**汽车数据保护监管趋严，管理新规恰逢其时**

杨洪泉、陈扬

**前言**

2021年5月12日，国家互联网信息办公室发布《汽车数据安全管理若干规定》并向社会公开征求意见，意见反馈截止时间为2021年6月11日。本文详细解读了该规定出台的背景、具体要求以及对相关企业的影响。

《征求意见稿》总体上是一部较为严格的规定，对于汽车产业链中的各企业、以及收集和处理与汽车场景相关数据的其他企业而言，《征求意见稿》提出了较高的合规要求，这些合规要求不但需要在法律文件层面（例如隐私政策、用户协议、内部管理制度）落实，还需要在数据管理体系和技术实现方式层面（例如车内显示屏展示告知内容、匿名化或脱敏处理敏感信息、向车主提供结构化的数据查询结果）进行落实。虽然在正式出台之前《征求意见稿》仍会进一步修改和完善，但结合最近公布的《个保法二审稿》、《数安法二审稿》以及相关国家标准的征求意见稿，我们倾向于认为《征求意见稿》的规定基本符合我国最近数据立法/标准所体现的各项原则，集中反映了相关立法部门对汽车领域数据保护问题的态度，《汽车数据安全管理若干规定》正式稿的内容可能不会偏离《征求意见稿》太多。我们建议相关企业仔细分析《征求意见稿》的具体要求，并对企业现有数据合规实践进行梳理和差距分析，及时开展合规工作。

《征求意见稿》针对汽车领域的个人信息和重要数据处理活动提出一系列的合规要求，但其中的一些要求实际上在此前已发布的法律法规和相关文件（包括征求意见稿）中已有类似规定。相关企业在开展数据合规工作中不仅要考虑如何落实《征求意见稿》中的要求，还需要考虑这些要求与已发布的法律法规和相关文件（包括征求意见稿）的衔接问题。

**一、背景**

对于汽车行业的数据合规从业者而言，2021年是特殊的一年。一方面，《数据安全法》和《个人信息保护法》二审稿公布，汽车行业作为收集和使用个人信息和其他数据的“大户”，无疑将受到较大影响；而另一方面，监管部门针对汽车行业也专门发布多个文件，在规范智能网联汽车道路测试、产品准入等问题的同时，也试图规范智能网联汽车的数据收集和使用行为：

**2021年1月**，工业和信息化部（“**工信部**”）发布《智能网联汽车道路测试与示范应用管理规范（试行）》（征求意见稿）（“《**管理规范**》”），向社会征求意见。《管理规范》对智能网联汽车道路测试与示范应用进行规范，其中要求道路测试车辆、示范应用车辆应当具备车辆状态记录、存储及在线监控功能，能实时回传相关信息，自动记录和存储相关数据；

**2021年4月**，工信部发布《智能网联汽车生产企业及产品准入管理指南（试行）》（征求意见稿）（“《**管理指南**》”），向社会征求意见。《管理指南》对具备有条件自动驾驶、高度自动驾驶功能的智能网联汽车生产企业和其产品提出了包括数据本地存储在内的合规要求；

**2021年4月**，全国信息安全标准化技术委员会（“**信安标委**”）发布《信息安全技术 网联汽车采集数据的安全要求（草案）》（“**《安全要求》**”）征求意见稿，向社会征求意见。《安全要求》对网联汽车采集数据的各环节（传输、存储、跨境）提出要求。

此外，我国智能电动汽车行业的迅猛发展、特斯拉车主维权等事件也引起了广泛的社会关注，将加强汽车数据监督管理的现实问题拉进大众的视野。

在此背景下，2021年5月12日，国家互联网信息办公室（“**网信办**”）发布《汽车数据安全管理若干规定（征求意见稿）》（“**《征求意见稿》**”），向社会公开征求意见。我们倾向于认为，这些规定被称为“若干规定”的原因可能在于：一，对于《数据安全法》和《个人信息保护法》已有的、且可普遍适用于各个行业的规定，《征求意见稿》不宜再进行全面照搬或重复；二，国家虽已出台与智能网联汽车相关的多个文件，但仍缺乏对于汽车领域数据合规更为详细、具体的规范；三，智能网联汽车仍属于新生事物，社会大众以及监管部门对于汽车相关场景下的数据保护及合理利用的边界仍有一个逐步认识的过程，现阶段还不宜对这类问题制定一个更加全面和系统的规范。在此背景下，《征求意见稿》以“若干规定”的方式，对汽车行业个人信息和重要数据保护提出一些普遍性原则和具体要求，可能是更为合适的做法。

**二 、适用范围**

《征求意见稿》第二条规定：“运营者在中华人民共和国境内设计、生产、销售、运维、管理汽车过程中，收集、分析、存储、传输、查询、利用、删除以及向境外提供（以下统称处理）个人信息或重要数据，应当遵守相关法律法规和本规定的要求。”我们可以从地域范围、适用主体和适用对象三个角度来理解《征求意见稿》的适用范围。

**1. 地域范围**

《征求意见稿》第二条中对地域范围的界定是“在中华人民共和国境内设计、生产、销售、运维、管理汽车过程中，收集、分析、存储、传输、查询、利用、删除以及向境外提供（以下统称处理）”，由此可见，《征求意见稿》原则上仅约束发生在中华人民共和国境内的个人信息和重要数据的处理行为，而不约束发生在境外的处理活动（对于向境外提供数据的行为，也仅约束出境方在境内的行为）。

这一点和《网络安全法》[1]以及《数据安全管理办法》（征求意见稿）[2]保持了一致，但和《个人信息保护法（草案）（二次审议稿）》（“**《个保法二审稿》**”）和《数据安全法（草案）（二次审议稿）》（“**《数安法二审稿》**”）的规定有所不同。根据《个保法二审稿》，除“组织、个人在中华人民共和国境内处理自然人个人信息的活动”外，如果组织、个人在中华人民共和国境外开展数据处理活动，且有下列情形之一的，也将适用《个保法二审稿》：“（一）以向境内自然人提供产品或者服务为目的；（二）分析、评估境内自然人的行为；（三）法律、行政法规规定的其他情形”。根据《数安法二审稿》，除“在中华人民共和国境内开展数据处理活动及其安全监管”外，对于在中华人民共和国境外开展的数据处理活动，如果“损害中华人民共和国国家安全、公共利益或者公民、组织合法权益”，也可依据该法追究其法律责任。在域外效力问题上，《征求意见稿》与《个保法二审稿》和《数安法二审稿》的相关规定如何衔接，仍有待明确。

**2. 适用主体**

《征求意见稿》第二条对于适用主体的表述为“运营者”，《征求意见稿》第三条对此作出定义：“本规定所称运营者指汽车设计、制造、服务企业或者机构，包括汽车制造商、部件和软件提供者、经销商、维修机构、网约车企业、保险公司等。”

尽管第三条没有说明“运营者”具体运营的对象，但根据上下文，应理解为这些“运营者”运营的是汽车设计、制造、部件和软件提供、经销、维修、网约车、保险等业务（或服务）。需要注意的是，《征求意见稿》明确将“保险公司”也列为“运营者”。但这一点也不难理解，《征求意见稿》旨在对“汽车数据”的安全管理做出规定，其适用对象明确为“个人信息和重要数据”，而保险公司在提供车险等保险服务的过程中也不可避免地会获取大量的个人信息和重要数据，因此也理应属于“运营者”的范畴。以此类推，我们认为，对于《征求意见稿》没有明确列举的其他类型企业或机构，只要其涉及收集和处理汽车设计、生产、销售、运维和管理过程中的个人信息和重要数据，也应受到《征求意见稿》的约束。

**3. 适用对象**

《征求意见稿》第二条明确“个人信息和重要数据”是本《征求意见稿》适用的具体对象。《征求意见稿》第三条对“个人信息”和“重要数据”分别作出定义：

**（1）个人信息**

《征求意见稿》规定，“个人信息包括车主、驾驶人、乘车人、行人等的个人信息，以及能够推断个人身份、描述个人行为等的各种信息。”

《征求意见稿》没有照搬《民法典》[3]、《网络安全法》[4]、《信息安全技术 个人信息安全规范》[5]（“**《个人信息安全规范》**”）、《车联网信息服务 用户个人信息保护要求》[6]和《个保法二审稿》[7]中“个人信息”的现有定义，而是对个人信息进行了自行定义。但以“个人信息”来定义“个人信息”（“个人信息包括车主、驾驶人、乘车人、行人等的个人信息”）似乎有用概念来解释概念的逻辑悖论。此外，“能够推断个人身份、描述个人行为等的各种信息”虽然看起来兼顾了“识别性”和“关联性”这两种“主流”的个人信息认定途径，但在实践中将不可避免地导致个人信息范围扩大化（当然，这也是个人信息定义的老问题了，在此不再赘述。）

**（2）重要数据**

《征求意见稿》规定：“重要数据包括：（一）军事管理区、国防科工等涉及国家秘密的单位、县级以上党政机关等重要敏感区域的人流车流数据；（二）高于国家公开发布地图精度的测绘数据；（三）汽车充电网的运行数据；（四）道路上车辆类型、车辆流量等数据；（五）包含人脸、声音、车牌等的车外音视频数据；（六）国家网信部门和国务院有关部门明确的其他可能影响国家安全、公共利益的数据。”

在《征求意见稿》之前，“重要数据”的定义已经有所规定。2019年网信办发布的《数据安全管理办法（征求意见稿）》（“**《管理办法》**”）[8]和2017年信安标委发布的国家标准《信息安全技术 数据出境安全评估指南（征求意见稿）》[9]都试图对“重要数据”进行定义和列举。但该办法和标准更多是对各行业/领域重要数据特征的一般性概括；而《征求意见稿》则专门针对汽车领域的“重要数据”予以明确。关于《征求意见稿》中的“重要数据”的范围，有两项重要数据类型需要特别予以关注：

(a) 高于国家公开发布地图精度的测绘数据：除本《征求意见稿》中将测绘数据作为重要数据保护以外，测绘数据一直以来都受到测绘相关法律法规的特别保护，例如对于测绘数据的本地化存储要求；[10]

(b) 包含人脸、声音、车牌等的车外音视频数据：此类数据一般属于个人信息，但《征求意见稿》同时也将其作为“重要数据”对待，因此运营者需同时满足处理个人信息和重要数据的双重义务。但这种双重数据属性的界定方法与《管理办法》的规定不符，在《管理办法》下，重要数据“一般不包括企业生产经营和内部管理信息、个人信息等”。在此背景下，值得商榷的问题是：《征求意见稿》对上述数据施加个人信息和重要数据的双重保护是否有必要？是否会加重企业负担？

**（3）特殊类型的个人信息和重要数据**

《征求意见稿》中还提及了以下几种特殊类别的数据，需要予以关注：

(a) 敏感个人信息：包括车辆位置、驾驶人或乘车人音视频等；

(b) 生物特征数据：指纹、声纹、人脸、心律等；

(c) 可以用于判断违法违规驾驶的数据；

(d) 敏感数据：包括重要数据以及车辆位置、生物特征、驾驶人或者乘车人音视频，以及可以用于判断违法违规驾驶的数据等。

与上文的分析类似，此四种特殊类型的数据不能当然地理解为如属于个人信息即不属于重要数据，或反之亦然。特别是对于其中“可以用于判断违法违规驾驶的数据”，可能既包括车外数据（车外音视频数据）也包括车内数据（车速）。根据具体涉及的数据类型，此类数据可能会被认定为既属于个人信息、也属于重要数据。

**三 、数据保护原则**

无论运营者处理的是个人信息还是重要数据，《征求意见稿》对运营者均规定了通用的的数据保护原则。这些原则与《民法典》、《网络安全法》、《个人信息安全规范》、《个保法二审稿》和《数安法二审稿》中的数据保护原则基本一致。具体如下：

（1）处理个人信息或重要数据的目的应当合法、具体、明确，与汽车的设计、制造、服务直接相关：符合合法、正当、必要，目的明确，最小必要等原则；[11]

（2）落实网络安全等级保护制度，加强个人信息和重要数据保护，依法履行网络安全义务：符合制定安全保障制度的相关规定；[12]

此外，《征求意见稿》对汽车数据的数据保护也提出了更为具体的要求，要求运营者处理个人信息和重要数据过程中遵守：（一）车内处理原则，除非确有必要不向车外提供；（二）匿名化处理原则，确有必要向车外提供的，尽可能地进匿名化和脱敏处理；（三）最小保存期限原则，根据所提供功能服务分类型确定数据保存期限；（四）精度范围适用原则，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；（五）默认不收集原则，除非确有必要，每次驾驶时默认为不收集状态，驾驶人的同意授权只对本次驾驶有效。（第六条）

以上第（一）项与《安全要求》的相关规定相符；[13] 第（二）至（五）项均可理解为是对数据处理“最小必要”原则在汽车领域的具体阐述。这些原则也与网信办牵头发布并已于5月1日生效的《常见类型移动互联网应用程序必要个人信息范围规定》的原则相符。

**四、个人信息处理要求**

在《征求意见稿》中，“知情同意”仍是处理汽车领域个人信息的最主要的合法途径。《征求意见稿》规定了有关处理个人信息的告知和同意规则：

1. **一般个人信息**

告知：运营者处理个人信息的，其应当通过用户手册、车载显示面板或其他适当方式向用户进行告知，告知事项包括：负责处理用户权益责任人的有效联系方式；收集数据的类型；收集每种类型数据的触发条件以及停止收集的方法；收集各类型数据的目的、用途；数据保存地点、期限，或者确定保存地点、期限的规则；删除车内、请求删除已经提供给车外的个人信息的方法步骤。（第七条）

同意：运营者收集个人信息应当取得被收集人同意，法律法规规定不需取得个人同意的除外。实践上难以实现的（如通过摄像头收集车外音视频信息），且确需提供的，应当进行匿名化或脱敏处理，包括删除含有能够识别自然人的画面，或对这些画面中的人脸等进行局部轮廓化处理等。（第九条）

如上所述，《征求意见稿》将个人信息主体的知情同意作为处理个人信息的最主要的法律基础。而对于难以获得车外人知情同意等情况，《征求意见稿》亦设置了平衡方法，即运营者可以通过删除能够识别自然人的画面等匿名化方式、或对人脸进行局部轮廓化等脱敏处理方式予以解决。

需要注意的是，有关在车载场景下获取用户知情同意，国家标准《信息安全技术 个人信息告知同意指南（征求意见稿）》（“**《告知同意指南》**”）有专章附录对此作出规定（附录G（资料性附录）车载场景下的告知同意），可供运营者在实践操作中参考。

根据《告知同意指南》，车载场景下选择个人信息处理有关的规则等内容的告知方式时，宜充分考虑车辆驾驶场景的特殊性，依据道路交通安全法律法规、国家及行业标准的相关规定，选择适当的告知方式。《告知同意指南》列举的告知方式有：车辆使用说明书或销售协议、系统控制层面的交互界面和可行设计、与车机互联的移动设备、语音提示方式等。《告知同意指南》强调，在进行告知及与个人信息主体交互时，不宜在行车场景下设置任何可能干扰驾驶的产品方案。

根据《告知同意指南》，在车载场景下选择同意模式的，则宜根据车辆购买者、车辆驾驶员、乘车人的不同特点进行考虑，在可能的情况下，应结合服务场景和个人信息处理活动的特性，采用不同的同意模式。例如，在前期购买车辆时，可向车辆购买者充分、完整的介绍功能、服务及信息收集情况，并可在销售协议设置相关条款，车辆购买者在采购协议签署中完成明示同意；而在个人信息主体驾驶车辆、使用语音交互、人脸识别等功能时，个人信息主体使用服务即可视为其同意个人信息控制者收集其个人信息的行为。

由于《征求意见稿》和《告知同意指南》（征求意见稿）均未正式出台，两部文件中关于设置告知和同意的途径规定仍有可能发生变化，运营者需予以紧密关注。

**2. 敏感个人信息和可以用于判断违法违规驾驶的数据**

根据《征求意见稿》，运营者收集和向车外提供敏感个人信息，包括车辆位置、驾驶人或乘车人音视频等，以及可以用于判断违法违规驾驶的数据等，应当符合以下要求：（一）以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、娱乐等；（二）默认为不收集，每次都应当征得驾驶人同意授权，驾驶结束（驾驶人离开驾驶席）后本次授权自动失效；（三）通过车内显示面板或语音等方式告知驾驶人和乘车人正在收集敏感个人信息；（四）驾驶人能够随时、方便地终止收集；（五）允许车主方便查看、结构化查询被收集的敏感个人信息；（六）驾驶人要求运营者删除时，运营者应当在2周内删除。（第八条）

相较于其他一般个人信息，《征求意见稿》对收集和向车外提供敏感个人信息和可以用于判断违法违规驾驶的数据施加了额外合规义务：其中，应仅限于直接服务于驾驶人或乘车人的要求（最小必要原则[14]）、通过车内显示面板或语音告知正在收集敏感信息（同步告知用户正在收集敏感信息[15]）、驾驶人能够随时、方便地终止收集（撤回同意的便捷性[16]）符合其他法律法规和相关文件规定的对收集使用个人信息/敏感个人信息的合规要求；而授权同意的单次有效性、允许车主方便查看、结构化查询被收集的敏感个人信息、信息删除应当在2周内完成均为《征求意见稿》新设的要求。

《征求意见稿》中对于一般个人信息、敏感个人信息和可以用于判断违法违规驾驶的数据设定的告知及同意的具体方式，为运营者提出较大的合规挑战和技术挑战。

1. **生物特征数据**

《征求意见稿》第十条规定：“仅当为了方便用户使用、增加车辆电子和信息系统安全性等目的，方可收集驾驶人指纹、声纹、人脸、心律等生物特征数据，同时应当提供生物特征的替代方式。”

该规定一方面限定了收集生物特征数据的目的和场景，另一方面要求运营者应当提供不收集生物特征数据的替代方案。但这些规定均不是新要求。目的限定原则一直是个人信息处理所需遵循的基本原则。而关于提供不收集生物特征数据的替代方案，在此前关于人脸信息收集使用的相关标准中亦有说明。[17]《征求意见稿》将此要求从针对人脸信息扩展到范围更加广泛的生物特征数据，也较为符合监管部门对于特殊类别个人信息予以特别保护的原则。

此外，《征求意见稿》还对敏感数据的查询利用作出额外规定。根据《征求意见稿》第十六条，应当严格限制对重要数据以及车辆位置、生物特征、驾驶人或者乘车人音视频，以及可以用于判断违法违规驾驶的数据等敏感数据的查询利用。

**五、重要数据处理要求**

相对于个人信息的合规要求来说，《征求意见稿》下运营者处理重要数据的合规要求较为简单：运营者应提前向省级网信部门和有关部门报告数据类型、规模、范围、保存地点与时限、使用方式，以及是否向第三方提供等。

类似的规定在《管理办法》中也有所体现。根据《管理办法》，网络运营者以经营为目的收集重要数据或个人敏感信息的，应向所在地网信部门备案。备案内容包括收集使用规则，收集使用的目的、规模、方式、范围、类型、期限等，不包括数据内容本身。[18]

**六、数据本地化及出境限制**

《征求意见稿》对数据的本地化和出境管理提出明确要求，包括数据本地存储和数据出境安全评估（第十二条）、国际条约、协议的适用问题（第十二条）、对接收方的管理和监督（第十三条）、响应用户请求（第十四条）、不得超范围向境外提供（第十五条）和政府部门的抽查核验（第十五条）。

其中有关数据本地存储和出境安全评估、对接收方的管理和监督、不得超范围提供的规定实际上是之前出台的若干文件中已经基本达成共识的要求。而针对国际条约和协议的适用、响应用户请求和抽查核验则有以下要点值得注意：

1.关于国际条约和协议的适用问题：《征求意见稿》规定：“我国参与的或者与其他国家和地区、国际组织缔结的条约、协议等如对向境外提供个人信息有明确规定的，适用其规定，我国声明保留的条款除外。”此处需要与《个保法二审稿》和《数安法二审稿》中关于境外司法或执法机构要求提供/调取存储于境内的个人信息/重要数据的规定进行区分。《征求意见稿》所针对的是根据国际条约/协定而向境外不特定主体提供个人信息的情形，因在相关条约或协定中我国已作出明确承诺，故在没有保留条款的情况下，应当适用相关国际条约或协议中的相关规定；而《个保法二审稿》和《数安法二审稿》则具体针对境外司法或执法机构要求提供/调取存储于境内的个人信息/重要数据的情形。在汽车领域的个人信息和重要数据出境的问题上，应理解为《个保法二审稿》、《数安法二审稿》和《征求意见稿》的规定均适用。

2.关于响应用户请求：《征求意见稿》规定，运营者向境外提供个人信息或者重要数据的，应当接受和处理所涉及的用户投诉；造成用户合法权益或公共利益受到损害的，应当依法承担相应责任。此处对于用户投诉的表述较为模糊，仅说明运营者应当接受和处理此类投诉。而根据网信办2019年6月发布的《个人信息出境安全评估办法（征求意见稿）》，网络运营者与个人信息接收者应当签订合同或者其他有法律效力的文件，约定个人信息的出境事宜。且该合同应当明确网络运营者须应请求向接收者转达个人信息主体诉求，包括向接收者索赔；个人信息主体不能从接收者获得赔偿时，先行赔付。[19] 接收者须为个人信息主体提供访问其个人信息的途径，个人信息主体要求更正或者删除其个人信息时，应在合理的代价和时限内予以响应、更正或者删除。[20]与《征求意见稿》的原则性规定相比，《个人信息出境安全评估办法（征求意见稿）》的规定则更为具体，运营者需予以额外关注。

3.关于抽查核验：《征求意见稿》规定，国家网信部门会同国务院有关部门可以抽查方式核验运营者向境外提供个人信息或重要数据的类型、范围等，运营者应当以明文、可读方式予以展示。《安全要求》中亦有类似的规定：“网联汽车通过加密方式跨境传输数据的，当监管部门开展抽查验证时，应提供传输的数据格式、加密方式等信息，并按要求明文提供相关数据内容”。[21]

**七、监管报告要求**

《征求意见稿》规定，运营者处理个人信息涉及个人信息主体超过10万人、或者处理重要数据的运营者，应当在每年十二月十五日前将年度数据安全管理情况报省级网信部门和有关部门。报告的内容包括：（一）数据安全负责人以及负责处理用户权益相关事务责任人的姓名和联系方式；（二）处理数据的类型、规模、目的及必要性；（三）数据的安全防护和管理措施，包括保存地点、期限等；（四）与境内第三方共享数据情况；（五）数据安全事故及处理情况；（六）与个人信息和数据相关的用户投诉及处理情况；（七）国家网信部门明确的其他数据安全情况。（第十七条）

如果存在向境外提供数据的情况，运营者则还应当报告：（一）接收者的名称和联系方式；（二）出境数据的类型、数量及目的；（三）数据在境外的存放地点、使用范围和方式；（四）涉及向境外提供数据的用户投诉及处理情况；（五）国家网信部门明确的向境外提供数据需要报告的其他情况。（第十八条）

与以上规定类似的，《数安法二审稿》要求重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告；且在发生数据安全事件时向主管部门进行报告。[22]《管理办法》要求网络运营者发布、共享、交易或向境外提供重要数据前应当进行安全风险评估，并报经行业主管监管部门同意；[23] 如果发生个人信息泄露、毁损、丢失等数据安全事件，或者发生数据安全事件风险明显加大时，也应当按要求向行业主管监管部门和网信部门报告。[24]

**八、结语**

《征求意见稿》总体上是一部较为严格的规定，对于汽车产业链中的各企业、以及收集和处理与汽车场景相关数据的其他企业而言，《征求意见稿》提出了较高的合规要求，这些合规要求不但需要在法律文件层面（例如隐私政策、用户协议、内部管理制度）落实，还需要在数据管理体系和技术实现方式层面（例如车内显示屏展示告知内容、匿名化或脱敏处理敏感信息、向车主提供结构化的数据查询结果）进行落实。虽然在正式出台之前《征求意见稿》仍会进一步修改和完善，但结合最近公布的《个保法二审稿》、《数安法二审稿》以及相关国家标准的征求意见稿，我们倾向于认为《征求意见稿》的规定基本符合我国最近数据立法/标准所体现的各项原则，集中反映了相关立法部门对汽车领域数据保护问题的态度，《汽车数据安全管理若干规定》正式稿的内容可能不会偏离《征求意见稿》太多。我们建议相关企业仔细分析《征求意见稿》的具体要求，并对企业现有数据合规实践进行梳理和差距分析，及时开展合规工作。

《征求意见稿》针对汽车领域的个人信息和重要数据处理活动提出一系列的合规要求，但其中的一些要求实际上在此前已发布的法律法规和相关文件（包括征求意见稿）中已有类似规定。相关企业在开展数据合规工作中不仅要考虑如何落实《征求意见稿》中的要求，还需要考虑这些要求与已发布的法律法规和相关文件（包括征求意见稿）的衔接问题。

**注释**：

[1] 《网络安全法》第二条在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

[2] 《数据安全管理办法》（征求意见稿）第二条 在中华人民共和国境内利用网络开展数据收集、存储、传输、处理、使用等活动（以下简称数据活动），以及数据安全的保护和监督管理，适用本办法。纯粹家庭和个人事务除外。法律、行政法规另有规定的，从其规定。

[3] 《民法典》第一千零三十四条 个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

[4] 《网络安全法》第七十六条 个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

[5] 《个人信息安全规范》3.1 个人信息是指，以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[6] 《车联网信息服务 用户个人信息保护要求》3.1 车联网信息服务用户个人信息是指，车联网产业相关的汽车厂商、零部件和元器件提供商、软件提供商、数据和内容提供商在提供服务过程中收集的能够单独或与其他信息结合识别用户和涉及用户个人隐私的信息。

[7] 《个保法二审稿》第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[8] 《管理办法》第三十八条 重要数据，是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。重要数据一般不包括企业生产经营和内部管理信息、个人信息等。

[9] 《信息安全技术 数据出境安全评估指南（征求意见稿）》附录A（规范性附录）重要数据识别指南

《重要数据识别指南》中的重要数据是指相关组织、机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：

a) 危害国家安全、国防利益，破坏国际关系；

b) 损害国家财产、社会公共利益和个人合法利益；

c) 影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

d) 影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；

e) 干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

f) 危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；

g) 影响或危害国家经济秩序和金融安全；

h) 可分析出国家秘密或敏感信息；

i) 影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。

[10] 例如，《地图管理条例》第三十四条 互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并制定互联网地图数据安全管理制度和保障措施。 又如，《关于加强自动驾驶地图生产测试与应用管理的通知》二、 当前，各单位、企业用于自动驾驶技术试验、道路测试的地图数据(包括在传统导航电子地图基础上增添内容、要素或精度提升的)，应当按照涉密测绘成果进行管理，并采取有效措施确保数据安全。未经省级以上测绘地理信息行政主管部门批准，不得向外国的组织和个人以及在我国注册的外商独资和中外合资、合作企业提供、共享地图数据，不得在相关技术试验或道路测试中允许超出范围的人员接触地图数据。

[11] 例如《民法典》第一千零三十五条、《网络安全法》第四十一条、《个人信息安全规范》第4条。

[12] 例如《网络安全法》第二十一条、《管理办法》第六条。

[13] 《安全要求》5. 数据传输 5.1 未经被收集者的单独同意，网联汽车不得通过网络、物理接口向车外传输包含个人信息的数据。将清晰度转换为120万像素以下且已擦除可识别个人身份的人脸、车牌等信息的视频、图像数据除外。5.2 网联汽车不得通过网络、物理接口向车外传输汽车座舱内采集的音频、视频、图像等数据及经其处理得到的数据。

[14] 例如，《个人信息安全规范》第5.2a）条。

[15] 例如，《App违法违规收集使用个人信息行为认定方法》第二条第3项。

[16] 例如，《个保法二审稿》第十六条。

[17] 例如，《信息安全技术 人脸识别数据安全要求（征求意见稿）》5基本安全要求 数据控制者：…… f) 开展人脸验证或人脸辨识时，应至少满足以下要求：……3）应同时提供非人脸识别的身份识别方式，并提供数据主体选择使用。……

[18] 《管理办法》第十五条。

[19] 《个人信息出境安全评估办法（征求意见稿）》第十四条。

[20] 《个人信息出境安全评估办法（征求意见稿）》第十五条。

[21] 《安全要求》第7.2条。

[22] 《数安法二审稿》第二十八条和第二十九条。

[23] 《管理办法》第二十八条。

[24] 《管理办法》第三十五条。