



数据合规专题

第六期

从第三方获取数据的合规建议

(2025年1月)

在日常经营管理中，为提高数据收集的高效性及广泛性，部分数据收集者选择通过购买、交换、共享等方式从第三方获取相关数据。在此过程中，若数据收集者对第三方缺乏充分地了解及约束，可能会因此陷入违法违规处理数据的不利境地。因此，从第三方获取数据时，数据收集者应采取更为审慎的态度以避免出现相关风险。

一、加强合法合规性审查

为保证数据收集的顺利进行、避免产生不必要的纠纷，数据收集者从第三方获取数据时，应当加强对第三方及所涉数据的合法合规性审查。

1、审查第三方资质及数据安全管理能力

在资质审查中，除审查第三方的营业执照、经营及征信等情况以确认其基本信息的真实性和完整性外，还可着重审查第三方是否具备从事相关业务的行政许可或资质，例如：第三方从事经营性互联网信息服务的，应办理互联网信息服务增值电信业务经营许可证；第三方为通过应用程序提供互联网新闻信息服务的应用程序提供者的，应取得互联网新闻信息服务许可等。通过对前述文件及信息的审查，可以



有效核实第三方主体资质，为后续的数据收集提供一定的可信基础。

对于深度合作或单次数据收集的数量及影响范围较大的，还可进一步了解第三方的数据安全能力以及是否存在违法违规记录等情况，包括：是否制定个人信息保护、数据安全、网络安全事件应急预案等内部制度及规范；在数据传输过程中，是否会采取有效措施以及采取何种措施以防止出现数据篡改、窃取等风险；是否存在网络安全、数据安全、个人信息保护等方面的负面舆论、行政通报或处罚、司法案件甚至刑事犯罪等情形。

2、审查第三方数据来源合法性

与直接从数据权利主体处获取数据不同，从第三方获取数据属于间接获取，还可能存在多次“转手”情形。因此，有必要对数据来源进行合法合规性审查，尽可能减少发生争议的可能性。

在审查第三方数据来源时，须注意审查第三方取得数据的依据或基础，并要求第三方提供相关证明文件。实践中，常见的证明文件包括：数据权利主体的授权文件，如用户隐私政策、个人信息授权书等个人信息授权文件，以及与企事业单位等其他数据权利主体之间就收集、处理及转让相关数据签订的协议等；其他可证明第三方权利的文件，如监管部门的批准函件、为履行法定职责或法定义务而获取相关数据的说明或其他相关证明材料等。

在审查数据来源的合法性时，还应特别注意进一步审查第三方获得的授权范围是否包含己方的使用范围及目的，以避免出现因超出数据权利主体授权范围而导致的违法违规处理数据的情形。例如：审查



数据权利主体是否实际授权第三方对外提供其相关数据以及授权的条件、应用范围和期限等，是否对第三方对外提供数据设置了限制条件（如仅可转让给特定主体、对受让方资质设定了特殊要求）。

在审查第三方资质及所提供数据的过程中，须同时做好审查情况的记录及留存工作，包括留存第三方主体信息、数据来源合法性资料、己方有权使用相关数据的证明材料以及第三方所涉的司法案件或行政处罚等。做好前述工作，不仅能对第三方及所涉数据有更深入的了解从而作出更合适的决策，也能于争议发生时在一定程度上证明己方的审慎态度及采取的切实举措。

二、明确数据合规方面的义务及责任

对第三方及其数据来源的审查有利于数据收集者对所获取数据的合法合规性有初步的认识和判断，但是对于合作过程中可能产生的数据合规风险仍需第三方及数据收集者共同防范，双方可通过签订合同等方式明确各自的义务和责任。

例如，实践中作为数据供应方的第三方有义务保证数据的合法性，因而可在合同中设置“第三方对所提供的数据来源、使用目的及范围，是否有权对外提供数据、对外提供数据是否会侵犯相关权利主体的合法权益，是否采取了必要的数据安全保障举措等事项作出承诺；以及第三方违反前述承诺应承担的责任”的条款。

三、数据获取与处理中的监督与管理

在数据获取与处理阶段，除应严格根据法律法规规定及合同约定



履行相关义务外，数据收集者还应详细记录、管理从第三方获取的数据，以便对相关数据处理全流程实时监管，确保在发生数据安全事故时能够有效追根溯源，在保障数据权利主体合法权益的同时维护自身权益。例如，数据收集者可以建立数据处理台账，详细记录从第三方收集的数据内容、数量、时间、类型、用途、处理方式、处理记录等事项，持续监管并定期核查数据的使用、处理及保护动态，以避免数据安全事故等相关法律风险。

若在数据获取与处理过程中，发现第三方存在违法违规违约情形的，如未采取约定的加密、访问控制等数据安全保护措施，或因第三方原因导致出现数据泄露、篡改等情形的，数据收集者可根据法律法规规定及双方约定，视情节轻重及时采取要求第三方限期改正或终止与其之间的合作等措施以有效维护自身权益，必要时还应依法依规告知数据权利主体及相关主管部门。

北京道商律师事务所

2025年1月【 】日