关注要点，并购交易的情景限于位于中国的并购标的公司或在中国实质开展业务运营活动的全球性企业（“**并购标的**”或“**目标公司**”）。本篇将着重讨论对并购标的进行数据合规尽调的关注角度，关注这些角度的监管背景和原因，并购标的常见数据合规风险等问题。

一、并购交易视角下的数据合规监管现状

（一）主线清晰的立法结构

我国数据合规领域的监管规则呈现在《网络安全法》《个人信息保护法》和《数据安全法》三部核心法律文件中，他们从不同的监管视角出发，统辖不同维度下数据合规的监管框架，共同助力于实现安全网络环境下的数据恰当处理和个人信息适当保护。

收购方对目标公司数据法律合规情况作出研判时，应当把握监管口径、监管对象和监管领域，并有针对性地核查监管要求与并购标的实践之间的合规差距。

1.最早书就与奠定的成熟监管领域：网络安全领域

2016年11月，《中华人民共和国网络安全法》（“**《网络安全法》**”）发布。《网络安全法》对包括关键信息基础设施运营者在内的网络运营者，从网络运行安全、网络信息安全、网络安全检测预警及应急机制等方面提出了全面的要求。网络安全领域是数据合规法律体系中最早开展系统性立法和执法监管的领域。举例而言，就《网络安全法》规定的网络安全等级保护制度，可追溯至2007年发布的《信息安全等级保护管理办法》。

从并购交易角度看，网络安全领域的监管规则可以较为粗略地被概括为关注偏向“硬件”或“基础设施”方面的问题。因此，网络安全领域会涉及、但绝不仅仅包含和个人信息保护、数据安全有关的问题。例如，网络安全领域对网络系统安全设置了等级保护制度，要求企业进行评测、定级、备案、整改；《网络安全法》制度性地提出关键信息基础设施保护制度。这些领域，侧重关注偏网络系统安全、设备和系统运行等方面的问题。

由于近年来个人信息保护领域的监管新规出台密度很高、受到的关注最多（如下文详述），因此部分并购标的可能仅仅侧重于关注个人信息保护领域的规定以及合规要求，并由此可能忽略了同样十分重要的网络安全领域的规定以及合规要求。例如，不乏相当一部分并购标的可能不太关注、甚至完全没有处理过网络安全等级保护的测评、定级、备案、整改等问题。收购方在交易中也需要对此有所关注，不应忽略网络安全领域的监管要求。

2.监管密度最高的监管领域：个人信息保护领域

2021年11月，《中华人民共和国个人信息保护法》（“**《个人信息保护法》**”）正式实施。《个人信息保护法》确立了个人信息处理的基本原则，明确了个人在个人信息处理活动中的法定权利，拓宽了处理个人信息的合法性基础，并就个人信息跨境传输的监管要求作出规定。目前，个人信息保护领域呈现出多部门高度关注、多阶层规范性文件多维监管的态势，是数据合规法律体系中监管规则最为丰富、最受各方关注、监管密度最高的领域。

顾名思义，个人信息保护领域的监管重点，在于如何对个人信息的处理活动进行监管，在商业利用、便利业务发展的大背景下确保如何更好地保护个人信息主体权益。当然，由于个人信息的处理和保护离不开系统与基础设施，个人信息的存储和大量经典处理场景（例如出境）也往往和其他类型的数据相互交融，因此个人信息保护领域的部分监管关注点也不可避免地涉及到网络安全、数据安全领域，但是总体来说，个人信息保护领域的监管还是主要关注保护个人信息、规管个人信息处理活动。

基于上述成熟且精密的监管生态，个人信息保护领域的合规问题，是并购交易中相对容易识别、目标公司相对容易违反的规则领域，应当作为收购方的关注重点。在并购交易开展过程中，收购方宜结合以《个人信息保护法》为代表的个人信息保护规范性文件，就目标公司是否落实个人信息处理者义务，是否履行特定个人信息处理活动的特别要求等进行识别与核查。

3.监管前沿和有待补完的拼图：数据安全领域

2021年9月，《中华人民共和国数据安全法》（“**《数据安全法》**”）实施。《数据安全法》相对宽泛地规定了数据分类分级保护、重要数据保护目录、数据安全风险预警机制、数据安全应急处置机制、数据活动的国家安全审查机制等数据安全管理制度。

数据安全领域的立法和监管工作，作为一个独立垂直领域开始启动，主要集中并爆发于近几年。同时，作为纲领性文件的《数据安全法》更注重宏观制度体系构建。因此，数据安全领域仍有相当一部分较为实质的制度内容（如各细分行业的重要数据目录和分级分类具体指引等），有待后续生效的规范性文件加以完善与补充。

此外，数据安全领域也关涉到一些最前沿、甚至在监管方向和操作范式上都有待进一步探讨的领域，典型如数据交易，这一领域还面临着数据权属基础制度、数据交易安全、数据交易价值确认等基本问题的进一步探索。

尽管数据安全领域一些细节的监管要求有待补完和落实，但是部分行业的主管部门已经就数据安全颁发了生效的监管文件，典型如针对汽车相关行业的《汽车数据安全管理若干规定（试行）》。

因此，收购方在交易中，还是应当根据《数据安全法》的总体要求，结合已经落实的监管细节，以及对具体垂直行业的具体监管要求（如有），对并购标的的数据安全合规情况进行核查。

（二）“全行业化”的监管覆盖面

在《个人信息保护法》《数据安全法》出台前，数据保护（重点体现为个人信息保护）在基本法律层面的规定主要体现在《网络安全法》《中华人民共和国民法典》（“**《民法典》**”）等法律中。

但是，该等规定大多为原则性或纲领性的内容，可以直接作为并购交易尽职调查中合规性判定依据或实践操作指引的内容较少。相关的配套细则主要呈现在自《网络安全法》项下的各行政法规、规章、国家标准性文件中，但是该等配套细则适用的对象更多侧重于《网络安全法》提出的“网络运营者”的范畴。尽管“网络运营者”可以通过解释的方式，在一定程度上涵盖较为宽泛的主体与行业，但是就实际项目操作而言，在对部分传统行业目标公司开展的数据合规审查工作中，可能面临数据合规规范性文件适用界限模糊的问题，需要具体论证和判断（有时甚至只能类比适用）部分目标公司是否属于“网络运营者”。

《个人信息保护法》《数据安全法》的出台将适用范围从“网络运营者”的行为延伸至一般性的“在境内实施个人信息处理活动、数据处理活动”的组织、个人，明确对个人信息保护、数据保护的要求不再仅限于“网络运营者”。如餐饮、线下教育等传统行业中涉及个人信息处理、数据处理的公司同样适用于相关数据监管规则。因此，收购方需要关注对传统行业的目标公司开展个人信息保护合规审查、数据安全审查，避免仅因目标公司所处行业而草率地排除数据合规审查工作。

（三）“垂直纵深”的监管颗粒度

与监管覆盖面横向拓展至全行业领域并行的，是监管机构基于部分行业或业务领域的高度敏感性，制定出一系列适用范围具有鲜明行业指向性、合规要求更高或更具执行性的规范性文件。收购方在对全行业目标公司数据合规审查保持关注的前提下，宜对处于特定行业领域的目标公司的数据安全、个人信息处理、网络安全工作给予更高的重视。

受限于本文篇幅，以下仅就部分热点行业领域及其部分专门规定进行举例：

细分行业领域	行业专门性监管要求举例
金融行业	根据《个人金融信息保护技术规范》《金融数据安全 数据安全分级指南》，应对个人金融信息按照敏感程度从高到低分为 C3、C2、C1 三个类别，对金融数据安全级别从低到高划分为五级，并在处理信息或数据时采取对应级别的保护措施等。 根据《中国人民银行金融消费者权益保护实施办法》，应健全消费者金融信息保护制度；留存向金融消费者说明重要内容和披露风险的相关材料至少 3 年等。
健康医疗行业	根据《信息安全技术 健康医疗数据安全指南》，应留存健康医疗数据控制者使用或披露其健康医疗数据的情况至少 6 年；应对健康医疗数据安全级别从低到高划分为五级，并在处理时采取对应级别的保护措施。 根据《互联网诊疗管理办法（试行）》，互联网医院信息系统实施第三级信息安全等级保护等。
汽车行业	根据《汽车数据安全管理若干规定（试行）》，汽车数据处理者处理的汽车充电网的运行数据，包含人脸信息、车牌信息等的车外视频、图像数据等属于重要数据；汽车行业企业应就重要数据处理活动等向有关主管部门报送年度汽车数据安全管理情况报告，并遵照《数据安全法》等规范对重要数据采取恰当保护措施（如报送风险评估报告等）。

（四）境外个人信息处理者“有条件适用”的监管态度

根据《个人信息保护法》，在境外处理我国境内自然人个人信息，且以向境内自然人提供产品或者服务为目的，或用以分析、评估境内自然人的行为的，应当适用《个人信息保护法》的规定。

为使得前述条款得到切实维护和保障，《个人信息保护法》第五十三条要求，境外个人信息处理者应当向履行个人信息保护职责的部门报送其在境内设立的专门机构名称或指定代表的姓名、联系方式，并由专门机构或指定代表负责处理该境外个人信息处理者在《个人信息保护法》下的相关事务。

基于此，收购方在对目标公司为跨国集团的并购项目进行尽职调查时，如果发现该跨国集团有相对实质的针对我国

境内个人信息的处理活动（例如目标公司的网站服务器设置在境外，但是面向中国境内大量用户提供服务，甚至设置中文网页、设置便利中国用户付款的支付渠道，并实质收集中国用户的个人信息），宜考虑对处理中国境内自然人个人信息的境外实体的处理行为进行合规性审查，并纳入整个并购交易的尽职调查范围内。

由于监管部门尚未出台实施细则，就《个人信息保护法》第五十三条下的报送程序、材料等进行明确，收购方宜在并购交易中要求目标公司（即存在由境外实体处理中国境内个人信息的跨国集团），对《个人信息保护法》第五十三条的实施细则、解释说明保持高度关注，并在相关文件出台后及时在境内设立专门机构或委托代表以履行有关信息的报送义务。

二、目标公司常见数据合规风险及收购方关注要点

（一）个人信息收集不合规

并购交易中，并购标的数据合规的常见问题，可能体现在个人信息收集不尽合规这一方面，举例而言：

1.收集个人信息通常情况下以取得个人信息主体的同意为主要合法性基础，但并购标的在这一环节往往容易出现问题

并购标的收集个人信息，必须具有《个人信息保护法》规定的某一合法性基础，在商业和业务运营场景中最常见的，是需要获得个人信息主体的同意作为信息收集的合法性基础。

并购交易中，并购标的由于种种原因，在这一环节容易出现问题。例如，一些并购标的因为对个人信息保护合规要求缺乏基本了解，没有注意设置一定环节，取得用户的同意。

此外，值得特别关注的是，部分场景下目标公司较难直接取得个人信息主体的同意，此时需要采取一些其他措施，降低合规风险。举例而言，如果目标公司以B端业务为主，且从B端业务合作伙伴获得个人信息，目标公司基本难以直接接触这些个人信息的个人信息主体并获得他们的同意。所以，目标公司往往需要采取如下措施以降低风险：

（1）在业务合作协议中包含数据保护条款，或者与B端业务合作伙伴单独签署了个人信息及数据保护协议，并且通过这些协议或者条款，要求B端业务伙伴（作为数据提供方）承诺其向目标公司提供个人信息已经获得适当同意或具有其他合法性基础，并约定如因个人信息提供给目标公司造成目标公司损失的处理方式与赔偿方；

（2）在涉及大量个人信息的收集合作中，或者在与目标公司主营业务高度相关或特别重要并存在个人信息收集活动的合作中，或者在明显可能存在个人信息收集瑕疵的业务合作中（例如审阅已知信息发现业务合作伙伴较有可能是从第三方购买或通过其他不合规方式获得个人信息），如条件或合作关系允许，目标公司应考虑对业务合作伙伴获得个人信息来源授权同意的适当性进行过一定的核查与确认（例如要求B端业务合作伙伴说明个人信息收集流程及合法性基础；如果以“同意”为基础的，提供获得同意的文书文本，并对同意的范围进行审核）。

如果目标公司未能完成上述工作，则其一方面无法获知（或者至少尽到合理努力以便在一定程度上获知）B端业务合作伙伴向目标公司提供个人信息的实际风险水平，另一方面则是在出现风险的情况下（例如信息提供方确实有较为明显的未经适当授权而向目标公司提供个人信息的行为，甚至引发个人信息主体的诉讼），其没有基本的合同依据向B端业务合作伙伴索偿。

因此，收购方应当在尽职调查中关注，目标公司直接收集个人信息时，是否已经进行告知并获得适当同意；在间接收集个人信息时，是否与个人信息提供方签署如上第（1）点所述的适当数据保护条款，以及是否在业务允许的情况下对个人信息提供方进行上文（2）所述的适当了解与调查。

2.“同意”以外的其他合法性基础的适用条件比较严格

尽管《个人信息保护法》为企业收集个人信息的合法性基础提供了多样化选择，在“同意”以外，设置了其他合法性基础，但是该等合法性基础的适用条件比较严格，在对目标公司尽职调查的过程中，需要慎重决策论证目标公司的部分个人信息处理行为是否确实能够适用“同意”之外的合法性基础。

举例而言，为订立、履行个人作为一方当事人的合同所必需而处理个人信息，是一项单独的合法性基础。适用该场景时，目标公司首先需要满足“必需”的前提，意味着无论是收集/使用个人信息的具体行为和频率，还是涉及的个人信息种类都应满足“必需”。同时，对于该场景下的“合同”指何种类型的文件，也需要特别关注，例如一般来说这里的“合同”应指双方经历充分、平等的意思表示达成的具有实质履行内容的合同，类似于APP中常见的格式条款《用户协议》通常不宜被认定为此场景下的“合同”。

与此类似的，按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需处理个人信息，也是一项单独的合法性基础。适用该场景时目标公司同样需要满足为人力资源管理所“必需”的前提，以及存在满足法定程序的劳动规章制度和依法签订的集体合同。并非任何与员工工作相关的个人信息处理活动，或者发生在员工工作时间段内的处理活动，都可以依赖本合法性基础。

3.需要注意目标公司是否落实收集个人信息的“单独同意”的要求

收集敏感个人信息应当取得个人的单独同意，敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

因此，在对目标公司尽职调查过程中，如发现涉及上述类别个人信息收集的，应进一步审查目标公司是否已落实“单独同意”的要求

（二）疏于制度建设及个人信息保护影响评估（“PIPA”）

1.网络安全等级保护制度

网络安全等级保护制度是对目标公司网络系统的测评、定级和整改，并且对于未及时履行等级保护制度的企业，法律法规也有相应罚则。

但是，在较早时期，特别是在《网络安全法》颁布之前，执法机关没有在所有时间段和所有领域内都对本制度的执行与落实保持较为严格的力度，可能有一些企业没有按时完成网络安全等级保护的评测、备案、整改等工作，但尚未被处罚，因此有的企业疏于开展等保工作。随着2017年《网络安全法》的颁布以及一系列配套国家标准的颁布，等级保护制度进入“2.0时代”；与此同时，与等保制度有关的执法案例频出。从目前的监管视角来看，目标公司如果没有进行等保工作，将面临比以往更高的实际处罚风险。**因此收购方的数据合规尽调有必要关注目标公司的等保完成情况。**

另外，《数据安全法》以及《网络数据安全管理条例（征求意见稿）》颁布后，处理重要数据的系统原则上应当满足三级以上网络安全等级保护和关键信息基础设施安全保护要求，所以随着对企业数据分级分类要求的落实和重要数据识别工作的有序展开，**收购方尽调过程中还需要关注目标公司是否涉及重要数据处理，以及其系统的等级保护定级备案是否达到了三级，目标公司是否按照规定完成评测、备案与整改。**

2.内部制度建设及PIPA

早期对于企业内部合规制度建设和个人信息保护影响评估（在有的文件中亦就实质类似的评估体系称为“个人信息安

全影响评估”，下称“**PIPA**”）的要求主要在《信息安全技术 个人信息安全规范》（“**《个人信息安全规范》**”）等国家推荐性标准中规定，在实践中有很强的指导作用和很高的参考价值，但效力层级低，没有强制的法律效力。在定位上，《个人信息安全规范》属于倡导性的良好实践要求，通常一些规模较大的企业可能会按照规范要求完成，其他大部分公司缺乏落实动力；另外，在《个人信息保护法》和《数据安全法》颁布前，也没有直接对应的罚则，有的并购标的对此重视度不高。

而《个人信息保护法》和《数据安全法》颁布后，目标公司如果未按照要求建设和完善内部制度，或者不按时完成PIPA，都可能面临《个人信息保护法》和《数据安全法》下的处罚。此外需要强调的是，内部制度的建设和PIPA在个人信息权益诉讼纠纷适用“举证责任倒置”的背景下，可以有效帮助目标公司自证其履行了保护个人信息和数据安全的合理义务。因此，没有履行这两项工作，会增加目标公司在数据合规争议中的败诉甚至高额赔偿隐患。

因此，收购方的数据合规尽调，也应当关注目标公司是否进行了适当的内部数据合规建设，是否就法定需要进行个人信息保护影响评估的场景进行了相应评估。

（三）部分典型场景下收购方宜特别关注的数据合规风险

1.APP、小程序等线上渠道

这是比较常见的个人信息处理场景。相当一部分目标公司，包括传统行业的公司，只要有线上宣发渠道或线上商城，都可能涉及。这些线上渠道的个人信息收集和处理合规，是主管机关关注和执法的重点，面临相对严格、密集的监管行动，以及更为体系化、复杂化的监管要求（需要满足一系列针对APP、小程序提出的合规要求）。目标公司线上渠道的不合规行为非常容易被主管机关察觉，可能造成即时性的负面后果，例如公开警告和应用商城下架等。

2.爬取数据的行为

数据爬取行为此前广泛存在于特定行业的公司，比如为营销目的爬取公开的个人信息，或者爬取大量电商、直播信息并汇总为一定的数据集进行售卖。在尽职调查过程中，如发现目标公司存在爬取数据的行为，应引起特别关注，审查目标公司是否遵守了信息来源网站的Robots协议；是否存在故意绕开数据来源技术手段的方式进行爬取；是否有爬取网页（含网页代码）表层公开可见的信息以外的、深入网站数据库（非公开可读信息）的爬取行为；爬取产生的日访问量是否会达到信息来源日均流量的较高比例（视具体爬取情形以及给信息来源服务器可能造成的具体负担而定，例如可以考虑以三分之一或者具体项目中其他更合理的比例）。

3.使用人脸识别摄像头的行为

这一行为是监管的重点。对于人脸识别信息的监管规定比较分散和细致。同时，近期的一些执法案例也日趋严格。例如，浙江多个房地产公司因在售楼处违规安装人脸识别设备被处罚；某卫浴线下门店因违规安装人脸识别和分析设备被处罚；某两家知名汽车厂商线下4S店因违规安装人脸识别和分析设备被处罚。这些案例中，部分场景下，使用人脸识别技术的经营者已经试图在较为明显之处张贴说明、通知，以对消费者进行告知并在一定程度上“获得同意”，但是执法机关在执法过程中采取相对严格的标准，依旧认定经营者违法。

4.算法推荐技术

许多互联网公司基于营销目的或者优化信息服务的目的使用算法推荐技术，也有相当一部分数据营销解决方案公司以此作为主营业务。此外，一些传统行业的公司也会在数字化转型、线上化营销的过程中，使用算法推荐技术。

《个人信息保护法》对应用算法推荐技术的企业提出了更严格、更明确的要求，需要在尽职调查过程中核查目标公司是否均已落实，包括保证算法推荐的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理

的差别待遇；向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式；如果作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过算法自动分析形成决策的方式作出决定。

值得关注的还有近期发布的《互联网信息服务算法推荐管理规定》，对算法设计和使用的过程提出一系列要求，落实了算法使用主体的责任，并具体建立了算法备案制度。收购方需要关注目标公司的算法推荐使用活动，也需要关注目标公司是否已经着手进行互联网信息服务算法备案。

因此，收购方在数据合规尽调中，可注意关注目标公司在上述四个典型的严监管场景下的合规现状，并进行风险研判。

（四）数据本地化与出境

如果在尽职调查过程中发现目标公司存的个人信息或数据出境行为，收购方应当予以特别关注。

在审查信息和数据的跨境行为时，应首先识别信息和数据的种类，分离出受到出境管控、备案要求或需要采取一定行动的信息和数据种类，再结合这些信息和数据适用的监管规则和要求，逐一确认目标公司是否履行了法定义务。目前，针对国家秘密、个人信息、重要数据与核心数据、特定行业数据（如人类遗传资源、地理测绘信息、汽车重要数据、证券活动有关的底稿等），都已有专门的监管要求。举例而言，就目前监管相对成熟的个人信息出境而言，境内向境外提供个人信息的处理者，应当取得个人信息主体的单独同意，应当就出境进行个人信息保护安全评估，应当视传输出境的个人信息的主体数量（例如根据《数据出境安全评估办法》及《个人信息出境标准合同规定（征求意见稿）》的规定，统计目标公司处理的个人信息是否满100万人，是否自上年1月1日起累计向境外提供达到10万人个人信息，是否自上年1月1日起累计向境外提供达到1万人敏感个人信息），提交网信部门进行数据出境安全评估或者与境外个人信息接收方签订网信部门发布的标准合同。

三、未恰当履行数据合规义务的后果和影响

（一）潜在的诉讼风险

《个人信息保护法》与《民法典》的规则相结合，明确了企业在处理个人信息过程中的法律义务，同时也为民事主体个人信息权益的诉讼提供了更明确的法律依据。

此外，《个人信息保护法》明确 了侵害个人信息权益诉讼中赔偿数额的计算方式：首先，以被侵害的个人信息主体受到损失或个人信息处理者因侵权行为获得的利益为标准；其次，在侵害个人信息权益导致的损失或获利无法确定时，根据实际情况确定赔偿数额。司法实践中，法院如何框定赔偿上限和确定具体数额，仍有待实施细则的出台并在司法实践中明确。

特别注意的是，《个人信息保护法》明确了侵害个人信息权益诉讼中的举证责任倒置规则，即处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。如果并购标的发生个人信息权益诉讼，与普通的不适用举证责任倒置的侵权案件相比，其可能面临较重的举证责任，以及随之而来的更高的败诉风险。当然，如上文所述，正是因为存在举证责任倒置的法定安排，收购方更需要关注目标公司是否有较为良好的内部个人信息保护管理制度，是否就重点场景进行过PIPA，因为这些措施有助于在争议中辅助证明并购标的的善意以及已经尽到了部分法定义务。

（二）可能面临的大额罚款、产品下架或停止经营或甚至刑事责任

如目标公司在数据合规领域违反法律规定，其可能面临罚款，甚至是较为大额的罚款。例如，在《个人信息保护法》颁布前，目标公司违法收集或处理个人信息通常会被依照《网络安全法》或《消费者权益保护法》的规定进行处罚，该等法规涉及的法定罚金的上限相对较低。《个人信息保护法》提高了对侵害个人信息权益行为的处罚力度。其中，对于处理个人信息不符合《个人信息保护法》规定或者未采取必要安全保护措施且情节严重的目标公司的违法行为，可能处以五千万元以下或上年度营业额百分之五以下的罚款，极大地提高了企业的违法成本，应当引起所有涉及个人信息处理行为的目标公司的充分重视。

除罚款以外，违反数据合规法律的目标公司可能面临停止产品或服务的后果。例如，《个人信息保护法》规定，如果违反了该法的条款，视具体情形，违法主体可能被监管机关责令改正，给予警告，对违法处理个人信息的应用程序，责令暂停或者终止提供服务。实践中，多部委近年频繁进行联合执法，宣布了多批违法违规收集个人信息的移动应用程序的案例，实践中，对于发现违规收集个人信息的移动应用程序，如果在主管部门要求的时限内未能完成整改，则将被直接从主流应用市场中予以下架，可能对目标公司的主营业务形成直接影响。

最后，除行政责任外，目标公司的数据或个人信息处理活动如果达到一定的违法严重后果，满足刑法的犯罪构成要件（典型如《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》当中规定的情形），目标公司或其主要责任人可能构成犯罪，需要承担刑事责任。

（三）对后续上市的潜在影响

收购方并购一个企业时，可能考虑在该企业运营一段时间后，进行首次公开发行，或者收购方自己进行上市等资本市场运作。因此，收购方在尽职调查中，也应充分考虑目标公司个人信息保护或者数据管理方面是否存在实质影响上市的情况。

1.网络安全审查与国外上市

国家互联网信息办公室于2022年1月4日联合其他部委正式发布了修订后的《网络安全审查办法》，该法规规定掌握超过100万用户个人信息的网络平台运营者赴国外上市需要申报网络安全审查。

就网络安全审查法定审查期限而言，根据适用的程序类型不同：理论上最短法定审查期限约55个工作日；最长法定审查期限约160个工作日或更长的时间。但是，实际操作中，由于材料提交及往复沟通并补充材料需要时间，且提交补充材料的时间不计入上述审查时限，所以实际需要的时间，可能超出上述时间框架。

目前在一些项目中，主管机关对于赴国外上市企业是否需要主动申报网络安全审查的判定态度仍比较模糊，不一定会向企业明确表达其是否需要报送。此外，特别值得关注的是，即使企业没有达到上述提及的申报门槛，进而决定不主动进行网络安全审查申报，后续主管机关仍可以依职权要求企业进行申报。

所以并购标的以及收购方应关注的是，提前对并购标的的个人信息处理和数据处理现状进行摸底，了解是否存在显著风险，对是否需要申报网络安全审查，以及是否有可能被主管机关主动启动网络安全审查进行较为谨慎的研判。例如，对于是否“掌握超过100万用户个人信息”，是否属于“网络平台运营者”，应当以更为严格的尺度进行全面衡量和评估，需要审慎判断公司的个人信息和数据处理活动是否可能影响国家安全，以免打乱既有时间表，将上市计划拖入被动局面。

2.上市监管机构在企业上市过程中对数据合规问题施加更高的关注

日趋严格的数据监管导致交易所和证券监管机构在上市审核过程中对发行人数据合规方面施加越来越多的关注，特

别是企业境内上市和香港上市。**我们建议收购方在对尽职调查的基础上，针对数据相关的尽调发现从上市角度进行评估，排除可能构成上市障碍的问题，并在交易后对尽调发现进行有针对性的整改。**

(1)数据收集、使用和共享的合规性

例如，监管机构可能重点关注并购标的（即未来的发行人）是否存在未经授权获取用户数据的情况、获取个人数据是否对用户有明示提示、收集的数据是否限制在必要的范围内、是否仅概括性提示收集用户信息、是否超出用户授权范围使用数据或存在未经其他平台的授权直接收取数据的行为。

(2)数据规模和权属

监管机构可能重点关注并购标的收集及储存的用户信息规模，数据收集使用情况，上市前后保护个人信息和数据安全的安排，是否符合《个人信息保护法》《数据安全法》等法律法规要求；并购标的及其原料数据采集供应商相关数据的获取方式及其合规性，并购标的是否享有数据的所有权或获得相关数据主体的授权许可，相关授权许可是否存在使用范围、主体或期限等方面的限制；并购标的及其原料数据采集供应商是否存在超出上述限制使用数据的情形，是否存在数据内容侵犯个人隐私或其他合法权益的风险。

(3)企业内部数据和网络安全管理制度

监管机构可能重点关注并购标的内部是否就个人信息保护、网络安全和数据安全，建立了相对完善的内部流程制度；实际运行中，并购标的是否对内部流程制度进行了行之有效的落实。

(4)主管部门数据立法与监管活动对企业未来合规趋势的影响

监管机构关注的问题中，有时可能涉及对未来合规趋势的影响，例如可能要求发行人说明一些已经颁布的征求意见稿对发行人业务的适用性，说明如果征求意见稿正式生效，对发行人业务可能存在的影响等。

（四）对目标公司价值及并购对价的影响

作为并购交易商业考虑的核心要点之一，目标公司不合规的情况是否影响标的估值及并购对价金额，是收购方及出售方都最关注的问题之一。

考虑到近年来数据合规领域的监管不断升温，违法后果愈发严重，如果目标公司确实在数据合规领域的某些方面存在实质的违法行为，可能对并购结构的设计以及交易对价产生影响。

以最受监管关注的个人信息保护领域而言，根据我们的经验，如果目标公司的部分业务确实涉及到个人信息保护是否合规的敏感边界，特别是如果涉及到这一话题问题频发的一些行业领域（典型如个人授权不甚清晰（且不容易清晰获得）的部分精准室内定位业务，数据来源不甚清晰的部分在线HR猎头业务，授权不甚清晰的部分在线个人大数据征信业务等），**收购方需要根据数据合规尽调的具体结构，审慎评估是否需要停止目标公司的部分业务，或者是否需要对该等业务进行剥离。如果需要停运或剥离，则收购方相应地会考虑这一操作对目标公司的业务收入的影响，以及是否因此需要调整收购价款。**

以上，我们重点介绍了数据合规尽调的关注角度以及并购标的常见数据合规风险。在下一篇文章中，我们将讨论何种类型的并购项目更应注意开展数据合规专项尽调，在并购项目交易文件中如何处理已经识别的数据合规问题，以及收集尽调材料过程中有哪些值得关注的数据合规问题。

2022-07-11