

千山叠障，百川赴海：北京自贸区数据出境负面清单解读（上篇）

作者：段志超 | 王雨婷 | 张子谦 | 李雅琪

导言

2024 年 8 月 30 日，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局会同有关部门制定发布了《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》（“《管理办法》”）、《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024 版）》（“《负面清单》”），适用于在北京自贸试验区内登记注册、开展数据跨境流动等相关活动的企业、事业单位、机构、团体或其他组织。

《负面清单》首批选取汽车、医药、零售、民航、人工智能 5 个领域，详细列举 23 个业务场景和 198 个具体字段。主管部门将采取动态管理机制，未来将分行业、分领域、分批次推进清单编制工作，持续优化迭代负面清单政策体系。

下文将针对《管理办法》与《负面清单》内容进行简要介绍，并详细分析汽车行业、零售与现代服务业、人工智能训练数据三个行业领域的清单内容，及其对该等行业企业的影响。后续我们将继续发布针对医药行业、民航业数据清单的解读。

一、概要

《管理办法》规定了负面清单制定及管理、实施、监督管理等事项，并通过附件《中国（北京）自由贸易试验区数据分类分级参考规则》（“《数据分类分级参考规则》”）明确重要数据统一识别参考规则。《负面清单》则是通过分行业分领域的方式，明确了汽车行业、医药行业、民航业、零售与现代服务业、人工智能训练数据等五个行业领域中需要通过数据出境安全评估（“安全评估”）、个人信息出境标准合同备案（“标准合同备案”）、个人信息保护认证的数据清单，并明确该等行业中的重要数据类别。

（一）管理流程

数据处理者根据负面清单出境数据时，需向相应的自贸组团提交申请，自贸组团会对数据处理者提交的申请材料进行审核并在 5 个工作日内反馈审核结果，并协助通过审核的数据处理者开展负面清单使用备案、指导数据处理者申报安全评估、标准合同备案、开展个人信息保护认证。

（二）数据分类分级与重要数据识别

《数据分类分级参考规则》响应国家数据分类分级保护的监管框架，提出重要数据统一识别参考规则以及 13 类 41 子类数据分类分级参考规则。重要数据的统一识别规则包括：

- 北京自贸试验区企业掌握的 1,000 万人以上个人信息（不含敏感个人信息）；100 万人以上敏感个人信息；10 万人以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的个人敏感信息；
- 关键信息基础设施运营者掌握的 10 万人以上个人信息；
- 北京自贸试验区企业在研发设计过程、生产制造过程、经营管理过程中收集和产生的与行业竞争力、行业生产安全相关的高价值敏感数据；涉及国家安全的企业供应链相关数据；
- 北京自贸试验区企业掌握的关系国计民生领域的自动控制系统参数以及控制、运行维护、测试数据。

《数据分类分级参考规则》所提出的重要数据识别规则符合重要数据的定义，考察该数据一旦泄露或非法利用是否可能“危害国家安全、经济运行、社会稳定、公共健康和安全”。在此基础上，《负面清单》针对不同行业的重要数据类型提供了更具体的字段描述。后续《负面清单》将结合相关行业主管部门制定的重要数据目录以及行业需求动态更新。

二、汽车行业

根据《负面清单》，汽车行业的 7 类重要数据及 2 类个人信息需要通过安全评估开展数据出境；2 类个人信息需要通过标准合同备案、个人信息保护认证出境。值得注意的是，该清单适用于汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等，但《负面清单》明确规定“自动驾驶领域相关企业不适用本清单”。

我们了解到主管部门已着手制定专门针对自动驾驶领域的数据出境监管细则与数据清单。因此，自动驾驶企业可持续关注自贸区相关立法，并相应调整数据出境策略。

（一）重要数据出境

《汽车数据安全若干规定（试行）》（“《若干规定》”）规定了汽车行业的重要数据类别，《负面清单》在此基础上明确了部分类别重要数据的应用场景，并对其定义与范围提供了字段级的说明。

1. **涉及军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据；在向政府机关、军工企业及其他敏感重要机构提供车联网信息服务过程中产生的不宜公开信息**

其中，重要敏感区域的地理信息包括涉及的车辆精准坐标、行踪轨迹，也包括该等区域的地址，在《负面清单》发布前，“地址”这一字段的敏感性可能并未得到行业内的充分重视。

服务敏感重要机构过程中产生的不宜公开的信息包括“军工企业较长一段时间内的联网汽车相关的信息”，这一字段可能广泛包含与军工企业就网联汽车项目合作过程中产生的各类数据，体现出主管部门对于敏感重要机构车联网数据的强监管态度。根据我们的观察，服务政府机关、军工企业及其他敏感重要机构的软件供应商，通常会在客户侧私有化部署车联网信息服务软件与系统，以期在最大程度降低企业自身处理重要敏感数据的合规义务与风险。针对确需处理客户网联数据的情况，企业通常采取严格的权限管控措施、制定客户数据管理制度，规范访问、分析、使用敏感重要机构客户数据的行为，包括限制相关数据出境活动。

2. 车辆流量、物流等反映经济运行情况的数据

根据《负面清单》，车流数据包括路面交通流量数据，物流数据包括物品流转精确路径信息。开展货运、物流业务的企业通常需要实施监控并记录物流车辆的精准定位与行踪轨迹，并在地图上可视化展示相关路径，这种情况下可能涉及处理物品流转精确路径信息。若相关监控平台部署在境外、或由境外技术团队负责运维，则可能涉及物流数据出境。

3. 能够反映一定区域内汽车充电网运行情况的数据

在《负面清单》提供的字段级描述中，充电桩/站位置信息、使用状态属于典型的电网运行情况相关字段，除此之外，计费 and 支付信息也属于重要数据的范围。除原始数据外，充换电车辆统计信息、站点统计、分布信息等统计类型数据也会被纳入重要数据的范围。

实践中，充电行业企业处理的数据类型相较《负面清单》提供的字段示例可能颗粒度更细，例如充电订单号、充电设备接口编码、开始/结束充电时间、电费金额、服务费金额，根据《负面清单》目前的规定，该等数据可能均会落入“计费和支付信息”的范畴，构成重要数据。此外，在重要数据统一识别参考规则的基础上，《负面清单》进一步将这一类别的重要数据限定为“能够反映一定区域”充电网运行情况的数据，如何划定该等“区域”的范围，有待主管部门进一步明确。

4. 包含人脸信息、车牌信息、路牌信息等的车外视频、图像数据

在《若干规定》基础上，《负面清单》将包含路牌的车外视频、图像数据也纳入重要数据的监管范围，这意味着企业数据匿名化的范围将从人脸、车牌信息延伸至路牌信息。

5. 包含车辆远程操控、车辆工况等的关键车联网信息服务数据

根据《负面清单》，这类重要数据包括身份鉴权信息、车辆远程操控类信息、车辆工况类数据、涉车服务类数据、车联网服务平台基础属性数据、车辆外部环境感知数据。参考《YD/T 3751-2020 车联网信息服务数据安全技术要求》，这一范围涉及车联网信息服务的所有环节和服务类别。

在汽车行业数据出境实例中，该等数据通常具有个人信息的属性，因此，诸多汽车行业企业将该等数据作为个人信息申报安全评估或标注合同备案。未来，数据处理者使用《负面清单》出境数据的，应注意将该等数据作为重要数据管理。

6. 包含车辆控制等在线升级数据；包含电控单元等售后数据

《负面清单》详细列举了 OTA 在线升级场景的重要数据字段，范围几乎涵盖了 OTA 升级所涉及的各类数据，这与数据出境主管部门一直以来对 OTA 升级数据出境的严格监管态度是一致的。根据我们的观察，有鉴于 OTA 升级相关的技术安全与内容安全风险，并综合考虑该场景数据处理本地化的可行性，数据处理者针对 OTA 升级数据出境场景进行必要性论证与风险评估时可能面临实质性障碍。

根据《负面清单》，电控单元等售后数据也属于重要数据，具体包括电控单元信息、固件配置信息、重编程相关数据、诊断仪数据、车辆钥匙相关数据等。同样是售后场景，《中国（上海）自由贸易试验区临港新片区》发布的《智能网联汽车领域数据跨境场景化一般数据清单（试行）》将售后场景的车辆信息、故障状态数据、诊断数据、售后订单数据、售后配件数据、售后跟踪数据作为一般数据进行管理。因此，数据处理者需要个案分析以判断售后场景是否存在部分字段不属于《负面清单》重要数据的范畴。

与此同时，《负面清单》也针对在线升级数据的认定作出了豁免，规定已在工信部备案，并通过相

关安全技术措施处理，可确保升级包数据不被篡改的情形除外。

7. 可能被利用实施对车联网关键设备、系统组件供应链的破坏，以发起高持续威胁等网络攻击相关的数据；可一定程度反映交通、运输等行业性关键信息基础设施网络安全保护情况，可被利用从而对车联网关键信息基础设施实施网络攻击的数据；涉及车联网信息服务的关键信息基础设施相关数据

这类重要数据关注对汽车行业关键设备、供应链、以及关键信息基础设施的保护，其识别标准与《GB/T 43697-2024 数据安全 数据分类分级规则》附录 G “重要数据识别指南”列举的考虑因素基本一致。

（二）个人信息出境

针对自贸区内汽车行业的个人信息出境，《负面清单》规定的需通过安全评估、标准合同备案、个人信息保护认证的数量门槛均与《促进和规范数据跨境流动规定》（“《数据出境新规》”）一致，并且明确规定，属于《数据出境新规》第三条、第四条、第五条第一款第一项至第三项、第六条规定的情形的，不计入累计数量。

在敏感个人信息认定方面，《负面清单》基本采纳了《若干规定》对汽车行业敏感个人信息的定义，并额外明确身份证号、行驶证号、驾驶证档案编号属于敏感个人信息。

值得注意的是，《若干规定》规定“涉及个人信息主体超过 10 万人的个人信息”属于重要数据，但《负面清单》并未直接将这一类数据认定为重要数据。换言之，若拟出境个人信息不涉及关键车联网信息服务数据或其他类型的重要数据，汽车数据处理者不会仅因为拟出境个人信息数量超过 10 万人而需申报安全评估。

（三）小结

自贸区内的汽车数据处理者在识别重要数据过程中可能首先面临判断准据法的难题，因为《负面清单》规定的重要数据识别标准与《若干规定》并不完全一致。虽然《管理办法》第 7 条第 2 款规定，“行业主管部门已公开发布或已在行业内部发布本行业、本领域数据分类分级标准规范的，优先按照其规定识别重要数据；行业主管部门未明确判定标准的，按照《中国（北京）自由贸易试验区数据分类分级参考规则》识别重要数据”。但《负面清单》规定的重要数据识别标准范围更广、颗粒度更细。我们合理预计，自贸区内的汽车数据处理者若希望通过《负面清单》开展数据出境活动，可能仍需要优先参考《负面清单》的规定进行重要数据识别。

针对自贸区外的汽车数据处理者，现阶段仍然优先适用《若干规定》开展重要数据识别工作，定期完成年度汽车数据安全情况报送与重要数据风险评估。

不可否认的是，相较于《若干规定》，《负面清单》对重要数据的识别标准进行了更为精确的描述，可以为汽车数据处理者开展重要数据识别给予更明确的指导。因此，不排除未来行业主管部门以《负面清单》为基础，根据其试行效果发布全国汽车行业重要数据识别目录的可能性。

三、零售与现代服务业

根据《负面清单》，在零售与现代服务业场景下，3 类个人信息需要通过安全评估开展数据出境，3 类个人信息需要通过标准合同备案、个人信息保护认证出境。

（一）重要数据出境

《负面清单》中未针对零售与现代服务业额外认定重要数据类别，因此目前该行业领域中的重要数据识别规则应适用通用规则（例如《数据分类分级参考规则》所明确的重要数据统一识别参考规则），并且当与其他行业存在交叉时需考虑其他行业的重要数据目录。同时，后续相关行业主管机构也可能发布重要数据目录认定该行业的重要数据类别。

（二）个人信息出境

1. 非敏感个人信息出境

《负面清单》规定在会员管理场景下，若自当年 1 月 1 日起累计向境外提供 500 万人以上的个人消费者会员个人信息（不含敏感个人信息），则需要开展安全评估；若提供 50 万人以上且不满 500 万人的个人消费者会员个人信息（不含敏感个人信息），则需要开展标准合同备案或个人信息保护认证。

相比《数据出境新规》，《负面清单》将需要开展安全评估的门槛由 100 万提升至 500 万，并将需要开展标准合同备案或个人信息保护认证的门槛由 10 万提升至 50 万，放宽了会员场景下的个人信息出境限制。

此外，并非会员场景下的所有个人信息出境均可以适用上述 500 万/50 万的门槛。《负面清单》并未对会员场景下的个人信息进行穷尽列举，因此其列举之外的个人信息类型也可能落入《负面清单》的适用范畴，但对于部分《负面清单》中明确限缩适用个人信息范围的情形，例如“地址（含邮编，**仅限**消费者选择跨境物流或上门售后服务的情形）”、“会员爱好偏好（**仅限**产品类型、编号数字、偏好语言、积分兑换方式）”，若出境的个人信息在该等“仅限”范围之外（例如出境会员偏好的生日祝福形式），仍应当适用《数据出境新规》的 100 万/10 万门槛。

2. 敏感个人信息出境

《负面清单》规定在会员管理场景下，若自当年 1 月 1 日起累计向境外提供 100 万人以上的个人消费者会员敏感个人信息则需要开展安全评估，若提供 10 万人以上且不满 100 万人的个人消费者会员敏感个人信息，则需要开展标准合同备案或个人信息保护认证。相较《数据出境新规》所规定的 1 万敏感个人信息（安全评估）和 0-1 万敏感个人信息（标准合同备案/个人信息保护认证）的门槛，《负面清单》显著放宽了相关限制。

需要注意的是，《负面清单》所定义的敏感个人信息类别相比 GB/T 35273-2020《信息安全技术 个人信息安全规范》（“《安全规范》”）、《信息安全技术 敏感个人信息处理安全要求（征求意见稿）》（“《安全要求》”）、《网络安全标准实践指南 — 敏感个人信息识别指南（征求意见稿）》（“《识别指南》”）有所扩宽。具体请见如下表格：

《负面清单》所定义的敏感个人信息	与《安全规范》、《安全要求》、《识别指南》的区别
个人上网记录（活动预订记录、软件列表等）	<ul style="list-style-type: none"> ■ 《安全规范》：个人上网记录中属于敏感个人信息的是网页浏览记录；个人常用设备信息中软件列表信息不属于敏感个人信息； ■ 《识别指南》：所列举的敏感个人信息不包括个人上网记录； ■ 《安全要求》：个人上网记录相关数据中属于敏感个人信息的是网页浏览记录。

《负面清单》所定义的敏感个人信息	与《安全规范》、《安全要求》、《识别指南》的区别
	因此，《负面清单》额外将活动预订记录、软件列表等除了网页浏览记录之外其他的个人上网记录纳入敏感个人信息范畴。
常用设备信息（仅 MAC 地址和设备序列号）	<ul style="list-style-type: none"> ■ 《安全规范》、《识别指南》、《安全要求》：个人常用设备信息通常不属于敏感个人信息。 因此，《负面清单》额外将个人常用设备信息中的 MAC 地址和设备序列号纳入敏感个人信息范畴。
会员登录验证信息	<ul style="list-style-type: none"> ■ 《安全规范》：个人财产信息中的鉴别信息（口令）属于敏感个人信息； ■ 《识别指南》：金融账户的账号及密码信息属于敏感个人信息； ■ 《安全要求》：金融账户的账号及密码信息属于敏感个人信息； 因此，《负面清单》额外将除金融/财产相关的账户之外的其他会员账户的登录验证信息纳入敏感个人信息范畴。

（三）小结

根据此前的《数据出境新规》，为订立、履行个人消费者作为一方当事人的合同而提供商品或服务（如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等）而确需向境外提供个人信息的情形已豁免安全评估、标准合同备案和个人信息保护认证，但对于基于上述跨境交易和服务而衍生的会员服务而言，虽然其可以为消费者提供更多福利，其通常较难被上述豁免情形包含（例如会员等级、会员积分、会员偏好等服务均较难属于为提供商品或服务所必需），因此企业仍需就会员场景履行相关出境义务。

在此背景下，《负面清单》为会员场景提供了更宽松的出境限制。受《负面清单》影响的企业主要是面向个人消费者建立会员制度并提供商品交易或服务的零售、住宿、餐饮、软件和信息技术服务、互联网信息服务等企业。对于其他企业或除会员外的其他场景，仍应按照此前《数据出境新规》等规定履行数据出境合规义务。

四、人工智能训练数据

根据《负面清单》，3 类重要数据及 4 类个人信息需要通过安全评估开展数据出境；2 类个人信息需要通过标准合同备案、个人信息保护认证出境。

（一）重要数据出境

根据《负面清单》，如人工智能模型训练、算法开发、产品测试等场景涉及的人工智能训练数据符合如下特征，将被认定为重要数据：

1. 在研发设计过程中，收集和产生的与行业竞争力相关的高价值敏感数据。因此，如北京自贸试验区内数据处理者在 AI 产品出海等业务中，涉及向境外传输可能影响行业竞争力的人工智能算法源代码、关键组件数据、控制程序、基础模型数据、数据挖掘分析数据、测试数据等数据，则需要事先申报数据出境安全评估。

2. 内容中涉及一旦遭到篡改、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、公共健康和安全的数据。因此，如北京自贸试验区内数据处理者拟向境外提供人工智能训练数据（包括音频、图像及文本），需要结合所涉领域、群体、区域、精度及规模等考虑因素，评估泄露或不当利用可能对国家安全、经济运行、社会稳定、公共健康和安全产生的危害后果。
3. 纳入出口管制或技术出口管理事项的数据。根据国家出口管制清单以及《中国禁止出口限制出口技术目录》，可能涉及人工智能的物项包括但不限于具备特定性能（机器翻译系统得分>4.5分，满分为5分）的中译外翻译技术、专门用于汉语及少数民族语言的语音合成技术/人工智能交互界面技术/智能阅卷技术、水下自治或半自治机器人制造技术及控制技术、专门设计用于航空/航天/船舶/火车的有源噪声控制的系统设计技术和算法软件等。如人工智能训练数据落入前述事项范围，须根据有关规定进行数据出境安全评估以及履行出口许可申请义务。

（二）个人信息出境

在个人信息出境方面，《负面清单》针对拟出境训练数据模态、出境场景设置了差异化的数量门槛：

对于在模型训练、算法开发、产品测试场景中的人工智能训练数据（仅限音频、图像、文本模态）出境，需通过安全评估、标准合同备案、个人信息保护认证的数量门槛相较于《数据出境新规》有所放松，具体如下图所示。其中，音频数据、图片数据、文本数据均包括相应模态的内容数据、标签数据等。

训练数据模态	安全评估	标准合同备案、个人信息保护认证
音频数据	自当年1月1日起累计向境外提供内容中涉及 5万人以上敏感个人信息 。	自当年1月1日起累计向境外提供内容中涉及 1万人以上且不满5万人敏感个人信息 。
图片数据		
文本数据	自当年1月1日起累计向境外提供内容中涉及 10万人以上敏感个人信息 。	自当年1月1日起累计向境外提供内容中涉及 1万人以上且不满10万人敏感个人信息 。

值得注意的是，除履行跨境合规机制外，前述音频数据、图片数据、文本数据出境还需按照《生成式人工智能服务安全基本要求》中的有关要求进行处理，包括但不限于：

- 确保语料来源可追溯，按要求保存不同类型语料的有关授权文件或记录；
- 对于包含个人信息/敏感个人信息的语料，应依法取得个人同意/单独同意，或者符合法律、行政法规规定的其他情形（例如已经合法公开的个人信息）。

对于其余出境场景或其他模态训练数据出境，需通过安全评估、标准合同备案、个人信息保护认证的数量门槛均与《数据出境新规》一致。

（三）小结

如前所述，《负面清单》进一步明确了北京自贸试验区内人工智能领域“重要数据”的认定规则，同时适当放宽了模型训练、算法开发、产品测试三大场景中特定模态训练数据出境的个人信息跨境合规机制数量门槛。

值得注意的是，《负面清单》明确“在研发设计过程中收集和产生的与行业竞争力相关的高价值敏感数据”也构成重要数据，因此，北京自贸试验区内具有行业竞争力的AI企业在AI产品出海时，如

将有关模型部署于境外，则也可能构成重要数据出境从而需要履行安全评估义务。

此外，实践中数据处理者直接向境外主体提供训练数据集、在境外服务器上训练人工智能模型、引入境外合作方开展数据标注或预处理、与境外主体合作开发优化或测试模型、或调用境外闭源大模型接口训练模型，均可能构成人工智能训练数据出境。因此，北京自贸试验区内的数据处理者在开展前述活动之前，需要依据《负面清单》评估通过安全评估、标准合同备案、个人信息保护认证的必要性，并采取相应的数据跨境合规措施。

五、结语

整体而言，我们理解《负面清单》针对重要数据出境的规定较为严格，与我国对于重要数据一贯的审慎监管口径相一致，为数据有序自由流动守牢安全底线。同时，《负面清单》在北京自贸试验区内适当放宽了特定场景下的个人信息跨境合规机制数量门槛，减轻了试验区内数据处理者在相应场景下的数据跨境合规负担。

值得注意的是，《负面清单》在特定行业的重要数据、敏感个人信息认定等方面有所创新，例如其中 AI 训练数据中重要数据识别的细化规定可能导致诸多 AI 出海企业需要履行数据出境安全评估义务。考虑到各行业、地区的重要数据目录制定工作仍在推进过程中，各自贸区的《负面清单》也可能作为重要参考。对此，建议试验区内外的企业持续关注有关规定的落实情况以及其他后续规定，及时调整数据处理和跨境传输策略，以确保有关数据跨境活动符合最新的法律合规要求。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123

Email: kevin.duan@hankunlaw.com