附件 4：

中汽协会《汽车企业数据安全管理体系要求》

团体标准编制说明

一、工作简要过程

（一）任务来源

1、项目立项背景

1）行业迫切需求：近年汽车的智能化、网联化程度不断加深，车辆在行驶过程中采集、使用和产生大量数据，并通过车联网发送这些数据至智能网联汽车生产和服务运营厂商进行存储、使用等。智能网联汽车生产和服务运营厂商作为汽车数据处理者，掌握着大量数据资产，一旦安全管理不当，发生滥用、泄露等危害数据安全的情形，会对用户个人利益、相关组织利益、公众利益、甚至国家利益产生不良影响。

2）监管明确规范：工信部发布的《工业和信息化部关于加强智能网联汽车生产企业及产品准入管理的意见》和《工业和信息化部关于加强车联网网络安全和数据安全工作的通知》中对智能网联汽车生产企业以及车联网服务提供商分别提出“建立健全汽车数据安全管理体系”的要求。

3）尽快填补空白：现阶段尚无针对汽车行业数据安全管理体系的要求标准发布。相关国家标准仍处于起草阶段，距离发布尚需较长时间。

2、计划任务编号

2023-63

（二）主要起草单位及任务分工

上海机动车检测认证技术研究中心有限公司：标准编制工作组牵头单位，全面负责标准项目的立项、标准文本以及编制说明的编写、标准编制工作的组织及协调等工作。

北京赛西科技与发展有限责任公司：标准编制工作组重点参与单位，全面参与标准文本的编写。

其他对于标准编制有重要贡献的单位包括（不分先后）：比亚迪汽车工业有限公司、北京市竞天公诚律师事务所上海分所、东风汽车集团有限公司技术中心、广汽研究院、一汽大众、吉利汽车研究院（宁波）有限公司、上汽通用五菱汽车股份有限公司、合众新能源、腾讯云计算（北京）有限责任公司、云从科技集团股份有限公司、上海富数科技有限公司。

（三）标准研讨情况

2022 年 11~12 月，上海机动车检测认证技术研究中心有限公司组织数据安全工作人员对于国内汽车数据安全管理体系情况进行了调研。

2023 年 3 月，上海机动车检测认证技术研究中心有限公司与北京赛西科技与发展有限责任公司共同成立核心工作组，对标准的方向、框架进行了确定，并初步编制了框架性草案。

2023 年 4 月，上海机动车检测认证技术研究中心有限公司组织召开线上专家立项评审会议。会上专家认为：1)目前行业内尚未有成熟的国标、行标可供企业使用，汽标委虽有相关国标起草计划，但国标整体流程较长，行业急需该领域共识的形成，因此建议团标先行，为后续国标要求的编制奠定基础；2)标准牵头单位具备数据安全管理体系建立的实际经验，是第三方机构，满足牵头标准制定的基本条件；3)本标准的编制，能有效支撑主管部门后续行业管理工作，同时能够给予企业数据安全管理工作的有效指导；4)建议标准制定过程中多吸纳整车企业参与，多与企业已有体系相结合，着重在标准的可操作性。整体同意立项。

2023 年 5 月，上海机动车检测认证技术研究中心有限公司召集整体工作组第一次会议，会议介绍了标准的初步方向与框架，并获得了各参与单位的确认和同意。针对具体条款内容，采取了组内征求意见的形式征集工作组内各成员单位意见，并于 5 月底完成了工作组内 88 条详细意见的汇总。

经过细致分析与非会议形式沟通，上海机动车检测认证技术研究中心有限公司于 6 月 8 日完成 88 条组内意见的沟通与回复，其中采纳 54 条、部分采纳 6 条、不采纳 28 条。同时召集全体成员单位再次确认，并针对以下意见较多的重点问题进行了具体沟通并达成一致意见：

1) 数据操作日志记录的保存时限：原要求为在技术条件允许的情形下保存 2 年；成员单位提出此要求过于模糊，且可以参照《网络安全法》第 21 条（三）的要求。因此修改为最低保存不少于 6 个月时间（公开征求意见稿 8.1.6）。
2) 数据提供和委托处理的义务责任：根据《个保法》内容，删除了原有的“共享”概念；同时，成员单位提出，参考《个保法》中针对个人信息提供和委托处理两种情形下的义务责任模型、并考虑到数据提供方无法持续对数据接收方保留约束能力，应不要求数据提供方持续监督和定期审计数据接收方数据安全保障能力（公开征求意见稿 8.9）；
3) 产品开发阶段的数据安全过程保障：成员单位提出，在产品开发过程中，应当针对数据安全保障的嵌入进行具体的要求，因此在原草案的基础上进一步明确应在产品开发启动前，结合数据安全目标和相关法律法规标准要求进行产品数据安全风险评估。相关评估结果应上报至数据安全管理负责人，并形成数据安全风险处置方案；风险处置方案应依照组织内部新产品开发流程要求的形式形成文件化信息，并向产品设计开发团队进行有效传递（公开征求意见稿 8.5）。

二、标准编制原则和主要内容

1、标准编制原则

1）规范性原则：本标准按照 GB/T 1.1-2020《标准化工作导则第一部分：标准的结构和编写》的规定和要求编制，在标准框架、结构和内容等方面符合要求。

2）科学实用原则：标准内容全面，采纳多方面实际经验，适应汽车企业数据安全的实际管理需要。

2、主要内容介绍

标准主要针对汽车企业数据安全管理体系提出相关要求。标准整体框架基于先行数据安全法律、法规和标准的内容进行确定，并充分参考 GB/T 22080-2016/ISO/IEC 27001:2013 要求。主要包括以下几个模块的内容：

1）内外部环境确认：本标准参照 GB/T 22080-2016 及其对应 ISO 标准（ISO

27001-2013），以涉及数据安全管理的组织的最高管理层为体系建设的发起者。在此前提下,标准本章节首先要求汽车数据处理者的最高管理层提出对于数据安全管理体系预期达到的目标，然后根据提出的目标识别相关的内外部影响因素（例如内部组织机构设置、人力技术资源情形、行业最佳实践等）。同时，最高管理层应识别确认数据安全管理的相关实体，以及其具体的需求。在综合考虑内外部影响因素和相关实体具体需求的情况下，最高管理层应对汽车数据安全管理体系的范围进行划定。

2）最高管理层：在数据安全管理体系划定完成之后，要求汽车数据处理者履行其领导职责，通过一系列承诺来自上而下地推动体系建设和落实。同时，要求以正式文件形式来将这种承诺正式化并在汽车数据处理者内部进行充分传播沟通。

3）汽车数据安全管理组织：在体系范围划定之后，要求汽车数据处理者建立相应的数据安全管理组织架构，并符合一系列强制性要求。至此，汽车数据处理者内部正式建立汽车数据安全管理组织。为了保证组织内各项具体活动有效开展，要求分解高层级目标形成具体的工作计划。

4）管理制度：前期规划与准备工作完成后，要求以规章制度的形式正式对于数据安全管理的活动进行规范。根据法律法规要求，包括：数据分级分类、全生命周期管理、数据访问权限管理、数据安全用户反馈及投诉管理、产品数据安全管理、数据安全运营管理、数据安全风险管理、数据出境安全管理、数据提供、数据安全审计、数据加密和数据安全文化建设等。

5）支持性措施：提出了数据安全管理体系正常运转在资源、人员能力、人员意识、文件管控等支持性方面需要满足的要求。

6）体系运行：要求当具体制度制定完成后，对于其规范的机制和流程进行规划和控制，从而确保其有效运行。同时，在机制和流程运行的过程当中，进行相应的数据安全风险评估和处置。

7）体系各环节效果评价：要求为了保障整个体系的有效运行，建立相应的监测、分析和评价机制，并对实际执行的记录进行审计。在结合监测、分析、评价结果以及审计结果的情况下，由最高管理层对于整个数据安全管理体系的运行效果进行评审，从而发现整个体系的不足之处。

8）进一步改进：在发现整个体系的不足之处后，要求组织进行相应的整改和持续改进。

三、采用国际标准和国外先进标准情况

本标准在制定过程中主要参照 ISO/IEC 27001:2013 中对于体系规划、检查和执行阶段的要求，编制了内外部环境确认、最高管理层背书、执行性组织搭建、支持性措施、体系运行保障、体系效果评价和进一步改进的相关内容。

四、主要关键指标及试验验证情况

本标准在 ISO/IEC 27001:2013 的体系框架基础上，对国内适用的数据安全法律、法规和标准内容进行整合与协调。在已发布的数据安全相关规定之外，本标准还结合最佳实践对数据安全管理手段进行了更深入的探索。

其中较为重要的如下所示：

重要内容	对应章节	详解
环境、最高管理层、汽车数据安全管理组织、支持性措施、体系运行、	5、6、7、9、10、11、12	主要参照 GB/T 22080-2016 内容进行编制，同时融合《个人信息保护法》、《数据安全法》、《汽车数据安全管理若干规定（试行）》的相

进一步改进		关要求
要求建立数据资产管理台账	8.1.2	根据企业最佳实践的反馈，结合智能网联汽车准入等其他相关要求，认为建立数据资产的管理台账更有利于企业统筹管理数据资产。
汽车数据安全管理组织应加强对重要数据、个人信息等数据的全生命周期保护，应留存至少6 个月的数据操作日志记录。	8.1.6	主要参考了《工业和信息化领域数据安全管理办法（试行）》第25条的相关要求，并考虑到数据安全审计和追溯的需求，针对云平台的数据相关操作进行记录并规定日志留存时限；相关时限在组内征求意见过程中改为“至少6个月”。
数据全生命周期管理	8.2	主要参考GB/T 35273-2020，GB/T 41871-2022和GB/T 41479-2022的要求；进行了整合和统一。
至少在产品开发启动前进行产品数据安全风险评估。相关评估结果应上报至数据安全管理负责人，并形成数据安全风险处置方案；风险处置方案应依照组织内部新产品开发流程要求的形式形成文件化信息，并向产品设计开发团队进行有效传递	8.5	参考欧盟个人信息保护的'Privacy by design and default'倡议，认为在产品生命周期当中（特别是概念开发阶段）嵌入数据安全内容，从而高效、严谨地实现产品端的数据安全合规
对受托方数据安全保障能力持续监督和定期审计的机制	8.9.4	参考《个保法》中针对个人信息提供和委托处理两种情形下的义务责任模型、并考虑到数据提供方无法持续对数据接收方保留约束能力，应不要求数据提供方持续监督和定期审计数据接收方数据安全保障能力

五、与现行法律、法规和政策及相关标准的协调性

本标准与现行国家法律、法规，现行标准，制定中标准均无任何相悖之处。

六、贯彻标准的要求和措施建议

本标准发布后，建议由数据分会协调组织宣贯会议进行行业宣贯。

建议国内各汽车厂参照本标准要求建立相应的数据安全管理体系或在本标准基础上制定相应的企业标准。

七、其他需要说明的事项

无其他需要说明事项。