汉坤法律评述
2026 年 2 月 24 日

HANKUN
汉坤律师事务所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港 | 海口 | 武汉 | 新加坡 | 纽约 | 硅谷

行稳致远：从《汽车数据出境安全指引》看汽车数据合规治理的系统化转向

作者：段志超 | 王雨婷 | 甘雨丰 | 左今

引言

2026 年 1 月 30 日，工业和信息化部、国家网信办、国家发展改革委、国家数据局、公安部、自然资源部、交通运输部、市场监管总局等八部门联合印发《汽车数据出境安全指引（2026 版）》（以下简称为**“《安全指引》”**），并于 2 月 3 日正式公开发布。《安全指引》在《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》等上位法律法规的基础上，结合汽车行业特性，细化了重要数据判定规则，明确了汽车数据出境活动的豁免场景和管理方式，并制定了汽车数据出境的安全保护要求。

在《安全指引》发布前，《汽车数据安全管理若干规定（试行）》（以下简称为**“《若干规定》”**）界定了汽车行业重要数据的类型，但部分类型仅基于数据性质进行判断，缺乏与具体业务场景的映射，也未设定细分的量化标准。随着行业实践中多样化业务需求的产生，企业在实际操作中缺乏明确的判断依据，导致一些落入宽泛分类，与国家安全、个人权益等关联度较低的数据，即使具备正当的业务理由，也难以合法出境，从而制约了汽车行业的数据跨境流动与应用。

随着智能网联汽车和相关技术的快速发展，汽车数据类型及应用场景日益多样化。在此背景下，《安全指引》应运而生，为更加贴近行业需求、安全可控的汽车行业的数据跨境提供了依据。此外，《安全指引》虽然以数据出境为直接着眼点，但其实际影响更为广泛，一方面通过八部委联动协同明确行业重要数据识别要求，另一方面也串联了重要数据目录报送、技术出口、测绘地理信息管理等合规工作，是汽车数据安全管理领域一项具有重要指导意义的规范性文件。

一、重要数据识别规则

在个人信息识别和出境监管已经日趋成熟的前提下，重要数据的识别和出境安全评估已经成为了相关企业关注的重点。《安全指引》第二章结合汽车企业常见业务场景提出了重要数据的判定规则。根据工信部的指导，汽车数据处理者在判断数据级别时，应先按照数据类别、数据项和数据项说明确定数据分类，再根据判定规则确定数据级别，识别是否属于重要数据。

（一）涉及的场景及数据类别

相较于既有规章文件，《安全指引》进一步明确了汽车重要数据的判定框架，从业务运行视角将相关数据划分为研发设计、生产制造、驾驶自动化、软件升级服务以及联网运行五大业务场景，并对各场景下可能涉及的 27 个重要数据类别、51 个数据项进行了映射与说明。根据《安全指引》，涉及汽车重

要数据的业务场景及数据类别汇总如下：

序号	业务场景	业务活动描述	数据类别
1-1	研发设计 — 产品研发	整合全球研发资源、产品协同设计开发	设计物料清单、研发设计文档、开发源代码
1-2	研发设计 — 产品测试	开展产品仿真、场地和实际道路测试	标注场景数据、仿真场景数据、测试场景数据
2	生产制造	汽车产品生产制造	工艺物料清单、生产控制程序源代码
3	驾驶自动化	组合驾驶辅助或自动驾驶功能开发、部署、应用	驾驶自动化算法数据、驾驶自动化算法训练数据、驾驶自动化算法特征数据
4	软件升级服务	升级汽车安全驾驶及电池管理功能的软件包对应源代码	软件升级数据
5-1	联网运行 — 车辆数据	车辆联网运行	车辆识别码、车联网卡标识码、车辆密钥、车辆数字证书、控制指令
5-2	联网运行 — 车路感知	车辆及路测设备联网运行	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
5-3	联网运行 — 车路分析	车路协同分析、构建车路协同系统	融合计算数据
5-4	联网运行 — 车联网平台运营	车联网平台建设、运行、维护	网络规划数据、充电运行数据、安全保障数据

值得注意的是，《安全指引》还设置了重要数据识别的兜底条款，即符合以下情形之一的汽车数据也应认定为重要数据：

1. 其他出境业务场景中符合重要数据判定规则的；

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、国家互联网信息办公室等相关部门公开或告知属于重要数据的。

因此，上述五类场景及对应的数据类别并非穷尽列举，原则上若相关数据项符合判定规则，均有可能被认定为重要数据，无论是否属于《安全指引》所列的特定场景。但鉴于该框架整体覆盖已较为全面，企业在实际开展重要数据识别工作时，可以优先参照明确列举的重要数据范围进行识别和管理，仅在确有必要的情况下结合兜底条款对未列举的数据场景及数据类别予以补充识别。

（二）重要数据判定规则

在明确重要数据所涉及的业务场景、数据类别和数据项的基础上，《安全指引》进一步细化了重要数据的判定规则。概括而言，在列举的数据类型范围内，具备特定属性或达到一定规模、精度或影响程

度的数据，将被认定为重要数据。根据工信部的指导[1]，重要数据判定规则的九类相关因素如下：

1. 成果相关
2. 地理信息相关
3. 公共安全执法相关
4. 出口管制相关
5. 系统功能相关
6. 累计时长相关
7. 规模精度相关
8. 车辆数量相关
9. 个人信息相关

上述判定规则遵循了《网络数据安全管理条例》对于重要数据的总体定义，并基于《若干规定》对汽车领域重要数据的定义进行了细化和完善。同时，《安全指引》还引入了《公共互联网网络安全突发事件应急预案》《工业和信息化领域数据安全事件应急预案（试行）》对重大及以上网络安全事件、数据安全事件的分级标准，以及《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》中关于技术出口管制、两用物项管理的相关规定，并结合智能网联汽车有关测绘地理信息数据的监管规则，将汽车领域重要数据的判定规则与其他相关领域监管规则衔接整合。整体而言，该判定体系从形式上体现为精度、规模、区域、科技成果、个人信息等多重因素的综合考量，本质上各项判定规则的底层逻辑仍是围绕车辆安全、公共安全和国家安全展开。

《安全指引》累计规定了 29 条重要数据判定规则，相关规则以目录形式匹配各业务场景、数据类型及数据项，不同场景和数据类型相关的判定规则有所重合和交叉。为帮助企业更好地把握其内在逻辑，我们基于对《安全指引》相关内容的理解，对重要数据判定规则进行了系统梳理与整合，将上述 29 条规则归纳为 10 类，并结合既有监管框架进行了分析解读，有助于企业理解重要数据判定规则的整体结构。

1. 重要敏感地区与公共安全执法相关数据

相关判定规则：

- 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
- 经汇聚、分析后能够推算出涉密、敏感地理信息数据的
- 涉及或经汇聚、分析后能推算出大型活动安保等管控现场情况、交通事故等突发案事件警情现场情况以及其他涉及社会公共安全行政执法活动和人员的

[1] https://wap.miit.gov.cn/zwgk/zcjd/art/2026/art_ab6b09a94b174017bbc32b8c00a9fe42.html。

解读：

“军事管理区、国防科工单位以及县级以上党政机关”是《若干规定》明确列举的重要敏感区域，在此基础上，《安全指引》将《测绘地理信息管理工作国家秘密范围的规定》《公开地图内容表示规范》规定的涉密、敏感内容也纳入重要数据判定的考虑因素。参考有关规定，根据这一判定规则被认定为重要数据的数据项可能包括体现和表明我国政府立场与主张的敏感、争议地区等可能涉及国家秘密的数据，以及武器弹药等物品的集中存放地、国家安全等要害部门、石油天然气重要管线、军民合用机场港口和码头、以及卫星导航定位基准站等公开地图禁止表示的内容。

此外，大型活动安保等管控现场、交通事故等突发案件警情现场等涉及社会公共安全执法活动和相关人员的数据，也可能被认定为重要数据。

2. 车辆流量、人员流量、物流等反映经济运行情况的数据

相关判定规则：

- 涉及道路的车辆流量、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
- 覆盖至少单个完整路口，时间跨度大于 1 个月的

解读：

该等规则基本沿用了《若干规定》中的重要数据判断标准，重点关注相关数据是否具备反映经济运行情况的能力。将此类数据纳入重要数据管理，有助于防范其被用于推断区域经济运行情况并引发潜在社会安全风险的可能性。

《安全指引》在《若干规定》的基础上引入了“累计时间”要求，将短期、分散数据与具有连续性、可用于持续研判的数据加以区分，使重要数据的风险把控更精细化，同时也为自动驾驶企业开展数字孪生路口等业务活动时，提供了更具可操作性的标准，便于准确识别和界定重要数据。

3. 包含人脸信息、车牌信息等的车外视频、图像数据

相关判定规则：

- 车外真实人脸边界框最小边长为 32 像素以上的
- 车外真实汽车号牌边界框最小边长为 16 像素以上的

解读：

该数据类别同样基本沿用了《若干规定》中的重要数据判断标准。针对包含人脸、车牌信息的车外视频、图像数据，《安全指引》在阈值设定上与《GB/T 44464-2024 汽车数据通用要求》（以下简称为**“《通用要求》”**）中匿名化处理的触发条件保持一致。

具体而言，针对车外人脸图像，《通用要求》第 5.6.2.1.1 条规定，汽车数据处理者至少应对图像或视频中满足以下要求的人脸目标进行匿名化处理：（1）人脸边界框最小边长像素大于或等于 32 像素；（2）人脸边界框内可见范围比值大于 50%且可见范围内眼睛、鼻子或嘴清晰可见。

针对车外车牌图像，《通用要求》第 5.6.2.1.2 条规定，汽车数据处理者至少应对图像或视频中满足

以下要求的汽车号牌目标进行匿名化处理：（1）汽车号牌边界框最小边长像素大于或等于 16 像素；（2）汽车号牌目标无遮挡且可识别全部数字及文字内容。

也即，在未依法实现车外视频、图像全量匿名化处理的情况下，凡达到相应清晰度和可识别程度阈值的车外人脸及车牌图像数据，原则上应被视为重要数据进行保护。

4. 大规模的传感器采集数据

相关判定规则：

- 涉及采集真实环境中累计 2,000 小时以上原始影像的，或者基于此影像生成的
- 涉及 1,000 万张以上原始图片的，或者基于此图片生成的

解读：

该等判定规则通常适用于标注、仿真、测试场景产生的数据，驾驶自动化算法特征数据，以及车路感知场景下车辆及路测设备产生的数据。

该数据类别衔接了近年来针对智能网联汽车测绘地理信息收集与处理的监管要求，并在《自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知》及《自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知》（以下简称为**“《139 号通知》”**）的基础上，结合时空数据的定义以及实际业务场景，从数据量、覆盖车辆数量、累计时长等角度细化了针对传感器数据的判定规则。

除重要数据监管外，收集和处理传感器数据还需关注地理信息数据的合规要求，具体可见下文第三章的分析。

5. 大规模的车辆数据与个人身份信息

《安全指引》为特定场景下的车辆数据和个人身份信息设置了不同的重要数据认定门槛：

- “10 万台车”。下述数据可能被认定为重要数据：
  - 涉及在境内运行的 10 万台以上车辆收集的标注场景数据、仿真场景数据、测试场景数据、驾驶自动化算法训练数据与算法特征数据、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
  - 涉及在境内运行的 10 万台以上车辆的远程启动、诊断、更新、通信过程中的密钥
  - 涉及在境内运行的 10 万台以上车辆的远程启动、诊断、更新、通信过程中的根证书
- “100 万人”。下述场景可能被认定为重要数据出境：
  - 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车辆识别码（VIN）以及车联网卡标识数据

解读：

该数据类别主要以数据量作为核心判定标准，将达到一定数据量的个人身份识别信息、车辆收集或运行产生的数据纳入重要数据范围。其规范重点不强调数据内容本身的敏感性，而在于数据主体数量、覆盖车辆规模以及由此引发的系统性安全风险。

从规则设计思路看，该类判定规则在《若干规定》确立的“10 万”数量阈值基础上进行了差异化细分。对于车辆收集的外部感知数据以及与车辆运行和系统安全高度相关的数据类型，《安全指引》沿用了“10 万”台车辆的判定标准。相比之下，对于车辆标识符类数据（如 VIN、车联网卡标识），《安全指引》将判定阈值提升至“100 万人”，并附加“可识别个人身份”的条件，在一定程度上反映出单纯与个人身份关联、但不直接影响车辆运行安全的数据，其敏感性在监管层面的评价相对更为审慎。这样的细分在一定程度上降低了企业因触发“10 万人”的单一标准而需履行数据出境安全评估程序的合规负担。

VIN 等车辆识别符是否属于个人信息，以及在何种情形下应按照个人信息进行处理，一直是汽车行业实践中较为棘手的问题。《安全指引》中关于车辆识别符类数据的重要数据判定规则，并未简单套用一般个人信息的适用逻辑，而是体现出一定的区分处理思路，也为理解相关问题提供了参考。从相关规则的表述来看，车辆识别符类数据本身通常并不具备直接识别自然人的能力，其可识别性有赖于与其他信息相结合，为处理相关问题保留了空间。

6. 充电运行数据涉及的车辆数据与充电服务数据

该类别项下的数据类型与判定规则包括：

- 向境外提供车辆**充电状态监测数据**，涉及在境内运行的 10 万台以上车辆收集
- 自当年 1 月 1 日起累计向境外提供 100 万人以上的**充电数据**

解读：

《安全指引》未沿用《若干规定》中“充电网的运行数据”这一概念，而是将充电运行数据归类在“联网运行场景 — 车联网平台运营”场景下，明确列示了充电设施位置数据、车辆充电状态监测数据、充电数据三类数据项。充电设施位置数据若涉及国防科工单位、党政机关的，将触发前述第 1 类“重要敏感地区”项下的判定规则，因此不再赘述。3 类数据项中：

- 车辆充电状态监测数据包括车辆充电功率、充电电流、充电电压、当前电池温度、电池健康状态
- 充电数据包括充电账号、开始时间、结束时间、充电站点位置、充电量、充电费用等

与前述第 5 类判定规则类似，《安全指引》为上述两类充电运行数据设定了不同的数量阈值，体现出对数据风险属性的差异化判断。对于与充电服务使用行为直接相关的订单类数据，《安全指引》将重要数据认定门槛提高至“100 万”人；而针对车辆产生的充电状态数据，则继续以《若干规定》项下的“10 万”作为标准。

7. 软件升级与车辆控制数据

该类别项下的数据类型与判定规则包括：

- 向境外提供**车辆控制指令**，涉及在境内运行车辆的
- 向境外提供安全驾驶、电池管理功能升级软件程序**源代码**，同时符合以下条件的：
  - 涉及升级境内运行车辆的；
  - 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；

- 涉及车辆启动行驶、动力丢失、紧急制动、巡航控制、车道保持、充放电控制、电池温度控制功能的。

解读：

在软件升级与车辆远程控制的场景下，《安全指引》设定了与前述数据类别不同的判定规则，体现了监管机构对车辆行驶安全风险防范的高度重视。如前所述，在车辆联网运行场景下，大部分数据类型以车辆数量作为重要数据认定的关键指标，但在涉及车辆控制的情况下，若车辆控制指令可以实现境内车辆车门开关、车辆启动、转向、加速、制动、泊车和充放电控制、温度控制等电池管理的远程控制，均会被认定为重要数据，无论实际涉及的车辆数量。

汽车安全驾驶、电池管理功能的远程升级软件包源代码也是类似的严格监管逻辑，但《安全指引》同时规定了豁免情形。对于 OTA 升级场景中跨境传输的重要数据，如属于因消除汽车产品缺陷、实施召回所需，且已按照《缺陷汽车产品召回管理条例》向国家市场监督管理总局备案的 OTA 升级软件包中对应的源代码，则可免于申报数据出境安全评估，具体请见下文第二章的分析。

8. 车联网平台网络规划数据

相关判定规则：

- 涉及服务境内运行车辆数量 100 万台以上的车联网平台**的网络规划数据**
- 同时满足提供在线升级服务，境内运行车辆数量 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**网络规划数据**

解读：

针对车联网平台的网络规划数据，符合以上任意一项条件的均可能被认定为重要数据。网络规划数据包括：

- 资产配置信息指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、服务端口、登录方式
- 网络拓扑图指能够显示内网网络结构的车联网平台网络拓扑图，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

对于在境内运营的外资车企而言，如其车联网平台构建在全球统一的 IT 架构上，基于集中式安全运维体系及跨境技术支持，其相关平台运营可能因此受到实质影响。例如，境外总部对境内车联网平台进行远程运维、漏洞扫描、安全监测或系统升级时，如需调取资产配置信息或网络拓扑结构数据，可能构成重要数据出境。类似的，云服务厂商为车联网平台提供底层云基础设施过程中，若需要境外团队参与运维支持，应避免向境外提供或允许境外团队访问符合上述条件的网络规划数据，否则将面临更为严格的数据出境合规义务。

9. 安全保障数据

相关判定规则：

- 涉及高危及以上安全漏洞的
- 涉及重大及以上网络和数据安全事件的

解读：

符合以上任意一项条件的威胁信息均可能被认定为重要数据。威胁信息指未公开的车辆及车联网平台安全漏洞信息以及相关系统名称、系统域名、IP 地址、端口、风险 URL，安全事件信息以及相关攻击方式、攻击活动、威胁主体等。

将此类数据纳入重要数据管理的核心考量在于防止相关信息被恶意利用，从而危害车辆安全。《安全指引》本身并未明确“高危”、“重大”的标准。参考《公共互联网网络安全突发事件应急预案》以及《工业和信息化领域数据安全事件应急预案（试行）》，“重大安全事件”通常需要达到涉及一千万人的个人信息泄露或其他标准。“高危安全漏洞”可参考《GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南》综合识别和判断。

此外，根据《安全指引》，出于修补安全漏洞或处置安全事件所需，并已经在主管部门备案或报告的安全漏洞、安全事件数据可免于申报数据出境安全评估，具体请见下文第二章的分析。

10. 技术成果

相关判定规则：

- 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
- 涉及《中华人民共和国两用物项出口管制清单》中相关物项的
- 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
- 国家重大专项、国家重点研发计划支持的
- 可能对国家科技安全、行业竞争力等产生影响的

解读：

该等判定规则通常适用于设计物料清单、研发设计文档、开发源代码、工艺物料清单、生产控制程序源代码、驾驶自动化算法数据、驾驶自动化算法特征数据。

《安全指引》不仅涵盖原始数据，还明确将算法源代码、算法参数、设计文档等技术成果和相关文件纳入重要数据监管范畴。同时，《安全指引》充分考虑了驾驶自动化业务场景的业务实践，明确将车端预置且无法导出使用的算法排除在算法参数出境的范围之外。

在上述判定规则中，“可能对国家科技安全、行业竞争力等产生影响”这一规则暂无明确的技术目录或量化参数供企业参考判断，企业需结合拟出境的技术成果进行个案论证。

二、对汽车数据出境合规路径的影响

整体而言，《安全指引》在数据出境合规路径的判断标准上延续了《跨境新规》的核心逻辑，汽车数据处理者需结合出境目的、出境数据类型与规模，选择所适用的合规路径，确保数据跨境流动合法合规。在此基础上，《安全指引》在数据识别和相配套的安全保护要求上做出了额外的规定，相关企业需参照指引及时调整内部的数据出境合规制度，避免由于制度衔接带来的额外风险。

（一）数据识别

1. 识别重要数据及出境规模

只要汽车数据处理者所处理的数据中包含有“重要数据”，除了跨境合规义务之外，该等主体即需履行作为“重要数据处理者”的法定合规义务，包括但不限于《数据安全法》《若干规定》规定的设立责任人、开展及报送风险评估、报送年度汽车数据安全管理情况等义务。有鉴于《安全指引》对汽车领域的重要数据进行了更加全面的定义，汽车数据处理者应尽快根据指引中的重要数据判定规则，全面识别并判断企业是否处理“重要数据”。

针对已识别的重要数据，需进一步梳理相关的数据出境情况。为满足各地年度汽车数据安全管理情况报送要求，数据识别阶段的数据出境情况梳理应至少包括数据出境目的、必要性、方式、频率、年度出境数据规模等必要维度。

2. 识别豁免情形

《安全指引》在《促进和规范数据跨境流动规定》（“**《跨境新规》**”）第 5 条、第 6 条规定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（统称为“**数据出境前置程序**”）的豁免情形基础上，新增了 3 类汽车行业特有的数据出境申报豁免情形，具体包括：

(a) 因修补安全漏洞需要，按照《网络产品安全漏洞管理规定》有关要求，已向工信部报告的安全漏洞数据；

(b) 因处置安全事件需要，按照行业网络安全、数据安全事件相关应急预案，已向工信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；

(c) 因消除汽车产品缺陷、实施召回需要，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。

此外，《安全指引》在豁免情形中重申了《跨境新规》第 6 条规定的自贸区豁免规则。根据目前公开信息，北京、重庆、天津、福建已发布的自贸区数据出境负面清单中包含有汽车行业子类清单内容。如汽车数据处理者登记注册于自由贸易试验区内，建议同步重点关注所在自贸区发布的数据出境负面清单。

（二）落实安全保护要求

《安全指引》从管理制度建设、技术防护措施、日志记录管理及应急处置机制四个方面，明确了汽车数据处理者在数据出境全流程中应落实的事前预防、事中监控和事后处置安全保护措施，为汽车数据处理者落实《跨境新规》第 11 条关于向境外提供数据时应履行的数据安全保护义务提供了具体可行的落地指引。相较于《数据安全法》《网络数据安全管理条例》等法律法规规定的数据出境合规要求外，汽车数据处理者应重点关注并落实如下《安全指引》规定的具体安全保护要求：

1. **管理机制：**应明确汽车数据出境管理部门、汽车数据出境安全负责人、针对性明确汽车数据出境安全管理要求、建立汽车数据出境内部登记审批机制。

2. **防护技术：**汽车数据出境相关系统应具备对境外数据接收方进行身份鉴权的能力；相关平台或系统应对数据出境网络通信流量进行留存，支持数据防篡改和内容解析，数据出境网络通信流量的具体留存要求如下：

- 全量留存时间为 1 周
- 按照起止时间、IP 地址范围等对数据出境网络通信流量的抽样留存，时间不少于 1 个月

3. 日志要求：

- 需留存的日志包括（i）“网络流量日志”（*对汽车数据出境的网络通信行为进行记录，至少包括日期、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、数据量大小等*）；（ii）“操作行为日志”（*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、操作结果、数据访问权限变更等*）以及（iii）“安全告警日志”（*对汽车数据出境传输网络通信、主机或系统操作行为安全监测形成的日志*）
- 上述日志留存时间应不少于 3 年
- 应对上述日志进行防篡改留存以及审计

三、与其他合规事项的联动

此外，由于《安全指引》设定的规则与重要数据识别和目录报送、技术出口管制、以及测绘地理信息数据合规等汽车行业合规事项有所交叉，相关企业应慎重考虑《安全指引》对其他合规事项的影响，综合进行调整。

（一）重要数据目录报送

尽管《安全指引》的规范重点在于汽车数据的出境管理，但系统梳理了各场景、各类型的重要数据判定规则，为汽车数据处理者识别和理解重要数据的范围提供了更具操作性的参考框架。

在现行监管实践中，汽车数据处理者识别并报送重要数据目录，主要依据《若干规定》、《YD/T 3867-2024 电信领域重要数据识别指南》，以及主管部门此前定向下发的《联网汽车运行及自动驾驶重要数据目录识别指引》等文件。随着《安全指引》的发布，未来不排除监管机构将基于《指引》进一步细化重要数据目录的报送要求，提升备案工作的统一性。

在此背景下，汽车数据处理者有必要结合《安全指引》所列的重要数据判定规则，对自身所处理的汽车数据进行前瞻性梳理和分类，并持续关注主管部门的最新要求，以更好地衔接重要数据目录报送及相应的安全保护义务。

（二）技术出口管制

《安全指引》出台前，技术出口管理以目录化监管为核心。若拟向境外提供的技术数据未被列入《中国禁止出口限制出口技术目录》《中华人民共和国两用物项出口管制清单》等管制目录，则相关数据出境活动原则上不受技术出口管制限制。

但《安全指引》在前述出口管制规则之外，将部分具有明显技术属性的数据类型（如设计物料清单、研发设计文档、开发源代码、工艺物料清单以及生产控制程序源代码等）同步纳入重要数据监管框架之中。根据《安全指引》，上述数据若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，国家重大专项、国家重点研发计划支持的，或可能对国家科技安全、行业竞争力等产生影响的，将被认定为重要数据，向境外提供需依法申报数据出境安全评估。

在实践层面，这意味着部分原本未落入出口管制目录管理范围的技术数据，可能因《安全指引》的适用而被纳入重要数据出境监管框架，从而面临严格的安全评估要求。

需要特别关注的是，在新增的重要数据判定规则中，“可能对国家科技安全、行业竞争力等产生影响的”这一表述具有一定概括性和开放性，具体适用边界仍有待进一步明确。在相关配套解释和监管实践逐步明晰之前，汽车数据处理者如拟向境外提供关键技术文件，尤其是涉及核心技术或处于行业领先地位的企业，宜通过自主论证、监管咨询等方式降低合规不确定性。

（三）测绘地理信息数据合规

《安全指引》在《139 号通知》确立的数据出境“双轨制”监管框架基础上，进一步明确了行业审批属于申报测绘地理信息数据出境安全评估的前置程序。《安全指引》明确指出，包含空间坐标、影像、点云及其属性信息等测绘地理信息数据的，应当在申报数据出境安全评估前依法履行对外提供审批或地图审核程序。

从实践情况看，测绘地理信息数据在收集、存储、传输、处理及地图制作等环节，原则上均需由具备相应测绘资质的主体开展，且相关处理活动通常在境内完成，因此，在实践中，严格依照上述路径向境外提供相关数据的情形相对有限。但需要注意的是，部分经确认无需按照测绘地理信息数据管理的汽车数据，仍可能因符合“涉及在境内运行的 10 万台以上车辆收集”等重要数据判定规则，而被纳入重要数据的管理范围。

因此，在汽车数据出境合规实践中，即便已完成测绘地理信息相关的合规判断，仍有必要同步关注其是否触及重要数据判定规则，从而在测绘地理信息管理与重要数据管理两个维度上进行综合评估与统筹安排。

结语

《安全指引》并非一部独立、封闭的数据出境操作文件，而是通过细化重要数据判定规则对汽车数据治理提出了更系统性的要求。对于汽车数据处理者而言，有必要在整体数据治理框架下分步骤落实汽车数据相关的各项合规工作：首先，应结合《安全指引》完善数据分类分级规则，开展重要数据识别工作，并匹配对应的安全保护措施；其次，应对照《安全指引》的新规则系统梳理数据出境情形，并选择合适的数据出境合规路径；最后，针对规则中仍存在不确定性的情形，尤其是涉及关键技术数据的跨境提供，应持续跟进监管动态、必要时开展监管沟通，以降低合规风险。

《安全指引》的意义不仅在于提高汽车数据出境监管体系的规范性和可预期性，也在于推动企业数据治理模式的转变。《安全指引》以数据出境为抓手，促使汽车数据合规管理由以单一合规事项为导向，逐步转向以数据全生命周期管理和风险识别为核心的综合治理体系。随着规则体系和监管实践的不断完善，能够在早期将相关要求内化为日常数据治理能力的企业，将在合规成本控制、业务灵活性以及跨境协同方面具备更为稳固的基础。

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