

The Regulatory Review for Intelligent Connected Vehicles and Automated Driving (August 2025)

Author: FU, Peng Zhao, Qingmeng Bao Jiewei

1、辅助驾驶与OTA监管走向纵深：智能网联产品召回、生产一致性与宣传规范

2025年8月13日，国家市场监督管理总局（“**市场监管总局**”）公开征求对《市场监管总局工业和信息化部关于加强智能网联新能源汽车产品召回、生产一致性监督管理与规范宣传的通知（征求意见稿）》（“**通知草案**”）的意见。[I]通知草案落实了《缺陷汽车产品召回管理条例》《关于进一步加强智能网联汽车产品准入、召回及软件在线升级管理的通知》（工信部联通装〔2025〕45号，“**工信部45号文**”）相关要求，与《广告法》《反不正当竞争法》衔接。

通知草案从监管方向上的信号意义在于：**监管部门对于辅助驾驶功能，监管视野从产品规格管理全面走向产品全生命周期监管。**

用户可感知的辅助驾驶产品“全生命周期”分为四个阶段：**装载阶段，宣传阶段，使用阶段，售后阶段。**

A. 装载阶段：强化生产一致性监督管理，关注OTA升级与关键信息填报

通知草案提出，工业和信息化部、市场监管总局将加强协调管理，发现企业未按照要求补充报送有关技术参数及验证材料、车辆性能与报送技术参数不一致、未经备案开展软件在线升级（“**OTA升级**”）活动、实际OTA升级活动与备案不一致的，依照有关规定进行处理。另外，对频繁开展OTA升级活动的企业，市场监管总局将进行重点抽查和专项核查。

海问评述：

若干年之前，OTA升级主要意在提升车机系统能力（特别是infotainment车载信息和娱乐系统功能）、修补车机系统常见漏洞。近年，随着新能源汽车和智能驾驶、辅助驾驶功能渗透率提升，OTA升级逐渐被部分主机厂主要用于升级、修正辅助驾驶能力，升级电源管理系统以及优化车控操作。

由此带来的问题也同样明显：主机厂可能通过频繁进行OTA升级，推出、改进、修补甚至取消部分稳定性并不十分完善的功能，甚至可以通过OTA升级直接覆盖产品缺陷。作为现象之一，部分主机厂OTA升级频率大幅度增加，引起了监管机构的关注。通知草案相当一部分内容，意在针对这一问题，进行监管规范。

对此，企业应当注意：

在机动车合格证系统中完整、准确填报组合驾驶辅助系统、储能装置单体及总成等关键信

严格执行OTA升级活动分类管理要求，未经备案不得开展OTA升级活动，不得将未经充分

确保生产的搭载组合驾驶辅助系统的智能网联新能源汽车产品与准入产品一致，并承担产

企业需要关注建立OTA升级的“备案—测试—推送—记录”全流程管理制度，明确每个环节的责任部门，并限定升级频率。

B. 宣传阶段：加强企业宣传行为监督，整治夸大宣传，避免误导消费者

监管机构关注的重点之一，是智能驾驶、辅助驾驶功能普及率“飙升”的背后，为提升车辆销量，部分主机厂对辅助驾驶功能进行重点宣传甚至“夸大宣传”，暗示具备高阶智能驾驶甚至“自动驾驶”能力。但与此同时，目前市场上普遍理

解量产乘用车并未标配L3或以上级别自动驾驶功能（在产品和驾驶事故责任承担方面尤其如此）。产品宣传、实际功能与法律责任承担一定程度上“脱节”。最严重的是，这一做法不利于保障驾乘安全。

因此，通知草案提出，市场监管总局将加大对企业广告活动和商业宣传行为中夸大组合驾驶辅助功能、欺骗或误导消费者等情形的监督检查力度，组织召回技术机构开展过度宣传等问题的技术认定工作，并会同工业和信息化部开展专项联合调查，依法做好整治规范工作。

海问评述：

对此，企业应当关注：

向消费者提供有关智能网联新能源汽车驾驶自动化等级、系统能力、系统边界等信息时，

在组合驾驶辅助系统或功能命名及营销宣传中，不得暗示消费者可以视其为自动驾驶系统

避免夸大宣传车辆驾驶性能，误导消费者以不合理的高速驾驶车辆。

注意涉及驾驶辅助功能、自动化等级的宣传文案（包括广告片、官网文案、销售人员话术

C. 使用阶段：加大缺陷调查与召回管理力度，聚焦驾驶辅助安全与网络安全

在用户使用辅助驾驶功能阶段，需要通过车书等车辆说明媒介，得到关于辅助驾驶功能的准确说明，有利于避免用户误解、准确使用产品。使用阶段，用户

可能因高度信赖辅助驾驶功能，产生驾驶懈怠，出现双手脱离方向盘甚至休息打盹等影响驾乘安全的操作，主机厂需要通过产品设计，有效防范此类风险。此外，智能网联系统也可能受到各类攻击、发现各种漏洞，主机厂需要作为责任主体，对系统网络安全准备充分的预案。

因此，通知草案提出，市场监管总局将对存在因安全提示和使用说明不完善、网络攻击、网络威胁和漏洞等安全事件开展缺陷调查，必要时督促企业通过召回方式进行改进。同时，市场监管总局将对驾驶员监测、警示和处置功能不足的问题开展专项调查，必要时纳入缺陷分析与调查工作。

海问评述：

对此，企业应当关注：

在车辆APP、车载信息交互系统显著位置和用户手册中显示组合驾驶辅助系统的安全提示

开发、使用安全优先的驾驶员监测、警示和处置功能，密切监测驾驶员的驾驶状态，在警示或控制措施，以便驾驶员及时接管车辆和降低安全风险。并且，不得通过用户操作或系

强化智能网联新能源汽车缺陷信息监测，减少网络攻击、网络威胁和漏洞引发的车辆事故

企业需要注意严格落实相关合规义务，避免因产品出现安全提示不显著、监测功能缺失或可关闭、网络安全漏洞未及时处理等问题，导致市场监管总局启动相应的缺陷调查，最终可能面临召回整改以及随之而来的经济损失和品牌声誉损害。

D. 售后阶段：强化事件事故报告与深度调查，明确报告义务与责任追究

通知草案提出，市场监管总局将联合工业和信息化部等有关部门加强事故深度调查与分析，并对企业事故报告情况进行监督检查，一经发现企业未按要求报告事故信息的，将向社会公开通报并督促整改。对企业在事件事故报告中存在隐瞒或遗漏重大事实的，市场监管总局、工业和信息化部将进行专项核查。

海问评述：

现实中出现了若干与辅助驾驶功能相关的严重事故，是本轮针对智能驾驶/辅助驾驶功能进行密集监管的直接导火索。对此，企业应当注意按照工信部45号文的要求，在获知其生产销售的智能网联汽车产品发生组合驾驶辅助系统失效导致功能退出等事件或搭载组合驾驶辅助系统车辆发生碰撞等事故的，应当根据有关要求向工业和信息化部、市场监管总局报告。

2、汽车数据安全合规检测：标准更新，安全加码

2025年8月18日，中国汽车工业协会等发布第三批次关于汽车数据处理5项安全要求检测情况的通报（“**第三批通报**”）[II]。部分车型存在如下数据安全问题：

车端匿名化处理的视频图像中人脸目标的匿名化检出率低于90%；

处理敏感个人信息的同意期限设置为始终允许或者永久；

持续收集敏感个人信息时，未通过车载显示面板图标或信号装置指示灯的闪烁可
车载系统上的应用程序缺乏隐私政策等。

另外，相较于2025年1月发布的第二批通报[III]，第三批通报对检验标准与检
验方法进行了调整，具体可见如下对比表格。

关于汽车数据处理4项安全要求检测情况 的通报（第二批） 检测标准与方法（2025年1月7日）	关于汽车数据处理5项安全要求检测情况 的通报（第三批） 检测标准与方法（2025年8月18 日）
--	---

检测依据：根据《汽车数据安全若干
规定（试行）》有关要求，按照 GB/T
41871-2022《信息安全技术 汽车数据处理
安全要求》、GB/T 44464-2024《汽车数
据通用要求》和 TC260-PG-20241A《网
络安全标准实践指南 - 车外画面局部轮廓
化处理效果验证》相关技术标准组织实施。

无变化

检测对象：截至2024年9月27日前，按照
《关于组织开展数据安全合规车型测评活动
的通知》（中汽协函字【2024】440号），
汽车制造商自愿向中国汽车工业协会和国家
计算机网络应急技术处理协调中心送检的汽
车。

检测对象：截至**2025年5月8日前**，
按照《关于组织开展数据安全合规
车型测评活动的通知》，汽车制造商
愿向中国汽车工业协会、国家计算
网络应急技术处理协调中心、**中国
息通信研究院、国家工业信息安全
发展研究中心**等送检的汽车。

检测标准：检测采用相同的测试要求、测试环境、技术标准和测试流程，包括车外人脸信息等匿名化处理、座舱数据不出车、座舱数据默认不收集以及处理个人信息显著告知**4项要求**。检测标准如下：

检测标准：检测采用相同的测试要求、测试环境、技术标准和测试流程，包括车外人脸信息等匿名化处理、座舱数据车内处理、默认不收集座舱数据、处理个人信息显著告知及精度范围适用**5项要求**。检测标准如下：

1. 车外人脸信息等匿名化处理要求

a. 车外数据未完成匿名化处理前，不应向车外提供；

无变化

b. 车端匿名化处理的视频、图像中的人脸目标和汽车号牌目标的匿名化检出率均应大于或等于90%。

2. 座舱数据车内处理要求

2. 座舱数据不出车要求

a. 通过摄像头、红外传感器、指纹传感器和传声器从汽车座舱采集包含个人信息的数据，以及对其进行加工后产生的数据应取得个人信息主体同意后向车外提供；

a. **为实现语音识别功能以实时判断汽车控制指令，需要将语音指令数据在车外处理的功能，应取得个人信息主体同意，功能实现后即时删除原始数据及处理结果；**

b. 为远程查看、云存储等功能，向使用者提供数据，应取得个人同意、限制他人访问并采取安全措施；

b. 为远程查看、云存储等功能，向使用者提供数据，应取得个人同意、限制他人访问并采取安全措施；

c. 在选定的测评环境中测试车辆不应直接向境外传输个人信息。

c. **在选定的测评环境中测试车辆不应向车外提供其他座舱数据；**

d. 在选定的测评环境中测试车辆不应直接向境外传输个人信息等数据。

3. 默认不收集座舱数据要求

a. 除非驾驶人自主设定，车辆应默认设定为**不收集个人信息**的状态；

b. **处理个人信息应取得个人同意**，处理敏感个人信息应取得单独同意

c. **提供自主设定处理敏感个人信息同意期限的途径，具备同意和拒绝的方式**，且期限不应设置为始终允许或永久；

d. **应提供撤回个人同意的途径；**

e. **撤回个人同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力；**

f. 在保证行车安全以及人身安全的情况下，驾驶人选择终止收集座舱内图像/视频数据后，应关闭车内摄像头收集座舱内图像 / 视频数据的部件；

g. **应具有删除车端存储的座舱数据的途径；**

h. **汽车数据处理者处理敏感个人信息，个人要求删除的，汽车数据处理者应当在十个工作日内删除。**

3. 座舱数据默认不收集要求

a. 除非驾驶人自主设定，汽车应默认设定为**不收集座舱数据**的状态；

b. 汽车数据处理者应提供便利的终止收集座舱数据的方式；

c. 在保证行车安全以及人身安全的情况下，驾驶人选择终止收集后，应关闭车内传声器和摄像头等收集座舱数据的部件；

d. 处理敏感个人信息时，应对每项敏感个人信息取得个人信息主体单独同意；

e. 取得敏感个人信息主体单独同意时，处理敏感个人信息的同意期限不应为“永久”或“始终允许”。

4. 处理个人信息显著告知要求

a. 取得个人同意时，应通过至少一种显著方式向个人告知。处理个人信息的种类、处理各类个人信息的必要性，包括目的、用途、方式等；

b. 应使用清晰易懂的文字向个人信息主体说明收集个人信息的具体情境和必要性；

c. 应向个人信息主体告知各类型个人信息的

保存期限，应具体且明确，例如30天或1年等，或保存期限的规则；

(2)汽车数据处理者持续收集敏感个人信息需通过车载显示面板图标或信号装置指示灯的闪烁或长亮等方式提示收集状态，提示方式应根据信息类型的不同做到差异明显且清晰易懂。

d. 应向个人信息主体告知其个人信息保存地点，应将保存地点位置精确到地级市并告知所有保存地点，或明确的保存地点规则；

e. 应为个人信息主体提供便捷的查阅、复制和删除等个人信息管理功能；个人信息管理功能应为交互式，且其功能入口应处于个人信息主体容易察觉的显著位置；

f. 应设置用户权益事务联系人，并对外告知准确有效的姓名和联系方式，联系方式包括电话号码、邮箱地址、网址或即时通信平台账号等；不便对外告知真实姓名的，应告知长期且固定使用的别名。

5.精度范围适用要求

a.收集个人信息时，汽车数据处理器应根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率；

b.因同一数据收集设备支持多个功能服务且所需数据精度要求不同时，至少应有一个功能服务符合精度适用要求，对不符合精度适用要求的功能应做出合理说明。

检测方法：针对不同车型（区分年款）的各项数据处理功能，在相同的标准下进行**4项合规要求**的检测，并根据相关功能的技术特点采取不同的检测方法。具体包括：

1.车外人脸信息等匿名化处理的检测方法：企业提供第三方测试机构出具的车端匿名化报告，由技术人员从车端进行数据采样，并进行匿名化效果分析和报告审核确认；

2.座舱数据不出车的检测方法：在车端进行车辆对外通信数据的抓取和分析；

3.座舱数据默认不收集的检测方法：在车内进行各项座舱数据收集功能的符合性确认；

4.处理个人信息显著告知的检测方法：在企业官方网站、车载应用程序或移动通信终端应用程序上进行《用户隐私协议》或其他告知方式内容的符合性确认。

检测方法：针对不同车型（区分年款）的各项数据处理功能，在相同标准下进行**5项合规要求**的检测，并根据相关功能的技术特点采取不同的检测方法。具体包括：

1.车外人脸信息等匿名化处理的检测方法：企业提供第三方测试机构出具的车端匿名化报告，由技术人员从车端进行数据采样，并进行匿名化效果分析。

无变化

无变化

无变化

5.精度范围适用的检测方法：企业应提供功能清单及相关技术资料，技术人员对功能及技术资料进行功能性确认。

海问评述：

检测标准的变化反映了监管逻辑由“框架性合规”向“全流程细节合规”转变。具体而言：

A. 细化座舱数据处理要求：“原则上车内处理+特定场景例外”规则延续

新增语音指令数据车外处理规则，明确了智能座舱语音控制功能的合规义务——要求车外处理需个人同意，功能实现后即时删除原始数据及处理结果。新增禁止测试车辆“向车外提供其他座舱数据”要求，扩大了管控范围（如座舱内环境数据、驾驶人操作习惯数据等）。

上述场景，一方面呼应了越来越多大模型“上车”场景的监管关注。大模型“上车”最高频触发的使用增强场景，是强化了智能座舱内部乘客语音交互理解的准确性和丰富度。

这也给究竟是进行“车内”数据处理还是“车外”数据处理带来一定难题。大模型需要一定算力，较多场景当中以数据中心云端统一处理并回传作为主要手段，本次明确车外处理的合规路径方案，有利于助推大模型在智舱内的广泛应用，促进智能场景协同发力。

针对上述要求，企业需要关注在技术层面设置“自动删除触发机制”并留存删除记录。同时企业需要关注梳理“座舱数据清单”，明确哪些数据属于“不应向车外提供”的范畴。

B. 细化默认不收集座舱数据的要求：明确用户同意与数据删除义务

将车辆默认设定为不收集“座舱数据”收缩至默认不收集“个人信息”，清晰界定了管控范

围，突出保护个人信息权益。

此外，在个人信息主体行权响应方面，与《个人信息保护法》的要求对齐，明确个人有权撤回同意，撤回不影响撤回前的个人信息合法处理，新增企业需提供落实敏感个人信息同意期限禁止“始终允许/永久”的途径。

此外，进一步与《汽车数据安全若干规定（试行）》要求对齐，新增企业需提供车端数据删除途径，汽车数据处理者还需落实敏感个人信息10个工作日删除时限要求。

C. 细化“处理个人信息显著告知”要求：保障用户知情权

新增敏感个人信息收集状态提示要求，要求通过车载显示面板图标或信号装置指示灯的闪烁或长亮等方式实时提示收集状态（如麦克风开启时亮灯），符合个人信息处理的公开、透明原则，建议企业在技术层面增设相关状态提示功能。

D. 新增“精度范围适用”要求：避免过度收集

要求摄像头、雷达等设备的覆盖范围、分辨率匹配“功能服务对数据精度的要求”，且当同一设备支持多功能时，至少1项功能符合精度要求，不符合的功能需“合理说明”。

该要求符合《汽车数据安全若干规定（试行）》的精度范围适用原则，建议企业针对每一项数据收集设备展示“功能—数据精度匹配说明”。

3、手机端APP和小程序的个人信息保护：合规关注依旧涵盖汽车行业

2025年8月5日，上海市通信管理局发布关于侵害用户权益行为移动应用（“APP”）和小程序的通报。[IV]其中，涉及汽车零部件公司、汽车销售公司等运营的APP和小程序，所涉问题包括违规收集个人信息、未明示个人信息处理规则、超范围收集个人信息和账号注销难。

海问评述：

目前，汽车企业越来越多地通过APP和小程序为用户提供服务，如车辆远程控制、售后服务预约、汽车资讯推送等，收集了大量用户的个人信息，包括姓名、联系方式、车辆识别码、行驶轨迹等。

上述场景收集的个人信息类型相对敏感，使用场景和目的相对重要。在部分提供车控功能的APP中，APP功能甚至可能成为第三方非法获得车辆控制权的媒介。在部分二手车交易环节，新旧车主也可能因为车控、历史记录等信息，产生个人信息不当交互甚至泄露，进而产生针对主机厂的客诉，影响用户体验和个人信息安全。

因此，企业在处理个人信息前，需要特别关注以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息的处理目的、处理方式，处理的个人信息种类、保存期限等事项；遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；提供账号注销渠道等，保障个人信息主体行权通畅。

4、APP违法违规收集个人信息监管行动：继续关注车载应用

国家计算机病毒应急处理中心于2025年8月13日发布《国家计算机病毒应急处理中心检测发现70款违法违规收集使用个人信息的移动应用》，检测发现70款APP存在违法违规收集

使用个人信息情况[V]。其中再度提及部分车端应用存在违法违规收集使用个人信息的情形。

海问评述：

A. 监管对“车端”形成常态化关注

在过去多年的APP违法违规收集个人信息执法活动中，监管部门几乎很少关注车端应用本身的个人信息保护问题。即使监管对一些主机厂的应用进行过检测、提出过批评或者通报，也集中在主机厂的手机端APP。

今年以来，在多批APP违法违规收集个人信息的通报中，提及车端应用，既涉及预装应用，也涉及通过车载应用市场下载的应用。

在智能网联车场景下，车端应用也通过移动网络（4G、5G等）连接和提供服务。相当一部分应用的核心运营内容以及对个人信息的处理方式与手机端高度相似，只是在交互逻辑、车端操作体验和行车安全性方面进行适配修改。

因此，对于个人信息保护和数据安全方面而言，车端应用的底层监管关注与手机端不应存在本质区别。主机厂和智能网联服务提供商应当更加关注车机端应用在个人信息保护方面的合规性，对标手机APP、小程序的个人信息保护实践标准，提升告知的透明度，获得用户的适当同意，在个人信息处理的一些细节方面严格对照监管要求，进行优化或整改。

B. 车端应用个人信息处理常见问题

本次通报主要涉及的合规问题如下：

合规问题一：

多款车机预装APP以及车机应用商店中的APP无隐私政策。经过多年APP违法违规收集个人信息的整改，目前手机端相当大部分主流APP以及小程序标配隐私政策，且大多可以实现单独成文。完全缺失隐私政策的情形在手机端越来越少。

但是，相当一部分场景的车机应用往往针对车机操作习惯进行修改，一部分主机厂也往往要求CP（内容供应方和服务方）针对具体车型做专门适配。在此开发过程中，由于过往对车机应用的个人信息保护合规重视力度不够，一些开发修改过程可能忽略对于隐私政策的适当纳入、放置，忽略适当的隐私政策弹窗及取得同意设计，最终导致个人信息保护方面存在严重瑕疵（例如完全缺失隐私政策等情况）。

合规问题二：

车机端APP在APP首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；以默认选择同意隐私政策等非明示方式征求用户同意；隐私政策难以访问；个人信息处理者在处理个人信息前，未以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理者的名称或者姓名、联系方式、个人信息的保存期限等。

该问题的出现与上述“合规问题一”提及的开发流程和定制也存在关系。由于一些车机端应用需要针对车端环境（甚至具体车型）进行适配修改，修改过程中没有充分重视个人信息保护功能和流程的设置，导致例如“未通过弹窗等明显方式提示用户阅读隐私政策”这类明显的合规瑕疵出现。

5、自动驾驶伦理指引：不同阶段的企业责任

2025年7月23日，国家科学技术部公布由国家科技伦理委员会人工智能伦理分委员会研究编制的《驾驶自动化技术研发伦理指引》（“[《指引》](#)”）[VI]，在《汽车驾驶自动化分级》（GB/T 40429-2021）的既有分级基础上强化伦理规范要求。

《指引》提出了以人为本、增进福祉，安全优先、尊重生命，公平公正、避免偏见，知情保障、信息公开的基本原则，明确驾驶自动化技术的研究开发和应用需做到**合法合规、效益提升、控制风险、及时调整、保护隐私**五大要求。

《指引》将驾驶自动化技术类型化，分为先进驾驶辅助阶段（2级及以下的驾驶自动化，包括“应急辅助”“部分驾驶辅助”和“组合驾驶辅助”）；有限制阶段的自动驾驶（3级和4级驾驶自动化，包括“有条件自动驾驶”“高度自动驾驶”）；无限制阶段的自动驾驶（5级的驾驶自动化，即“完全自动驾驶”），并相应提出伦理规范要求。

对于先进驾驶辅助阶段，驾驶自动化系统在有限制的设计运行范围内发挥辅助作用，责任主体立伦理审查机制要求。

对于有限制阶段的自动驾驶，责任主体因具体运行场景而异。当自动驾驶系统作为自动驾驶系统生产商、自动驾驶汽车权利人、自动驾驶系统用户，下同）清晰追责。本阶段除需遵循前两个阶段的要求之外，《指引》提出企业还需决策行为可追溯审查、行车策略变更主动告知用户、决策逻辑体现普遍社会认同、避免决策

对于无限制阶段的自动驾驶，除非特殊情况下有用户主动介入操作，否则无限制阶段自动驾驶系统责任主体或法人主体清晰追责。本阶段除需遵循前两个阶段的要求之外，《指引》提出企业还需及时干预。

《指引》作为国家科技伦理委员会主导的规范，后续可能转化为监管依据。建议企业在研发、生产、销售、运维全链条嵌入伦理规范，提前布局合规。

[I] 参见

https://www.samr.gov.cn:3030/hd/zjdc/art/2025/art_a0f9b1ebf0894a5ea1eb5260c

[II] 参见 http://www.caam.org.cn/chn/1/cate_3/con_5236838.html。

[III] 参见 http://www.caam.org.cn/search/con_5236617.html。

[IV] 参见 <https://mp.weixin.qq.com/s/UsNF45FRAPt9ape5Zv8D4A>。

[V] 参见：<https://www.cverc.org.cn/zxdt/report20250813.htm>。

[VI] 参见 https://www.most.gov.cn/kjbgz/202507/t20250723_194082.html。

2025-09-12