（2025 年 6 月）

目录

一、法规速递

《网信部门行政处罚裁量权基准适用规定（征求意见稿）》

发文机关：国家互联网信息办公室

发文时间：2025.05.30

生效时间：待定

第一条 为了规范网信部门行政处罚行为，保护公民、法人和其他组织的合法权益，根据《中华人民共和国行政处罚法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《网信部门行政执法程序规定》等法律、法规、规章和国家有关规定，结合网信工作实际，制定本规定。

第二条 网信部门依据行政处罚裁量权基准行使行政处罚裁量权，适用本规定。法律、法规、规章另有规定的，从其规定。

第三条 本规定所称行政处罚裁量权基准，是指网信部门在实施行政处罚时，按照裁量涉及的违法行为的事实、性质、情节、社会危害程度、当事人主观过错等因素，对法律、法规、规章中的原则性规定或者具有一定弹性的执法权限、裁量幅度等内容进行细化量化而形成的具体执法尺度和标准。

第四条 网信部门适用行政处罚裁量权基准，应当遵循法制统一、公平公正、过罚相当、宽严相济、处罚与教育相结合等原则。

第五条 网信部门行政处罚裁量权基准划分为不予处罚、减轻处罚、从轻处罚、一般处

罚、从重处罚等裁量阶次。

不予处罚是指因法定原因对实施违法行为本应给予行政处罚的当事人不再给予行政处罚。

减轻处罚是指减少并处法律、法规、规章规定的行政处罚种类或者低于最低限度的处罚幅度，对当事人实施行政处罚。

从轻处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用较轻、较少的种类或者较低的幅度，对当事人实施行政处罚。

一般处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用适中的种类或者幅度，对当事人实施行政处罚。

从重处罚是指在法律、法规、规章规定的行政处罚种类和处罚幅度内，适用较重、较多的种类或者较高的幅度，对当事人实施行政处罚。

第六条 有下列情形之一的，应当不予处罚：

（一）违法行为轻微并及时改正，没有造成危害后果的；

（二）当事人有证据足以证明没有主观过错的，法律、法规另有规定的，从其规定；

（三）法律、法规规定的其他情形。

初次违法且危害后果轻微并及时改正的，可以不予处罚。

依法不予处罚的，网信部门可以根据情节采取相应的行政监管措施，并应当对当事人进行教育。

第七条 有下列情形之一的，应当从轻或者减轻处罚：

（一）主动消除或者减轻违法行为危害后果的；

（二）受他人胁迫或者诱骗实施违法行为的；

（三）主动供述网信部门尚未掌握的违法行为的；

（四）配合网信部门查处违法行为有立功表现的；

（五）法律、法规、规章规定的其他情形。

第八条 有下列情形之一的，应当从重处罚：

（一）违法行为严重危害网络信息内容安全、网络运行安全、网络数据安全的，违法处理个人信息或者处理个人信息未履行个人信息保护义务情节严重的；

（二）因同种违法行为一年内受到网信部门两次以上行政处罚的；

（三）教唆、胁迫、诱骗他人实施违法行为的；

（四）拒不配合、阻碍、以暴力威胁网信部门执法人员依法执行公务的；

（五）隐匿、毁损、伪造、篡改有关证据的；

（六）对证人、举报人、网信部门工作人员进行打击报复的；

（七）违法行为引起群众强烈反映，引发群体性事件或者造成其他不良社会影响的；

（八）违反未成年人保护相关规定情节严重的；

（九）性质恶劣、情节严重、社会危害性较大的其他情形。

第九条 违法行为不具有不予处罚、减轻处罚、从轻处罚或者从重处罚情形的，应当给予一般处罚，法律、法规、规章另有规定的除外。

第十条 当事人同时存在减轻处罚、从轻处罚或者从重处罚等情形的，应当根据案件具体情况综合考量进行处罚。

第十一条 罚款有一定幅度的，在相应的幅度范围内分为从轻处罚、一般处罚、从重处罚。

从轻处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间低于 30%的数额；一般处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间的 30%至 70%的数额；从重处罚的罚款数额应当在法定最低限至法定最高限幅度或者倍数区间超过 70%的数额。

在确定具体处罚数额时，综合考量违法行为的性质、情节和本地区经济社会发展状况等因素，结合执法实践和执法案例，可以以前款规定的百分比为基础上下浮动十个百分点。

第十二条 依法单独处警告、通报批评、没收违法所得的，仅适用不予处罚、一般处罚两种裁量阶次。

第十三条 单位实施违法行为的，对直接负责的主管人员和其他直接责任人员的处罚，应当综合考量相关责任人员的岗位职责、任职时间、履职行为与违法行为的关联性、主观过错程度、主次责任，以及是否对违法行为采取整改措施等因素，参照对单位行政处罚裁量阶次，确定适当的行政处罚。

第十四条 网信部门适用行政处罚裁量权基准，判断违法行为性质、情节以及社会危害程度等，应当综合考量以下因素：

（一）违法行为的具体方法或者手段，当事人实施违法行为的主观过错程度；

（二）违法行为的持续时间、发生次数，违法行为造成的社会影响、危害后果；

（三）违法行为的危害对象及其数量；

（四）当事人本年度内的处罚情况；

（五）当事人获取的违法所得；

（六）当事人的生产经营类型规模、经营情况及其影响力；

（七）当事人改正违法行为的主观态度、配合检查的情况、所采取的整改措施及效果；

（八）法律、法规、规章规定的其他因素。

第十五条 对当事人的同一个违法行为，不得给予两次以上罚款的行政处罚。同一个违法行为违反多个法律规范应当给予罚款处罚的，按照罚款数额高的规定处罚。有两个以上应当给予行政处罚违法行为的，应当分别裁量，合并处罚。

第十六条 市（地、州）级以上网信部门可以结合工作实际制定本行政区域内的行政处罚裁量权基准。对同一行政执法事项，上级网信部门已经制定行政处罚裁量权基准的，

下级网信部门原则上应当直接适用；如下级网信部门不能直接适用，可以结合本地区经济社会发展状况，在法律、法规、规章规定的行政处罚裁量权范围内进行合理细化量化，但不能超出上级网信部门划定的阶次或者幅度。下级网信部门制定的行政处罚裁量权基准与上级网信部门制定的行政处罚裁量权基准冲突的，应当适用上级网信部门制定的行政处罚裁量权基准。

第十七条 网信部门作出行政处罚决定前，应当告知当事人拟作出的行政处罚的内容及事实、理由、依据，并在行政处罚决定书中对行政裁量权基准的适用情况予以明确。

第十八条 网信部门实施行政处罚，适用本部门制定的行政处罚裁量权基准可能出现明显不当、显失公平，或者行政处罚裁量权基准适用的客观情况发生变化的，经本部门主要负责人批准或者集体讨论通过后可以调整适用，批准材料或者集体讨论记录应当列入处罚案卷归档保存。

适用上级网信部门制定的行政处罚裁量权基准可能出现前款情形的，报请上级网信部门批准后，可以调整适用。

第十九条 上级网信部门应当通过行政执法情况检查、行政执法案卷评查等方式，对下级网信部门行使行政处罚裁量权工作进行监督。

因不规范适用行政处罚裁量权基准造成严重后果的，应当依规依纪依法严格追究有关人员责任。

第二十条 本规定自 年 月 日起施行。

《汽车数据出境安全指引（2025 版）（征求意见稿）》

发文机关：工业和信息化部,国家互联网信息办公室,国家发展和改革委员会,国家数据局,公安部,自然资源部,交通运输部,国家市场监督管理总局

发文时间：2025.06.13

生效时间：待定

为贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规，引导规范汽车数据处理者高效便利安全开展汽车数据出境活动，提升汽车数据出境流动便利化水平，制定本指引。

一、总则

（一）适用范围

汽车数据处理者按照本指引开展数据出境活动。本指引所称汽车数据是指汽车设计、生产、销售、使用、运维等过程中涉及的个人信息和重要数据。汽车数据处理者是指开展汽车数据处理活动的组织，包括汽车制造商、零部件和软件供应商、电信运营企业、自动驾驶服务商、平台运营企业、经销商、维修机构以及出行服务企业等。

（二）数据出境行为

汽车数据处理者向中华人民共和国境外[1]提供汽车数据，符合以下情形之一的属于数据出境行为：

(1)汽车数据处理者将在中华人民共和国境内[2]运营中收集和产生的汽车数据传输至境外；

(2)汽车数据处理者收集和产生的汽车数据存储在境内，境外的机构、组织或者个人查

[1] 以下简称境外

[2] 以下简称境内

询、调取、下载、导出；

(3)符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他数据处理活动。

（三）数据出境路径

1．汽车数据处理者向境外提供汽车数据，符合以下情形之一的，应当申报数据出境安全评估：

(1)向境外提供重要数据；

(2)自当年 1 月 1 日起累计向境外提供 100 万人以上[3]个人信息（不含敏感个人信息）；

(3)自当年 1 月 1 日起累计向境外提供 1 万人以上敏感个人信息；

(4)关键信息基础设施运营者向境外提供个人信息；

(5)国家有关规定明确的其他需要申报数据出境安全评估的情形。

2．汽车数据处理者（关键信息基础设施运营者除外）向境外提供个人信息，符合以下情形之一的，可在与境外接收方订立个人信息出境标准合同、通过个人信息保护认证两种方式中任选其一：

(1)自当年 1 月 1 日起，累计向境外提供 10 万人以上、不满[4]100 万人个人信息（不含敏感个人信息）的；

(2)自当年 1 月 1 日起，累计向境外提供不满 1 万人敏感个人信息的。

3．有下列情形之一的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：

(1)在境外收集和产生的汽车数据传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的；

(2)为订立、履行个人作为一方当事人的合同，如跨境购车、跨境寄递、跨境支付、跨境注册账户等，确需向境外提供个人信息（不含重要数据）的；

(3)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跨境人力资源管理，确需向境外提供员工个人信息（不含重要数据）的；

(4)紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息（不含重

[3] 本指引所指“以上”均含本数。

[4] 本指引所称“不满”，均不包含本数。

要数据）的；

(5)关键信息基础设施运营者以外的汽车数据处理者自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息（不含敏感个人信息和重要数据）的；

(6)自由贸易试验区内登记注册的汽车数据处理者符合自由贸易试验区有关要求，向境外提供负面清单外的数据的；

(7)因修补安全漏洞需要，汽车数据处理者按照《网络产品安全漏洞管理规定》有关要求，已向工业和信息化部报告的安全漏洞数据；

(8)因处置安全事件需要，汽车数据处理者按照行业网络安全、数据安全事件相关应急预案[5]，已向工业和信息化部及相关行业监管部门报告的汽车产品、车联网平台及相关系统的安全事件数据；

(9)因消除汽车产品缺陷、实施召回需要，汽车数据处理者按照《缺陷汽车产品召回管理条例》已向国家市场监督管理总局备案的 OTA 升级软件包对应的源代码。

二、重要数据出境

汽车数据处理者向境外提供以下业务场景所列重要数据[6]的，应当申报数据出境安全评估。

（一）研发设计场景

1．产品研发

汽车数据处理者在整合全球研发资源、产品协同设计开发过程中，收集和产生的物料清单、研发设计文档、产品技术开发源代码数据。

序号	数据类别	数据项	数据项说明	判定规则
1	物料清单	设计物料清单	设计阶段所需原材料、零部件或组件清单文件，包括物	被列入国家重大专项、国家重点研发计划的。

[5] 网络安全事件依据《公共互联网网络安全突发事件应急预案》，数据安全事件依据《工业和信息化领域数据安全事件应急预案（试行）》。

[6] 位置轨迹、自动驾驶地图数据、构图类数据等含有空间位置坐标的地理信息数据均应为采用国家认定的地理信息保密处理技术完成处理后的数据。

			料规格、数量、层级关系等	
2	研发设计文档	研发设计文档	技术开发过程中的设计模型、图纸、方案、技术文档、测试报告等	
3	产品技术开发源代码	产品技术开发源代码	产品及技术开发源代码	

2．产品测试

汽车数据处理者开展汽车产品仿真、场地和实际道路测试过程中，收集和产生的标注场景数据、仿真场景数据、测试场景数据。

序号	数据类别	数据项	数据项说明	判断规则
1	标注场景数据	图片标注	产品测试过程中涉及的图片文件	符合以下任意一项条件的： 1．涉及或经汇聚、分析后能推算出军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的； 2．经汇聚、分析后能够推算出涉密、敏感
2		点云标注	产品测试过程中涉及的点云文件	
3		多模态标注	产品测试过程中涉及的多模态数据文件	
4		路网仿真文件	产品测试过程中涉及的路网仿真文件，包括仿真道路的	地理信息数据[7]的； 3．涉及道路的真实车辆流量、人员流量、物流等反映地级及以上行政区经济运行情况的数据，且累计时

[7] 按照《测绘地理信息管理工作国家秘密范围的规定》识别涉密地理信息数据。

			拓扑结构、属性等	间大于等于 30 天； 4．涉及或经汇聚、分析后能推算出涉及社会公共安全行政执法活动的； 5．车外真实人脸边界框最小边长为 32 像素以上的； 6．车外真实汽车号牌边界框最小边长为 16 像素以上的； 7．涉及在境内运行的 10 万台以上车辆收集的。
5		环境仿真文件	产品测试过程中涉及的环境仿真文件，包括道路基础设施模拟、车道线模拟、道路标识模拟等	
6		交通流量仿真文件	产品测试过程中涉及的交通流量仿真文件	
7		仿真合成文件	品测试过程中通过算法或模型生成的用于模拟真实数据的仿真文件	
8		回灌仿真文件	产品测试过程中重新注入目标系统或模型以验证其功能、性能的仿真文件	
9	测试场景数据	测试场景文件	产品测试过程中涉及的测试场景文件，包	

			括事故场景、危险场景、边缘场景等	

（二）生产制造场景

汽车数据处理者在汽车产品生产制造过程中，收集和产生的物料清单、生产控制程序源代码。

序号	数据类别	数据项	数据项说明	判定规则
1	物料清单	工艺物料清单	汽车产品、零部件或组件的工艺物料清单	符合以下任意一项条件的： 1．被列入国家重大专项、国家重点研发计划的； 2．符合《中国禁止出口限制出口技术目录》中相关技术控制要点的。
2	生产控制程序源代码	数控机床控制程序源代码	用于生产汽车产品、零部件或组件的数控机床控制程序源代码	
3		工业机器人控制程序源代码	用于生产汽车产品、零部件或组件的工业机器人控制程序源代码	

（三）驾驶自动化场景

汽车数据处理者在组合驾驶辅助或自动驾驶功能开发、部署、应用等过程中，收集和产生的算法、训练数据、特征数据。

序号	数据类别	数据项	数据项说明	判定规则
1	驾驶自动化算法	驾驶自动化算法文件	组合驾驶辅助或自动驾驶算法原	符合以下任意一项条件的： 1．被列入国家重大专项、国家重点研发计划的；

			理、流程等文件	2．涉及车联网网络与数据安全、驾驶自动化功能相关成果获得省部级及以上奖励的； 3．可能对国家科技安全、行业竞争力等产生影响的。
2		驾驶自动化算法源代码	基于人工智能技术的未开源的组合驾驶辅助或自动驾驶算法源代码	
3		驾驶自动化算法参数	组合驾驶辅助或自动驾驶算法模型训练参数和权重系数	
4	驾驶自动化算法训练数据	训练影像及消息集	用于训练、验证组合驾驶辅助或自动驾驶算法模型的初始数据集，包括文本、视频、图像、音频等	符合以下任意一项条件的： 1．被列入国家重大专项、国家重点研发计划的； 2．涉及车联网网络与数据安全、驾驶自动化功能相关成果获得省部级及以上奖励的； 3．涉及或经汇聚、分析后能推算出军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的； 4．经汇聚、分析后能够推算出涉密、敏感地理信息数据的； 5．涉及道路的真实车辆流量、人员流量、物流等反映地级及以上行政区经济运行情况的数据，且累计时间大于等于 30 天；

				6．涉及或经汇聚、分析后能推算出涉及社会公共安全行政执法活动的； 7. 涉及在境内运行的 10 万台以上车辆收集的； 8. 涉及采集真实环境中 5000 万公里以上或 2000 小时以上的原始图片或原始影像的； 9．涉及 1000 万张以上原始图片的； 10．涉及 100 万个以上原始影像的。
5		驾驶员决策数据集	用于训练、验证组合驾驶辅助或自动驾驶算法模型的驾驶员决策数据集，包括档位信息、加速踏板开度、刹车踏板开度、方向盘转向角等	与车外实景影像、雷达数据融合关联后，符合以下任意一项条件的： 1．涉及或经汇聚、分析后能推算出军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的； 2．经汇聚、分析后能够推算出涉密、敏感地理信息数据的； 3．涉及道路的真实车辆流量、人员流量、物流等反映地级及以上行政区经济运行情况的数据，且累计时间大于等于 30 天； 4．涉及或经汇聚、分析后能推算出涉及社会公共安全行政执法活动的； 5. 涉及在境内运行的 10 万台以上车辆收集的。
6		组合驾驶辅助或自动驾驶系	用于训练、验证组合驾驶辅助或自动驾驶系统	

		统决策或预测规划数据集	决策或预测规划数据集，包括档位信息、加速踏板开度、刹车踏板开度、转向角、转向力矩等	
7		运行数据集	用于训练、验证组合驾驶辅助或自动驾驶算法模型训练的车辆运行数据集，包括车辆的经纬度、海拔高程、航向角、横滚角、俯仰角、速度、侧倾角速度、横摆角速度、横纵向加速度等	
8	驾驶自动化算	图像特征数据	用于组合驾驶辅助或自	符合以下任意一项条件的： 1．被列入国家重大专项、国家重点研发

	法特征数据		动驾驶算法的图像特征数据，包括原始图片、影像数据等经过特征提取出的道路标志、标线、车辆、行人目标物等	计划的； 2．涉及车联网网络与数据安全、驾驶自动化功能相关成果获得省部级及以上奖励的； 3．涉及或经汇聚、分析后能推算出军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的； 4．经汇聚、分析后能够推算出涉密、敏感地理信息数据的； 5．涉及道路的真实车辆流量、人员流量、物流等反映地级及以上行政区经济运行情况的数据，且累计时间大于等于 30 天； 6．涉及或经汇聚、分析后能推算出涉及社会公共安全行政执法活动的； 7. 涉及在境内运行的 10 万台以上车辆收集的； 8. 涉及采集真实环境中 5000 万公里以上或 2000 小时以上的原始图片或原始影像的； 9．涉及 1000 万张以上原始图片的； 10．涉及 100 万个以上原始影像的。
9		点云特征数据	用于组合驾驶辅助或自动驾驶算法的点云特征数据，包括原始点云数	符合以下任意一项条件的： 1．被列入国家重大专项、国家重点研发计划的； 2．涉及车联网网络与数据安全、驾驶自动化功能相关成果获得省部级及以上奖励的；

			据经过特征提取出的物体的三维空间位置、形状等	3．涉及或经汇聚、分析后能推算出军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的； 4．经汇聚、分析后能够推算出涉密、敏感地理信息数据的； 5．涉及道路的真实车辆流量、人员流量、物流等反映地级及以上行政区经济运行情况的数据，且累计时间大于等于 30 天； 6．涉及或经汇聚、分析后能推算出涉及社会公共安全行政执法活动的； 7. 涉及在境内运行的 10 万台以上车辆收集的； 8. 涉及采集真实环境中 5000 万公里以上或 2000 小时以上的原始图片或原始影像的。

（四）软件升级服务场景

汽车数据处理者升级汽车动力系统、底盘系统、安全驾驶功能的软件包对应的源代码。

序号	数据类别	数据项	数据项说明	判定规则
1	软件升级数据	安全驾驶功能升级软件程序源代码	安全驾驶功能升级软件包对应的源代码	同时符合以下条件的： 1．涉及升级境内运行车辆的； 2. 涉及车辆远程控制功能的，不包含通过近场通信方式实现的控制功能； 3．涉及车辆启动行驶、动力丢失、紧急制动、巡航控制、车道保持功能。

（五）联网运行场景

1．车辆数据

汽车数据处理者在车辆联网运行过程中，收集和产生的车辆识别码、车联网卡识别码、车辆密钥、车辆数字证书、控制指令。

序号	数据类别	数据项	数据项说明	判定规则
1	车辆识别码	车辆识别码（VIN)	原始 VIN、去标识化后且可还原的 VIN	自当年 1 月 1 日起向境外提供与其他出境信息结合可识别累计 100 万人以上个人身份的。
2	车联网卡识别码	车联网卡识别码	国际移动设备识别码（IMEI）、国际移动用户识别号（IMSI）、集成电路卡识别码(ICCID)	
3	车辆密钥	对称密钥	车云通信过程中所涉及的对称密钥	涉及在境内运行的 10 万台以上车辆的安全启动、诊断、更新、通信过程中的密钥。
4		非对称私钥	车云通信过程中所涉及的非对称私钥	
5	车辆数字证书	数字证书	车云通信过程中所涉及的根证书、中间证书、注册证书、用户证书	涉及在境内运行的 10 万台以上车辆的诊断、更新、通信过程中的证书。
6	控制指令	车辆控制指令	用于控制车门开关、车辆启动、转向、加速、制动、和电池管理、远程泊车的相关指令	涉及在境内运行车辆的。

2．车路感知

汽车数据处理者在车辆及路侧设备联网运行过程中，收集和产生的车外实景影像、雷达

数据、位置轨迹数据、惯性导航数据、自动驾驶地图数据、构图类数据。

序号	数据类别	数据项	数据项说明	判定规则
1	车外实景影像	摄像头拍摄图片	车端或路侧摄像头收集的图片	符合以下任意一项条件的： 1. 涉及或经汇聚、分析后能推算出军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的； 2. 经汇聚、分析后能够推算出涉密、敏感地理信息数据的； 3. 涉及道路的真实车辆流量、人员流量、物流等反映地级及以上行政区经济运行情况的数据，且累计时间大于等于 30 天； 4. 涉及或经汇聚、分析后能推算出涉及社会公共安全行政执法活动的； 5. 车外真实人脸边界框最小边长为 32 像素以上的； 6. 车外真实汽车号牌边界框最小边长为 16 像素以上的； 7. 涉及在境内运行的 10 万台以上车辆收集的。
2		摄像头拍摄视频	车端或路侧摄像头收集的视频影像	
3	雷达数据	点云数据	车端或路侧雷达收集的点云数据	
4		结构化数据	基于车端或路侧雷达收集的点云数据分析提取的目标级信息，包括目标识别数据、位置数据、运动状态数据、属性数据	
5	位置轨迹数据	时空定位数据	全球导航卫星系统（GNSS）速度、时间戳、载波、伪距以及收集的车辆经纬度数据	
6		车辆高	全球导航卫星	

		程	系统（GNSS）收集的车辆高程数据	
7	惯性导航数据	惯性导航数据	车辆在导航坐标系中的速度、偏航角和位置等数据	
8	自动驾驶地图数据	引导交通参与者的数据集	引导交通参与者从出发到目的地的数据集	
9	构图类数据	坐标相关的矢量数据	坐标相关的矢量数据	

3．车路分析

汽车数据处理者在开展车路协同分析、构建车路协同系统过程中，收集和产生的融合计算数据。

序号	数据类别	数据项	数据项说明	判定规则
1	融合计算数据	人员流量	人员流量数据，包括路侧设备收集的数据进行汇聚分析后得到的用于反映人员流动情况的数据	符合以下任意一项条件的： 1．涉及或经汇聚、分析后能推算出军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的； 2．经汇聚、分析后能够推算出涉密、敏感地理信息数据的； 3．涉及或经汇聚、分析后能推算出涉及社会公共安全行政执法活动
2		车辆流量	车辆流量数据，包括路侧	

			设备收集的数据进行汇聚分析后得到的用于分析车辆运行情况的数据	的； 4．涉及道路的真实车辆流量、人员流量、物流等反映地级及以上行政区经济运行情况的数据，且累计时间大于等于 30 天。
3		目标物成像数据	目标物表面点三维坐标	
4		交通流指标数据	红绿灯排队时长、路口交通流量、绿灯时间、溢流事件	符合以下任意一项条件的： 1．涉及或经汇聚、分析后能推算出军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域； 2．涉及或经汇聚、分析后能推算出涉及社会公共安全行政执法活动的； 3．覆盖至少单个完整路口，时间跨度大于 1 个月。

4．车联网平台运营

汽车数据处理者在开展车联网平台建设、运行、维护过程中，收集和产生的网络规划数据、充电运行数据。

序号	数据类别	数据项	数据项说明	判定规则
1	网络规划数据	资产配置信息	车联网平台操作系统、数据库、应用等核心资产的配置信息，包括版本、ip 地址、服务	符合以下任意一项条件的： 1．涉及服务境内运行车辆数量达 100 万台以上的车联网平台的； 2．同时满足提供在线升级服

			端口、登录方式	务，境内运行车辆数量达 50 万台以上，升级内容涉及汽车动力系统、底盘系统、安全驾驶功能中的一种或多种的车联网平台的。
2		网络拓扑图	能够显示内网网络结构的车联网平台网络拓扑图文件，包含网络边界出口设备信息、网络区域划分以及内网 IP 地址	
3	充电运行数据	充电设施位置数据	充电桩、充电站的地理位置信息	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。
4		车辆充电状态监测数据	车辆充电功率、充电电流、充电电压、当前电池温度、电池健康状态	涉及在境内运行的 10 万台以上车辆收集的。
5		充电消费数据	充电账号、开始时间、结束时间、充电站点位置、充电量、充电费用等数据	自当年 1 月 1 日起累计向境外提供 100 万人以上的充电消费数据。

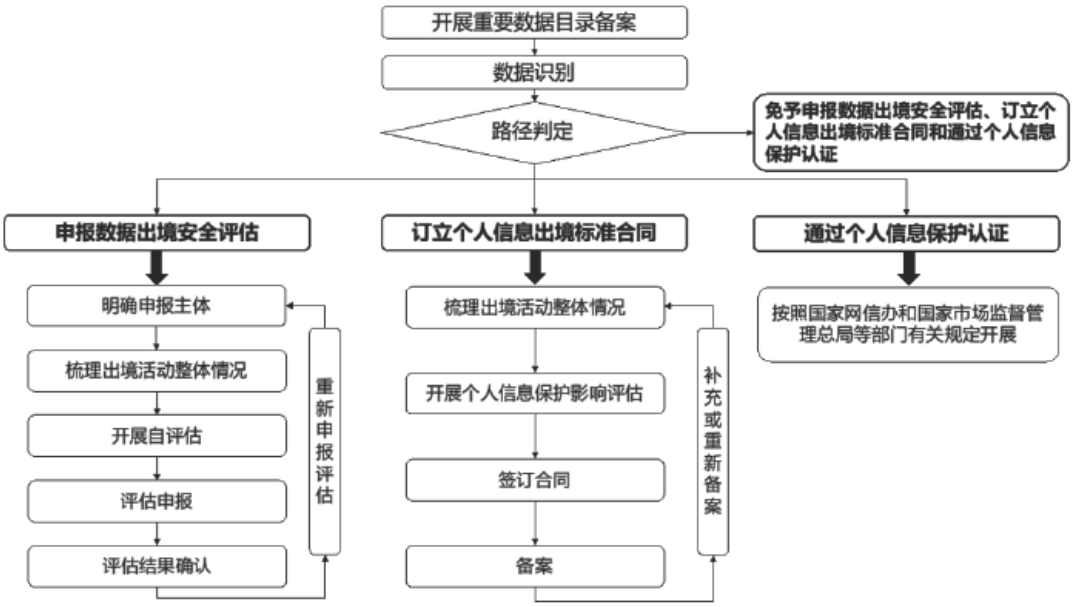
（六）其他情形

符合以下情形之一的汽车数据：

1．其他出境业务场景中符合上述判定规则的；

2．汽车数据处理者按照国家有关规定和行业标准规范识别、申报重要数据，工业和信息化部、国家网信办等相关部门公开或告知企业属于重要数据的。

三、数据出境实施流程数据出境实施流程图如下：



（一）数据识别

汽车数据处理者在重要数据目录备案基础上，按照本指引识别需申报出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的汽车数据。

对于向境外提供个人信息的，汽车数据处理者应当依法依规履行告知、取得个人单独同意、进行个人信息保护影响评估等义务。

（二）路径判定

根据本指引“一、总则（三）数据出境路径”判断和确定数据出境路径。符合本指引“一、总则（三）数据出境路径”第 3 项规定情形的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

（三）实施数据出境安全评估

汽车数据处理者实施数据出境安全评估应按照《数据出境安全评估办法》《促进和规范数据跨境流动规定》《数据出境安全评估申报指南（第二版）》规定申报评估。

1．明确申报主体

汽车数据处理者应通过境内法人主体申报数据出境安全评估；境内无法人主体的，应由境内分支机构申报；境内多家子公司如同属一家集团公司（母公司）且数据出境业务场景相似，可由集团公司（母公司）作为申报主体合并申报。

2．梳理出境活动整体情况

收集本企业及境外接收方等相关方材料，梳理出境活动整体情况，包括：

(1)汽车数据处理者基本情况，包括股权结构、实际控制人、境内外投资情况等；

(2)汽车数据处理者拟出境数据情况，包括：

a)数据出境场景涉及业务、数据资产等情况；

b)数据出境的目的、范围、方式；

c)出境数据项情况，并以列表形式呈现；

d)拟出境数据在境内存储的系统平台、数据中心（包含云服务）等情况，数据出境链路相关情况，计划出境后存储的系统平台、数据中心等；

e)数据出境后向境外其他接收方提供的情况；

f)涉及个人信息的，按照自然人（去重）统计当年的出境数量，预估未来 3 年的出境数量。

(3)汽车数据处理者安全保障能力情况，包括数据安全管理能力、技术能力、数据安全保障措施有效性证明、遵守数据和网络安全相关法律法规的情况；

(4)境外接收方情况，包括境外接收方基本情况，境外接收方处理数据的用途、方式，境外接收方履行责任义务的管理和技术措施、能力等；

(5)与境外接收方以法律文件形式约定出境数据情况，明确双方责任义务，具体内容包括：

a)数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；

b)数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；

c)对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；

d)境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化，以及发生其他不可抗力情形，导致难以保障数据安全时，应当采取的安全措施；

e)违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；

f)出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用时，妥善开

展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

(6)汽车数据处理者认为需要说明的其他情况。

3．开展自评估

(1)自评估事项

汽车数据处理者应结合数据出境活动整体情况和相关材料重点评估以下事项：

a)数据出境和境外接收方处理数据的目的、范围、方式等是否具有合法性、正当性、必要性；

b)出境数据的规模、范围、种类、敏感程度，数据出境是否会对国家安全、公共利益、个人或者组织合法权益带来风险；

c)境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；

d)数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

e)与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务；

f)其他可能影响数据出境安全的事项。

(2)发现问题并整改

汽车数据处理者在开展数据出境安全自评估过程中发现存在影响数据出境的风险和问题的，应及时整改，并记录相关情况。

(3)形成自评估结论

汽车数据处理者综合风险自评估情况和相应整改情况，对拟申报的数据出境活动作出客观的风险自评估结论，并充分说明理由。

(4)编制自评估报告

汽车数据处理者整理自评估工作情况、出境活动整体情况、出境活动的风险自评估情况及结论，编制形成数据出境风险自评估报告，并附相关证明材料。

4．评估申报

(1)准备申报材料

汽车数据处理者按照相关规定准备申报材料，包括：

a)统一社会信用代码证件影印件；

b)法定代表人身份证件影印件；

c)经办人身份证件影印件；

d)经办人授权委托书；

e)数据出境安全评估申报书；

f)与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件；

g)数据出境风险自评估报告；

h)其他相关证明材料。

汽车数据处理者需对所提交材料的真实性负责，提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。

(2)确定申报方式

关键信息基础设施运营者以外的汽车数据处理者申报数据出境安全评估一般适用线上申报，关键信息基础设施运营者或者其他不适合通过线上系统申报数据出境安全评估的，采取线下申报流程。

(3)评估材料提交

汽车数据处理者按国家有关规定，向网信部门申报数据出境安全评估，并按要求补充或修改材料。

5．评估结果确认

汽车数据处理者按照数据出境安全管理相关法律法规和评估结果通知书的有关要求，规范开展数据出境活动；

对评估结果有异议的，可以在收到评估结果通知书 15 个工作日内向网信部门申请复评。

6．重新申报评估

出现以下情形之一的，汽车数据处理者应重新申报数据出境安全评估：

(1)向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的；

(2)延长个人信息和重要数据境外保存期限的；

(3)境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力的；

(4)汽车数据处理者或者境外接收方实际控制权发生变化的；

(5)汽车数据处理者与境外接收方法律文件变更等影响出境数据安全的；

(6)有效期届满仍需继续开展数据出境活动，但不满足评估结果延长条件的；

(7)已经通过评估的数据出境活动在实际处理过程中因不再符合数据出境安全管理要求被终止，汽车数据处理者在按照有关要求整改后，需要继续开展数据出境活动的；

(8)出现影响出境数据安全的其他情形。

（四）订立个人信息出境标准合同

汽车数据处理者应按照《个人信息出境标准合同办法》《个人信息出境标准合同备案指南（第二版）》规定，订立个人信息出境标准合同。

1．梳理出境活动整体情况

收集本企业及境外接收方等相关方材料，梳理出境活动整体情况，包括：

(1)汽车数据处理者基本情况，包括股权结构、实际控制人、境内外投资情况、组织架构和个人信息保护机构信息、整体业务与处理个人信息情况等；

(2)拟出境个人信息情况，包括：

a)个人信息出境涉及业务、个人信息收集使用、信息系统等情况；

b)汽车数据处理者和境外接收方处理个人信息的目的、范围、方式；

c)出境个人信息的规模、范围、种类、敏感程度，处理敏感个人信息情况；

d)拟出境个人信息在境内存储的系统平台、数据中心等情况，个人信息出境链路相关情况，计划出境后存储的系统平台、数据中心等；

e)个人信息出境后向境外其他接收方提供的情况。

(3)境外接收方情况，包括境外接收方基本情况，境外接收方处理个人信息的用途、方式，境外接收方履行责任义务的管理和技术措施、能力等；

(4)汽车数据处理者认为需要说明的其他情况。

2．开展个人信息保护影响评估

(1)评估事项

汽车数据处理者应结合个人信息出境活动整体情况和相关材料重点评估以下事项，包括：

a)个人信息出境和境外接收方处理个人信息的目的、范围、方式等是否具有合法性、正当性、必要性；

b)出境个人信息的规模、范围、种类、敏感程度，个人信息出境是否会对国家安全、公共利益、个人或者组织合法权益带来风险；

c)境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全；

d)个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

e)境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响；

f)其他可能影响个人信息出境安全的事项。

(2)发现问题并整改

汽车数据处理者在开展个人信息保护影响评估过程中发现存在影响个人信息出境的风险和问题的，应及时整改，并记录相关情况。

(3)形成个人信息保护影响评估结论

汽车数据处理者综合个人信息保护影响情况和相应整改情况，对个人信息出境活动作出客观的影响评估结论，并充分说明理由。

(4)编制个人信息保护影响评估报告

汽车数据处理者整理个人信息保护影响评估工作情况、出境活动整体情况、出境活动的风险评估情况及结论，编制形成个人信息保护影响评估报告。

3．签订合同

汽车数据处理者与境外接收方签订个人信息出境标准合同。

4．备案

(1)材料提交

汽车数据处理者按国家有关规定，向网信部门提交统一社会信用代码证件影印件、法定代表人身份证件影印件、经办人身份证件影印件、经办人授权委托书、承诺书、《个人信息出境标准合同》、《个人信息保护影响评估报告》等备案材料。并按要求提交补充

完善材料。

(2)结果反馈

汽车数据处理者获得备案编号后按照个人信息出境安全管理相关法律法规有关要求，规范开展个人信息出境活动。

5．补充或重新备案

在标准合同有效期内出现下列情形之一的，汽车数据处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：

(1)向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化的；

(2)延长个人信息境外保存期限的；

(3)境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；

(4)可能影响个人信息权益的其他情形。

（五）通过个人信息保护认证

按照国家网信办和国家市场监督管理总局等部门有关规定开展。

四、汽车数据出境安全保护要求

（一）管理要求

1．部门要求

汽车数据处理者应当明确企业内部汽车数据出境管理部门，统筹协调推进数据出境安全管理，监督检查数据出境相关管理要求的落实情况。

2．人员要求

汽车数据处理者应当明确汽车数据出境安全负责人，对本企业数据出境活动以及采取的保护措施进行监督，对本企业数据出境活动的安全性负责。

3．制度要求

汽车数据处理者应当明确网络安全、数据安全、个人信息保护等方面的制度要求，针对

性明确汽车数据出境安全管理要求。

4．审批要求

汽车数据处理者应当建立汽车数据出境内部登记审批机制，设定审批权限和审批流程，对审批材料进行整理存档。

（二）防护技术要求

1．数据出境传输安全

汽车数据处理者应当采取以下保护措施：

(1)采用校验技术、密码技术、安全传输通道或者安全传输协议等措施，保证数据出境传输过程中汽车数据的保密性和完整性。

(2)汽车数据出境相关系统应当具备对境外数据接收方进行身份鉴权的能力，确保境外数据接收方身份真实性。

2．数据出境安全监测要求

汽车数据处理者应当对汽车数据出境传输行为进行安全监测，形成安全日志并留存。

3．检查支持要求

汽车数据出境相关系统应当具备数据出境安全检查技术支持能力，对数据出境原始流量进行留存，支持数据防篡改和内容解析。

(1)全量留存。按照起止时间对数据出境流量进行全量留存，留存时间 1 周。

(2)抽样留存。支持按照起止时间、IP 地址范围对数据出境流量进行抽样留存，留存时间不少于 1 个月。

（三）日志要求

1．日志记录

(1)网络流量日志

汽车数据处理者应当对汽车数据出境的网络通信行为进行记录，包括日期、时间、源 IP 地址、目的 IP 地址、源端口、目的端口、传输层协议、应用层协议、数据包大小等，形成通信日志并留存。

(2)操作行为日志

汽车数据处理者应当对直接向境外传输汽车数据的主机的操作行为进行记录，包括用户

信息、操作时间、操作对象、操作类型、登录 IP、设备信息等，形成操作行为日志并留存。

2．日志留存

汽车数据处理者应对网络流量日志、操作行为日志、安全日志进行防篡改留存，留存时间不少于 3 年。

3．日志审计

汽车数据处理者应当对网络流量日志、操作行为日志、安全日志进行审计，当发现存在非法操作等安全风险隐患时，及时响应处置。

（四）应急处置要求

汽车数据处理者应当建立汽车数据违规出境的处置能力，发现异常行为时应及时处置，并按有关要求向本地区行业监管部门报告。

二、热点案例

强源头治理 促规范发展 上海市委网信办深入开展“清朗·整治 AI 技术滥用”专项行动第一阶段工作

发布机关：上海市委网络安全和信息化委员会办公室

发布时间：2025.06.12

为贯彻落实中央网信办“清朗·整治 AI 技术滥用”工作部署，4 月下旬以来，上海市委网信办聚焦 6 类突出问题深入开展第一阶段专项行动。现向社会公布阶段性工作成果，进一步凝聚共识，共同营造清朗网络生态。

强化合规，全面清理整治违规 AI 产品和信息

试试文字发笔记 去发布 >

小红书关于整治AI技术滥用的治理公告

为维护清朗网络空间，营造积极健康、文明和谐的社区环境，小红书积极响应中央网信办、上海市委网信办关于“清朗 · 整治AI技术滥用”专项行动的要求，重点聚焦利用AI批量生产虚假内容涨粉、利用AI起号引流带货、售卖AI起号课程、售卖AI账号等违规行为开展专项整治工作，切实履行平台责任，深入清理违规问题。本阶段具体治理情况如下：

哔哩哔哩关于整治AI技术滥用的公告

哔哩哔哩治理小分队

编辑于 2025年05月12日 12:23

为贯彻落实中央网信办“清朗·整治AI技术滥用”专项行动要求，哔哩哔哩平台将持续加强内容管理，严格防范AI技术滥用行为，重点整治以下内容：

- **虚假信息治理**
  - 严禁利用AI技术生成、传播虚假新闻、不实信息，尤其是涉及社会热点、公共事件等误导性内容。
  - 禁止伪造官方机构、新闻媒体或他人身份发布虚假信息。
- **侵权内容治理**
  - 禁止未经授权使用AI技术复制、仿冒他人形象、声音、作品（如影视、音乐、绘画等），或生成侵犯他人肖像权、著作权的内容。
  - 严禁利用AI技术篡改、拼接他人原创内容进行恶意传播。
- **恶意行为治理**
  - 禁止利用AI技术制作、传播淫秽色情、暴力恐怖、诈骗等违法违规内容。
  - 打击利用AI“换脸”“变声”等技术实施侮辱诽谤、敲诈勒索、仿冒诈骗等行为。
- **内容标识管理**
  - 根据《互联网信息服务深度合成管理规定》，平台将对AI生成内容（如AI绘画、AI语音、AI视频等）进行显著标识，确保可溯源、可区分。
  - 用户发布AI生成内容时需主动添加标签说明（如“AI合成”），未标注内容将限制传播或下架处理。

社区坚持倡导和维护积极向上、健康友爱的社区氛围，将依据《哔哩哔哩社区公约》对违规内容及账号进行严肃处理。同时，也呼吁广大用户共同监督，如发现相关违规行为，欢迎通过站内在线客服或客服邮箱 网页链接 进行反馈，社区期待与大家一起维护良好社区氛围，让我们携手维护清朗网络空间，推动AI技术合规健康发展，共建绿色网络空间。

上海市委网信办指导小红书、哔哩哔哩、拼多多等 15 家重点网站平台，集中清理“一键脱衣”、未经授权的人脸或人声克隆编辑、未备案等违规 AI 产品、商品及相关营销、炒

作、推广、教程信息。小红书、哔哩哔哩主动发布专项行动治理公告，开通了有害 AI 内容的举报受理处置渠道；星野开展智能体全面排查清理。各重点网站和 AI 平台共拦截清理相关违法违规信息 82 万余条，处置违规账号 1400 余个，下线违规智能体 2700 余个。经整治，网络违规 AI 信息显著减少。

上海市委网信办深化大模型合规指导服务中心作用，指导各类提供生成式人工智能服务的主体落实合规义务，强化安全评估，迄今已完成 82 款大模型备案，87 款应用登记。对 3 款未履行备案或登记程序提供服务且存在风险的应用，依法约谈并给予行政处罚。

督导联动，提升 AI 平台安全风控能力

上海市委网信办指导重点 AI 平台加强技术源头治理，深化自查自纠，加强训练语料管理机制，加强新版本新应用上线、API 接入应用的安全管理，用好大模型能力持续提升安全水平，建立健全与业务规模相适应的风控机制。组织专业机构对 8 家企业 14 款 AI 类应用开展了巡查测试，对部分重点平台开展现场检查和上门指导，发现并督导整改优化内容审核、意图识别等安全措施的薄弱环节。通过系统性排查和闭环整改，上海重点 AI 平台和重点平台 AI 应用的合规性、安全可控性持续增强。

以人为本，强化重点领域 AI 安全管理

针对关乎人民群众“生命线”“钱袋子”和“未成年人保护”等社会高度关注的 AI 应用，上海市委网信办会同市卫健委、金融监管等主管部门，对申请备案、登记的垂域模型和应用加强审核和业务指导，对 33 款已完成备案、登记提供医疗健康、金融、教育、情感陪伴服务的 AI 应用开展督导检查，要求完善行业领域安全审核和控制机制，加强专业知识库和检索增强能力建设，提升输出准确性，防范虚假、误导、诱导沉迷对患者、投资者、未成年人带来的不良影响。

联合市卫健委，指导上海人工智能实验室举办了医疗大模型开源评测社区上线发布会和上海网络安全博览会“医学人工智能安全”论坛，面向全市各医疗机构、医疗服务企业开展 AI 安全宣贯和合规指导，依托上海市医疗大模型应用检测验证中心对 16 家机构 20 个 AI 医疗场景开展评估，结合模型安全性评价和业务验证，强化行业规范和伦理审查，指导安全加固，引导规范应用。

多策并举，强化 AIGC 标识示范和全链条治理

上海市委网信办将高标准落实《人工智能生成合成内容标识办法》及配套强制性国家标准作为专项治理的关键抓手，切实保障公众知情权。先后组织开展了 4 场面向大模型企业、重点网站平台、应用企业的法规宣贯和专题交流，覆盖企业 400 余家，深入解读标识要求和技术路径，推动企业从“要我落实”转向“我要落实”。指导成立 AIGC 标识生态联盟，上海人工智能安全治理实验室联合重点大模型企业、网站平台，合力推进标识互认、能力共享与标准协同。

围绕“制作-传播”环节，指导重点网站平台加快配备显式与隐式标识功能，不断提升

AIGC 内容、AI 高风险行为的检测识别和治理能力。通过政策指导、生态协同与技术落地，稀宇科技、阶跃星辰、通义、小红书、哔哩哔哩、Soul 等已基本完成显式标识规范上线，加快开发上线隐式标识和传播链互认验证，小红书牵头编制图片模态元数据标识实践指南，上海标识工作取得阶段性成效。

上海市委网信办将持续深化专项行动，统筹技术治理、制度建设和生态优化，强化对重点问题、平台、环节的常态化监管，推动智能向善。第二阶段将聚焦 AI 造谣、低俗内容等 7 类突出问题加大整治力度，维护良好网络生态。上海将切实落实习近平总书记考察上海的重要指示，力争在人工智能发展和治理各方面走在前列，产生示范效应。

三、实务解读

1. 买来的数据，就没风险了？

供稿人：潘永建（上海市通力律师事务所）、邓梓珊（上海市通力律师事务所）、嵇若琳（上海市通力律师事务所）

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？**

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：

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，某司最近受到政府调查，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。