

并购场景中的数据转移若干问题初探

作者：蔡航、杨洪泉、姚婷、葛鹤

前言：并购语境下数据合规问题的复杂性

数据作为一项资产，其重要性在企业运营中的作用日益凸显，在一些经营模式中，数据的持有量以及处理能力已构成企业的核心竞争力与价值所在。

并购活动特别是跨境并购中，针对参与并购企业的数据合规监管具有复杂性：

1. **并购中的数据转移行为受到多个执法部门监管。**监管机构组成既有网络安全及数据安全一般执法部门，也有反垄断执法部门，某些数据内容亦涉及来自行业主管部门的监管（例如对于医疗数据而言，相关医疗医事领域主管部门），特种数据（例如人类遗传资源数据）还受专门设置的监管机构管辖；
2. **单一项目可能受到不同法域内主管部门的监管。**例如，Google 收购 Github 案中的数据反垄断合规问题，受到美国、欧盟及澳大利亚多国的审查；
3. **数据于宏观层面涉及国家及公共安全，于微观层面具有资产属性，受到跨部门法多元规制。**例如，个人信息附带个人对其自身数据的请求权，受到《个人信息保护法》及《民法典》保护，经营者获取的数据受到《反不正当竞争法》的保护。因此行为主体的数据违规行为易招致民事诉讼；大量数据集合并后可能还涉及国家安全及社会公共利益，违规收集使用数据的主体可能会受到行政处罚乃至承担刑事责任。

此外，随着中国网络安全及数据安全法律法规日益健全以及执法的严格化，网络安全与数据安全领域的行政处罚涉及没收违法所得或根据营业额数额计算罚款额度等惩罚手段，一旦被监管部门确认为严重违法行为，可能给企业带来巨额罚单，并且影响其后续上市或其他资本市场行动。

正因为数据问题的复杂性与违法处罚导致的后果的难以预见性，并购交易时对于交易方数据的专项尽职调查尤为重要，不过这并非本文探讨的重点，本文主要探讨并购交易在进行时企业数据转移带来的衍生问题对交易架构可能产生的影响，其中并购中可能出现的数据反垄断合规已在《新反垄断法解读系列：并购交易中的数据与反垄断监管》中阐述。本文将重点阐述并购活动涉及的数据迁移、数据本地化存储以及数据出境等问题。

一、资产收购项下个人信息数据迁移法律适用

1. 资产收购相较股权收购场景更加容易产生个人信息转移合规义务

在典型的股权收购案中，因数据处理者的法律主体不会进行变更，因此数据一般不会仅因股权收购的完成而发生转移。与员工迁移事宜（可见《浅析业务线收购交易中的员工安置问题》一文）类似，个人信息数据迁移是资产并购情境下比较突出的法律问题。在《网络安全法》实施前，因数据合规的成本较低，不少 TMT 公司之间的并购以资产并购的方式进行。但在《网络安全法》、《数据安全法》、《个人信息保护法》以及配套规则和行业标准陆续出台及加大执法力度的今日，此种交易架构是否仍具可行性，应根据个案进行具体评估。

新经济企业可能涉及到大量对 C 端的服务，其用户由庞大的消费者人群构成，为服务之需要，这些消费者已经将大量的个人信息授权给企业使用，在部分业务场景中极具商业价值。在资产并

购发生时，买方一般希望这些个人信息随整体资产包一起发生转移。然而，个人信息的转移因存在诸多合规要求，如何适用转让规则以尽量保证用户个人信息集的完整性，从而确保资产包的商业价值，是交易双方共同关心的课题。

2. 资产并购模式中个人信息转移一般规则

资产并购项下个人信息数据迁移法律适用，主要存在适用《个人信息保护法》（以下简称“《个保法》”）22条或是适用23条的实务差异。《个保法》第22条和第23条的规则如下表所示：

表一：《个保法》第22条及第23条对比

条标	适用情形	行为要件	接收方变更原先的处理目的、处理方式的
22条	个人信息处理者因合并、分立、解散、被宣告破产等原因需要转移个人信息的。	向个人告知接收方的名称或者姓名和联系方式。	重新取得个人同意。
23条	个人信息处理者向其他个人信息处理者提供其处理的个人信息。	应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。	

3. 资产并购模式下《个保法》22条和23条适用之辨

《个保法》22条和23条均为个人信息处理者向第三方转让个人信息的规则，23条为一般规则，22条为特殊规则，适用于因“合并、分立、解散、被宣告破产”等情景下的个人信息转移的情况；22条要求的转移要件更为宽松，只需要对个人履行告知义务，且告知的内容可以只包括姓名和联系方式，而无需包括处理目的、处理方式和个人信息的种类。

在并购落地执行时，若根据22条执行个人信息转移，则相关小程序、应用或者网站弹窗告知相关个人即可；而根据23条操作时，除弹窗告知外，还应安排用户勾选或点击“同意”，用户不进行勾选操作或者拒绝迁移，则买方会损失该用户的信息甚至损失该用户。损失的用户数量达到一定程度，甚至会影响资产包的整体商业价值。因此，在没有其他障碍的情况下，交易双方倾向于选择适用22条的规则，这样的操作方式简单，且能够最大程度确保资产包的商业价值。

《个保法》22条的特殊规则是因合并、分立、解散、被宣告破产等情景下的个人信息转移的情况，是否直接涵盖“并购”情形，值得商榷。“合并”一词在《民法典》与《公司法》项下具备更特定的含义，也是市场监督管理总局管理的特殊类型的工商变更，即更类似于“吸收合并”，也即英美公司法体系下的“Merge”，是与“分立”互为相反情况的措辞，《个保法》此处“合并”是否包含吸收合并之外其他类型的“并购”值得谨慎斟酌其适用。

相关案例

2022年2月，某跨国运动品牌宣布完成旗下某子品牌的出售，其选择直接使用《个保法》二十二条。在中国的消费者收到了其个人信息将被转移的通知，但并不是所有的消费者都满意仅仅“被通知”的结果。

在上述案例中，若经过交易双方协商，该项资产并购项下的个人信息转让都只能适用 23 条而不适用 22 条，则交易双方可能就个人信息转让的成果设置专项并购价格调整机制；若预估适用 23 条将导致大量个人信息不被二次授权，使得资产包商业价值锐减，为保证资产包的价值并兼顾合规性，交易结构可能会出现颠覆性调整：从资产收购模式变更为股权收购模式。

4. 资产并购数据转移特殊规则

除上述一般规则外：若资产包标的涉及特殊行业或涉及到特殊主体，相关资产包在转移时，还应符合特殊行业涉及该特殊主体的数据转移规则（详情可见本文第二部分）；若买方为外方，标的资产包的数据将转移给外方的，还需考虑数据本地化及数据出境事宜（详情可见本文第三部分）。

二、其他特别种类的数据转移规则

个人信息因为其数据内容特殊，涉及到个人的隐私与权利，同时又因大量个人信息集合的转移会影响社会安全，因此《个保法》特别规定了个人信息转移的规则。

除对于个人信息转移的限制外，相关法律法规会因数据主体特殊、数据重要程度特殊、数据行业属性特殊对相应类别的数据的转移进行规范。下文对相关特殊安排进行了非穷尽式列举：

1. 特殊数据主体的特殊转移规则：儿童数据

儿童数据因主体特殊，区别于一般的个人数据，转移儿童数据具有更高的标准。根据《儿童个人信息网络保护规定》，网络运营者转移儿童个人信息的：

- 网络运营者应以显著、清晰的方式告知儿童监护人，并应当征得儿童监护人的同意；
- 网络运营者应当自行或者委托第三方机构进行安全评估；
- 若转移前后儿童个人信息使用及存储的目的、方式和范围、存储的地点、期限和到期后的处理方式、安全保障措施、更正、删除儿童个人信息的途径和方法等存在变更的，需要在征求监护人同意时明确告知该等事项。

由于《儿童个人信息网络保护规定》于 2019 年发布并实施，早于《个保法》的发布和实施时间，对于其中转移儿童个人信息均需征得儿童监护人的同意的“一刀切”要求，似与《个保法》第 22 条（因合并、分立、解散、被宣告破产等原因需要转移个人信息的，无需个人同意）有所冲突，《个保法》实施后《儿童个人信息网络保护规定》的该要求是否仍然适用，有待立法部门后续进行解释澄清。

2. 因数据重要性程度特殊导致转移规则特殊：重要数据

2017 年 6 月 1 日生效的《网络安全法》中首次出现了“重要数据”这一表述，但《网络安全法》并未对重要数据进行定义。此后网络安全以及数据安全领域的各项规则、国家标准及两者的征求意见稿就不断提及“重要数据”，例如 2022 年 7 月 7 日发布的《数据出境安全评估办法》定义了数据出境领域的“重要数据”：“是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。”

目前尚无统一的关于“重要数据”的概括性概念，但相关规则或征求意见稿中“重要数据”的概念与《数据出境安全评估办法》均比较接近。2021年9月1日生效的《数据安全法》没有对重要数据直接作出定义，但明确了国家建立数据分类分级保护制度，国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护，因此，“重要数据”的具体清单待主管部门在后续工作中逐渐制定并公布。

正如重要数据的具体清单未最终明确，重要数据的转让规则也未完全明确，但经观察相关法律法规的征求意见稿可以看出，未来主管部门很可能会对重要数据的转让进行特殊要求：《网络数据安全条例（征求意见稿）》（目前已被国务院列入2022年立法工作计划）第14条规定，数据处理者发生合并、重组、分立等情况的，**数据接收方应当继续履行数据安全保护义务，涉及重要数据和一百万人以上个人信息的，应当向设区的市级主管部门报告**；第29条规定，重要数据的处理者，应当在识别其重要数据后的十五个工作日内向设区的市级网信部门备案，处理数据的目的、范围、类型及数据安全防护措施等有重大变化的，应当重新备案。

重要数据的出境规则已基本明确，可见本文第三部分。

3. 特殊行业的特殊转移规则：工业数据、重要互联网平台

《工信数据安全管理办法草案》规定，工业和信息化领域数据处理者因兼并、重组、破产等原因需要转移数据的，应当明确数据转移方案，并通过电话、短信、邮件、公告等方式**通知受影响用户。涉及重要数据和核心数据的，应当及时向地方工业和信息化主管部门（工业领域）或通信管理局（电信领域）或无线电管理机构（无线电领域）更新备案。**

根据《网络数据安全条例（征求意见稿）》规定，**汇聚掌握大量关系国家安全、经济发展、公共利益的数据资源的互联网平台**运营者实施合并、重组、分立，影响或者可能影响国家安全的，应当按照国家有关规定，**申报网络安全审查。**

4. 特殊数据转移操作建议

若拟转让的资产包涉及儿童个人信息的，则需要指定儿童数据转让的特殊方案，并在交易交割前推进开展安全评估工作。

因重要数据以及部分特殊行业数据的转移规则相关立法已经纳入日程表，交易方应当留意规则的出台及变化情况，并留意主管部门逐步明确的“重要数据”范围，提前做好重要数据或特殊行业数据转移的规划。

三、数据本地化及数据出境事宜

当买方是外方时，数据本地化与数据出境监管规则也极有可能影响收购项目的整体执行成本、交易架构以及交割节奏。

在中国法律框架下，数据“本地化”和“数据出境”是有所区别但又紧密联系的两个不同概念。“数据本地化”通常是指数据需“存储于境内”或“境内有备份”。

但数据本地化要求并不天然导致数据不能出境，对于存在数据本地化要求的数据，在确有必要的情况下通常数据仍可以出境，但需要遵守一系列的数据出境合规义务，包括进行评估或其他要式行为；而对于没有数据本地化义务的数据，数据出境需遵守一系列的数据出境合规义务，包括进行评估或其他要式行为。《网络安全法》、《数据安全法》和《个人信息保护法》均采用此“二分法”来阐述数据本地化和数据出境这两个概念的关系。

尽管如此，在三部法律出台前已颁布的一些个别法规中，“数据本地化”也含有“数据不能出境”的含义，企业仍需具体规定具体分析。

1. 数据本地化要求

并非所有的数据均有数据本地化要求，目前三大类别的数据具有数据本地化要求：关键信息基础设施数据及重要数据、大规模的个人信息数据以及特殊行业数据。下表对这三个类别的数据进行了非穷尽式列举：

相关法规	本地化要求	是否可以出境
《网络安全法》	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储	前者待细化明确；后者可以，但应当履行出境合规行政义务
《个人信息保护法》	关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者收集的个人信息应当在境内存储	可以，但应当履行出境合规行政义务
《人口健康信息管理办法（试行）》	不得将人口健康信息在境外的服务器中存储	不得托管、租赁在境外的服务器
《关于印发国家健康医疗大数据标准、安全和服务管理办法（试行）的通知》	健康医疗大数据应当存储在境内安全可信的服务器上	因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核
《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》	在中国境内收集的个人信息金融信息的储存、处理和分析应当在中国境内进行	除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息
《地图管理条例》	互联网地图服务单位应当将存放地	地图服务单位很可能

例》	图数据的服务器设在中华人民共和国境内，并制定互联网地图数据安全管理制度和保障措施	会被列为关键信息基础设施运营者，具体规则待明确
《汽车数据安全 管理若干规定 (试行)》	重要数据应当依法在境内存储	因业务需要确需向境外提供的，应当通过国家网信部门会同国务院有关部门组织的安全评估
《网络预约出租 汽车经营服务管 理暂行办法》	网约车平台公司应当遵守国家网络和信息安全有关规定，所采集的个人信息和生成的业务数据，应当在中国内地存储和使用，保存期限不少于 2 年	除法律法规另有规定外，所采集的个人信息和生成的业务数据不得外流

根据上述表格，数据本地化要求是否可以出境还分为两种情况：数据本地化后仍可以依法安排数据出境、数据本地化后仍无法安排数据出境。

若交易买方是外方，且交易采用资产收购方式进行，买方应当将数据本地化成本进行考量；若相关数据本地化后仍然无法依法出境的，则建议买方考虑设立中国境内运营实体，以承接需要本地化的数据，并搭设境内数据管理团队或其他必须运营团队，以避免被认定为“数据出境”。

2. 数据出境评估

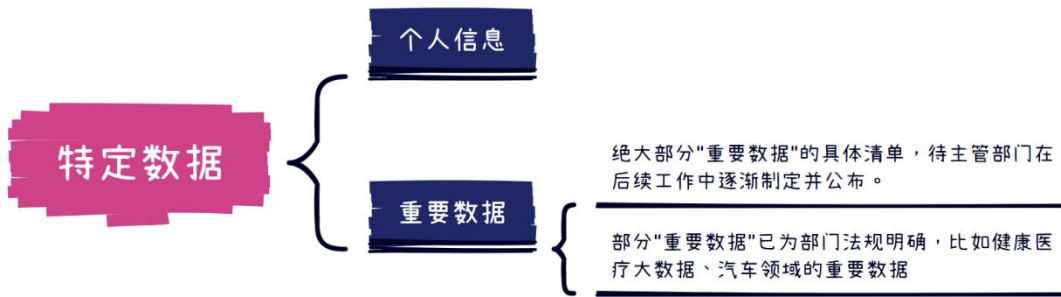
不是所有的数据都可以直接出境的监管要求极大提高了涉及数据并购交易的难度及流程的复杂度。

根据国家互联网信息办公室就拟于 2022 年 9 月 1 日生效的《数据出境安全评估办法》的答记者问，数据出境是指：

- 数据处理者将在境内运营中收集和产生的数据传输、存储至境外（“实质出境”）；或
- 数据处理者收集和产生的数据存储在国内，境外的机构、组织或者个人可以访问或者调用（“境外可访问”）。

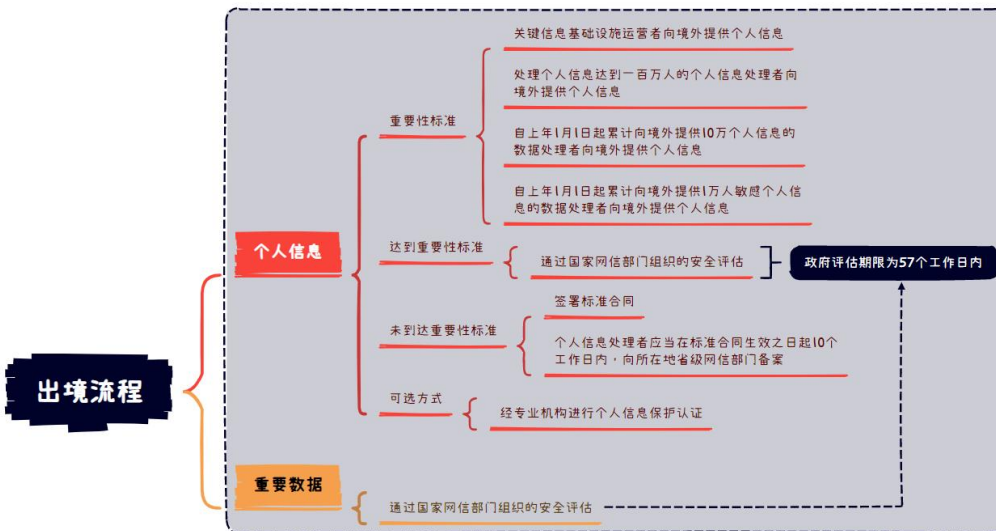
根据上述规定，在股权收购或者资产收购交易中，若卖方作为数据处理者向买方转移法律规定的特定数据（见下文），或者卖方将拟转让标的公司转让予境外买方后，境外买方可以访问或者调用法律规定的标的公司的特定数据，则买方应当将数据出境相关行政义务履行流程纳入交易方案整体进行考虑。实质出境与境外可访问均作为“数据出境”行为认定，实质上宽泛性认定了数据出境行为。

受到《数据出境安全评估办法》监管的特定数据包含两种数据：



下图说明了出境合规流程以及触发数据出境安全评估的重要性标准。简言之：

- 重要数据出境均应评估；
- 个人信息出境达到重要性标准的，应当进行评估；
- 个人信息出境不符合重要性标准的，应当与境外接收方订立按照国家网信部门制定的标准合同，或取得专业机构的个人信息保护认证。



对于个人信息，除上述出境流程外，境内的个人信息处理者还应履行如下普遍性义务：

- 事前进行个人信息保护影响评估，并对处理情况进行记录；
- 告知个人境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项；
- 取得个人的单独同意（有其他合法依据的除外，见个人信息保护法）。

因此，重要数据与达到重要性标准的个人信息出境流程冗长，且因为境外可访问境内数据也作为“数据出境”行为进行认定，实质上大大提高了涉及个人信息并购的时间跨度与难度：买方不仅需要履行耗时较久的安全评估流程，还应取得相关个人单独同意，对交易的节奏及交易后留存的有

效个人信息数量均有影响。为减少相关数据出境流程对交易的影响，买方可视情况设立境内实体并搭设境内 IT 及运营团队，以避免数据实质出境或境外可访问现象。

四、结语

随着网络安全与数据安全立法健全化及执法严格化，网络安全与数据安全义务足以影响涉及数据的并购交易的交易结构以及交割节奏。在充分完成尽职调查流程基础上，建议交易各方结合相关要求，确立最佳的交易方案。



蔡 航 | 合伙人

业务领域：风险投资与私募股权、收购与兼并、医疗与生命科学

邮箱：caihang@anjielaw.com



杨洪泉 | 合伙人

业务领域：科技、媒体和电信（TMT）、数据保护和网络安全、合规

邮箱：yanghongquan@anjielaw.com



姚 婷 | 合伙人

业务领域：风险投资与私募股权、收购与兼并、医疗与生命科学、一般性公司事务

邮箱：yaoting@anjielaw.com



葛 鸽 | 律师助理

业务领域：私募股权投资、融资、合规

邮箱：gege@anjielaw.com