解读《汽车数据安全管理规定》

作者：潘永建 | 杨迅 | 杨坚琪 | 沙莎

智能网联时代，汽车可以全方位收集车内、车外数据，不仅包括车内驾驶人、乘车人的个人信息，还涉及敏感区域周边地理环境等可能关系国家安全的重要数据。此前，智能汽车行业已发生多起个人信息安全事件，如 2018 年 2 月，某德国品牌车日本分公司的个人数据服务器受到多次攻击，导致超过 28,700 个客户电子邮件地址被泄露。这一背景也激发了智能汽车行业法律监管与技术监督的迫切需求。

自 2021 年 4 月起，工信部、全国信息安全标准化技术委员会等部门陆续发布了汽车行业数据保护相关法律法规、国家标准、行业标准或该等规定的征求意见稿。2021 年 8 月 20 日，《汽车数据安全管理若干规定(试行)》(“**《汽车数据规定》**”)公布，正式落地对于汽车数据的保护要求，并将于 2021 年 10 月 1 日正式生效。本文从最新发布的《汽车数据规定》出发，试图探索中国政府对于汽车行业数据的监管逻辑。

1. 汽车数据中的“个人信息”和“重要数据”

根据数据关联性的区分，通常的汽车数据可以分为两类：一类是关于车辆本身的数据，如各传统部件的数据、自动驾驶软硬件数据以及车辆外部的数据等；另一类是与行车人相关的个人信息，如驾驶人的身份信息、使用车辆产生的行为数据、人脸和语音数据等。《汽车数据规定》则继承《网络安全法》和《数据安全法》的精神，划分出汽车行业的“个人信息”和“重要数据”，并根据其敏感性采取不同的分类监管措施。结合近期发布的《车联网信息服务 数据安全技术要求》和《车联网信息服务 用户个人信息保护要求》，我们整理了如下监管视角下不同类型的汽车数据：

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

汽车相关数据		个人信息	
一般数据	车牌号、车辆型号、车辆平均行驶速度、年行驶里程、路面情况(是否完好、湿滑)、道路拥堵情况、车载娱乐系统使用行为数据等	一般个人信息	电话号码、邮箱、车辆防碰撞预警服务中的个人信息、红绿灯车速引导过程中的个人信息
重要数据	(1) 重要敏感区域的地理和人流车流数据 (2) 反映经济运行情况的数据 (3) 汽车充电网的运行数据 (4) 包含人脸、车牌等的车外视频、图像数据 (5) 涉及个人信息主体超过 10 万人的个人信息 (6) 其他	敏感个人信息	(1) 个人生物识别信息：指纹、人脸、声纹、心律、虹膜、脸谱 (2) 个人身份信息：身份证、驾驶证、社保卡 (3) 车辆位置、行踪轨迹 (4) 驾驶人或乘车人音视频等 (5) 车联网交易类：交易账号和密码、交易记录

值得注意的是，《汽车数据规定》是目前生效的中国法律中，**第一次(也是目前的唯一一次)对特定行业中的"重要数据"进行定义，并随之激活了不同法律下对"重要数据"的保护要求，值得引起各行各界的重视**。《汽车数据规定》的颁布实际上也体现了《数据安全法》下由各行业主管部门制定相应的"重要数据"清单的要求。

就"重要数据"的范围，《汽车数据规定》对此前发布的征求意见稿进行了几处修改：

(1) 增加包含"人脸、车牌信息的图像数据"，删除"音频数据"；
(2) 增加"重要敏感区域的地理信息"，删除了"高于国家公开发布地图精度的测绘数据" (但实际上测绘数据仍然可能受到其他法律的限制)；
(3) 增加"涉及个人信息主体超过 10 万人的个人信息" (这与 2019 年颁布的《数据安全管理办法(征求意见稿)》中的规定相左，**同样值得其他行业的企业关注**)；
(4) 将"车辆类型、车辆流量数据"修改为"车流、物流等反映经济运行情况的数据"；
(5) 明确发展改革、工业和信息化、公安、交通运输等有关部门可以另行确定"重要数据"类型。

从以上修订可以看出，正式生效的《汽车数据规定》对"重要数据"的界定更为严谨：例如，对个人信息的保护予以量化；删除实践中可能无法识别到个人信息主体的声音数据等。**但更为重要的是，《汽车数据规定》对汽车行业的"重要数据"的认定方式对于其他行业的数据处理者亦有重要的参考意义。**

2. 数据保护主体

在智能网联行业中，能够收集、使用、存储、利用、共享、运维汽车数据的主体类型多样，收集情况亦各有不同。为了保证数据处理的安全性，《汽车数据规定》明确要求汽车数据的处理者以"合法、正当、具体、明确"的方式处理个人信息。在正式生效的《汽车数据规定》下，履行数据保护义务的

主体为“汽车数据处理者”，包括汽车厂商/汽车制造商、零部件供应商、第三方供应商、经销商、维修机构以及出行服务机构。从“汽车数据处理者”的范围来看，正式生效的《汽车数据规定》与此前的征求意见稿差异不大，但是将保险公司排除在了“汽车数据处理者”的范围之外，这可能是不同监管部门之间的执法协调安排后的结果。

尽管“保险机构”自正式生效的《汽车数据规定》中删除，但是《汽车数据规定》下的适用主体仍然非常宽泛：无论是“硬件工程”方面的传统整车厂企业和 Tier-1 的供应商，还是智能网联时代新兴玩家的“软件工程”服务商，亦或是销售环节的经销商，以及面向终端用户的应用程序开发者，只要其处理的数据落入了《汽车数据规定》的范围之内，就需要履行《汽车数据规定》下的数据保护义务。

3. 处理“个人信息”与“重要数据”的基本要求

如前所述，《汽车数据规定》适用范围广泛：其不仅规范与车主、司机相关的数据和个人信息，还要求对乘客甚至行人相关的数据和个人信息进行保护，这一规定符合我国当前对个人信息和重要数据保护加强监管的趋势；而另一方面，《汽车数据规定》也明确了在汽车行业内被认为属于可能影响国家安全和重大社会利益的“重要数据”的范围，给予从业者明确的指引。根据《汽车数据规定》，汽车数据处理者处理“个人信息”与“重要数据”，应当符合以下要求：

(1) 基本原则

《汽车数据规定》“倡导”汽车数据处理者处理个人信息以及重要数据需要符合“车内处理”“默认不收集”“脱敏处理”“精度范围适用”四项非强制性原则，这反映了监管部门对于汽车数据处理者的合理期待。

第一，《汽车数据规定》的“车内处理”原则和“脱敏处理”原则对数据处理的空间范围和对外提供均提出要求。此前的征求意见稿规定下的“车内处理原则”和“匿名化处理原则”(在正式生效的《汽车数据规定》中变更为“脱敏处理”原则)要求处理者除非确有必要不向车外提供(“车内处理原则”)；确有必要向车外提供的，需要应尽可能采取匿名化和脱敏处理(“匿名化处理原则”)。正式生效的《汽车数据规定》则在“脱敏原则下”**删除了“确有必要向车外提供”**这一表述，并统一要求所有的汽车数据处理场景，均应当“尽可能采用匿名化和去标识化处理”，而不再仅仅局限于“向车外提供这一场景”。这一修订体现了监管部门更为严格的执法目标，即通过强化“脱敏处理”要求，实现数据主体不被识别或关联这一最终目的，并以此保护汽车行业数据(尤其是车内外收集的个人信息)的安全。

“精度范围适用”是 “最小必要原则”在信息收集精度要求方面的体现。智能网联汽车搭载的摄像头和雷达通常可以收集不同类型的数据：车载摄像头可能收集的信息包括交通信号灯的状态、行人的位置和移动路线以及行车过程中的各类障碍，而汽车雷达则需要对盲点监测、紧急刹车、前后防撞等作出反应，因此需要收集的信息中就含有诸如面部信息等个人敏感信息，以及车外

视频、敏感地区人流车流等重要数据。因此，汽车数据处理者有必要根据具体的服务场景，对数据收集的颗粒度进行划分。

《汽车数据规定》在“默认不收集”原则方面也对征求意见稿进行了修订。征求意见稿曾对运营者获取驾驶人的授权提出了较高的要求：无论是智能汽车被临时使用，还是长期使用，处理者必须在每次处理个人信息和重要数据前，获得驾驶人的同意。这一规定在很大程度上同时加重了汽车数据处理者和驾驶人的负担：例如，在临时停车的场景下，同一驾驶人可能需要在短时间内进行多次授权。而修订后的《汽车数据规定》则调整了权利授予的范式，即“**除非驾驶人自主设定**，每次驾驶时默认设定为不收集状态”，取消了征求意见稿中“确有必要下可以默认设定为收集状态”的可能性。将“默认收集”的权利配置将选择权交还给驾驶人，则意味着汽车数据处理者需要结合自身的服务场景设置适当的授权机制，以满足现有法律的要求。

值得注意的是，《汽车数据规定》删除了《征求意见稿》曾经提出的“最小保存期限”的原则。我们理解，由于征求意见稿本身并未对服务场景、以及各类服务场景对应的数据存储期限进行界定，还需后续的细化规定或标准出台予以澄清，因此删除“最小保存期限”也存在一定的合理性。实际上，我们同样注意到《汽车数据规定》在“履行个人信息处理告知义务”、“重要数据的风险评估报告”“重要数据安全管理制度”和“跨境提供个人信息和重要数据”四个场景下要求企业自行提供或说明数据保存期限的情况，借此“间接地”要求企业自身判断数据储存期限的合理性。

(2) 知情同意

在个人信息收集方面，《汽车数据规定》继承了《民法典》《网络安全法》以及《个人信息保护法》下的“告知同意”要求，即：汽车数据处理者收集个人信息，应当取得被收集人的同意，但法律法规规定不需要取得个人同意的除外。需要注意的是，即便是在不需要取得个人同意的“法律法规规定的例外”场景下，汽车数据处理者仍应当对收集个人信息的行为进行告知(即纳入到诸如隐私政策等文件中)，并采取相应的保护措施。以车联网卡实名登记为例，2021 年 6 月，工信部公布《关于加强车联网卡实名登记管理的通知(征求意见稿)》，要求车辆厂商在售前、售中、售后建立车联网卡采购、使用、实名登记等管理制度，并需要将登记和核验的用户实名信息、车联网卡号码或识别码传送给相应的电信企业，由电信企业进行查验和登记，否则将按照《网络安全法》第 61 条的规定承担法律责任。该等用户实名信息、车联网卡号码构成可以识别特定自然人的个人信息， 但该等个人信息是法律法规要求的取得车联网卡前必须提供的信息，因此不属于必须征得个人信息主体同意才能收集的信息，但是汽车生产企业仍应当在用户购买车辆时就其收集其个人信息的情况进行告知，并通过技术或其他必要措施对收集的个人信息严格保密。

结合智能网联汽车的特点，《汽车数据规定》在知情同意原则的基础上，特别提到采集到的车外音视频信息(尤其是车外个人信息)应当进行匿名化或者脱敏处理。实践中，自动驾驶、自动刹车、自动泊车等功能的实现都需要通过车载摄像头、激光雷达等传感器实时收集车辆外部的各类数据，包括车外行人的音视频信息，车辆收集此类个人信息难以取得个人信息主体的同意，在此类场景下，通过匿名化处理则能够有效地防止特定个人信息主体被识别，降低数据泄露给个人

信息主体带来的风险。在《汽车数据规定》正式生效后，对于可能收集到车外行人数据的汽车数据处理者而言，如何从技术手段上满足“匿名化处理”要求则是当务之急。

(3) 目的限制

依据个人信息的敏感性，《汽车数据规定》还特别针对不同的数据类型提出**处理目的限制，**实际上也是**中国法律首次在法律层面对于个人信息处理的目的限制进行直接规定**:

数据类型	目的限制
敏感个人信息	直接服务于驾驶人或者乘车人为目的，包括增强行车安全、辅助驾驶、导航等
个人生物识别信息	除敏感个人信息的目的限制外，还应当限定在方便用户使用、增加车辆电子和信息系统安全性

在敏感个人信息方面，生效版的《汽车数据规定》删除了“娱乐”这一目的；在个人生物识别信息方面，生效版的《汽车数据规定》删除了“方便用户使用”这一目的，同时将“增加车辆电子和信息系统安全性”修改为“增强行车安全的目的和充分的必要性”。在此前的征求意见稿中，无论是“直接服务于驾驶人或乘车人”还是“方便用户使用”，其涵盖的范围可以十分广泛，《汽车数据规定》对征求意见稿的修订将企业获取敏感个人信息以及生物识别信息的场景进一步限缩，增强了对该等类型个人信息的保护。

(4) 敏感个人信息删除要求

《汽车数据规定》将征求意见稿中的“驾驶人要求处理者删除时，处理者在 2 周内删除敏感个人信息和用于判断违法违规驾驶数据”的要求，修改为“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”。这一规定延续了征求意见稿所确认的驾驶人的删除权，对那些与人身、财产安全密切相关的个人信息和数据，予以更为严格的保护。

就这一修订而言，尽管《汽车数据规定》删除了“用于判断违法违规”的数据类型，但仍然存在以下问题：第一，对于法律法规要求保留的敏感个人信息，例如与国家安全直接相关，或者与刑事侦查起诉和审判直接相关的数据等，汽车数据处理者不宜将该等数据删除；第二，实践中，汽车数据处理者可能以分布式存储的方式存储海量数据，汽车数据处理者可能难以在十个工作日内删除该等数据并进行确认，还可能使汽车数据处理者付出高额的经营成本；第三，按照《汽车数据规定》，汽车数据处理者应当根据驾驶人的要求无条件删除数据，但如果数据已被匿名化处理，则该等数据无法识别或关联到特定的信息主体，因此，即便汽车数据处理者不删除该等数据，也不会导致个人信息主体的权利受到侵害，从这一角度看，汽车数据处理者无需按照驾驶人的要求删除数据。

(5) 境外传输要求

根据《汽车数据规定》的要求，个人信息和重要数据应当存储在境内，境外传输则需要通过国家网信部门组织的数据出境安全评估。《汽车数据规定》无疑对汽车行业个人信息和重要数据的出境提出更为严苛的要求。

此前，《网络安全法》《数据安全法》仅要求关键信息基础设施处理者(CIIO)对重要数据进行出境时进行安全评估，CIIO 是指"一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等"的处理者，显然，并非汽车行业的所有数据处理者都属于 CIIO，在上位法已经明确仅有 CIIO 适用政府部门组织的安全评估的情形下，《汽车数据规定》第 12 条规定的合法性有待商榷。不过，2021 年 5 月颁布的《信息安全技术 网联汽车 采集数据的安全要求(征)》则规定"网联汽车通过摄像头、雷达等传感器从车外环境采集的道路、建筑、地形、交通参与者等数据，以及车辆位置、轨迹相关数据，不得出境"，进一步细化了不得出境数据的范围，值得汽车数据处理者关注。

《汽车数据规定》要求，向境外传输重要数据的，同样应当向省级网信部门等有关部门进行报告，这一要求也可结合"数据安全审查"制度综合理解。《数据安全法》规定，"国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查"，尽管目前尚未有"影响或可能影响国家安全"的判断标准和判断依据，但汽车数据处理者的业务中如果涉及处理大量的个人信息和重要数据，并将该等数据进行境外传输，则应当密切关注后续出台的配套法规，以判断自身是否可能落入被审查的范围。

稍早于《个人信息保护法》发布的《汽车数据规定》，其更为重要的意义在于首次界定了特定行业内的"重要数据"范围，使得《网络安全法》《关键信息基础设施保护条例》以及《数据安全法》下对于"重要数据"的保护义务得以激活。更为重要的是，汽车数据处理者如何履行诸如"重要数据"的风险评估、出境安全评估等要求，将对于其他行业的从业者具有极大的参考意义。从这个角度而言，中国政府对于重要数据"数据安全"的真正执法实践，很有可能始于《汽车数据规定》的颁布。

结语

作为《数据安全法》颁布后首部在细分行业制定的部门规章，《汽车数据规定》对汽车行业的个人信息与重要数据的界定、处理与保护设立了审慎且具有开创性的制度，有助于在数据领域为我国快速发展的汽车业(尤其是新能源车和车联网等)提供有效的制度保障。然而，囿于上位法某些制度的付诸阙如，《汽车数据规定》仍有诸多未决问题。例如，车辆产生的个人信息与重要数据究竟归属于车辆所有人、驾驶人、整车厂商、电机电池等部件生产商、抑或是经销商等?基于前一问题的答案，在汽车数据发生泄漏、篡改、毁损、丢失等安全事件情形下，哪一(几)方又该对另一(几)方承担责任?我们希望，随着行业与执法实践的发展，《汽车数据规定》未来的修订版对上述问题做出回应。

如您希望就相关问题进一步交流，请联系：

潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

杨 迅
+86 21 3135 8799
xun.yang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市建国门北大街 8 号 华润大厦 4 楼 T: +86 10 8519 2266 F: +86 10 8519 2929	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	伦敦	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野