ICS 07.040
CCS A 75

TB

团　　体　　标　　准

T/CSGPC XXX-20XX

智能网联汽车　时空数据安全保护要求

Security protection requirements for intelligent and connected vehicle spatio-temporal data

（征求意见稿）

20XX-XX-XX 发布　　20XX-XX-XX 实施

中国测绘学会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国测绘学会提出并归口。

本文件起草单位：中汽智联技术有限公司、中汽智能科技（天津）有限公司、自然资源部地图技术审查中心、自然资源部测绘发展研究中心、中国测绘科学研究院、清华大学、武汉大学、国家计算机网络应急技术处理协调中心、天津市测绘地理信息研究中心、中国质量认证中心、广州小鹏汽车科技有限公司、中汽研汽车检验中心（武汉）有限公司、中汽研临港数科有限公司、中移智行网络科技有限公司、湖北亿咖通科技有限公司、沈阳美行科技股份有限公司。

本文件主要起草人：张庆余、陈会仙、王旭、周博雅、杨殿阁、贾宗仁、马小龙、梁宇、杨蒙蒙、乐鹏、张奕欣、王万峰、张敬、姜同舟、王晓萌、谢蓉、纪东方、陈婧韬、柳东威、胡勇庆、耿东伶、贾月飞、刘秋平、蒋鑫、蔡传威。

智能网联汽车　时空数据安全保护要求

1　范围

本文件规定了自动驾驶地理信息数据安全保护的技术要求和管理要求。

本文件适用于自动驾驶地理信息数据的安全应用。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

T/CSGPC 57-2025 自动驾驶地理信息数据分级规则

3　术语和定义

T/CSGPC 57-2025 中界定的以及下列术语和定义适用于本文件。

3.1

自动驾驶地理信息数据　autonomous driving geographic information data

由车载传感器采集生成或经加工处理，用于支撑自动驾驶功能实现、具有时间和空间特征的地理信息数据，分为实时数据和先验数据两类。

3.2

数据处理者 data processor

指开展自动驾驶地理信息数据收集、存储、加工、传输、提供、公开、销毁等活动的单位或组织。

3.3

数据使用者 data user

指仅接收、使用非敏自动驾驶地理信息数据（含 II 级重要数据、一般数据），不开展自动驾驶地理信息数据处理活动的单位或组织。

3.4

脱敏处理 desensitization processing

对自动驾驶地理信息数据采取技术措施降低其敏感程度，使核心数据或 I 级重要数据降级为 II 级重要数据或一般数据的处理活动。

4　技术要求

4.1　分级防护要求

4.1.1　一般数据

4.1.1.1　存储阶段应采取物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等技术，加强数据存储安全管控。

4.1.1.2　传输阶段应根据传输的数据类型和应用场景等，制定安全策略并采取保护措施。
4.1.1.3　加工使用阶段应采取访问控制、数据防泄露、操作审计等技术，确保过程安全、合规、可控、可溯源。
4.1.1.4　应采取安全监测、日志审计等技术工具开展安全审计，实时记录地理信息数据全生命周期下的操作日志，并采取技术手段保障日志的完整性。
4.1.1.5　应采用不可逆删除技术实施数据销毁，确保销毁后数据不可恢复。
4.1.1.6　一般数据在落实相应安全防护要求的前提下，可向数据使用者提供使用。

4.1.2　II级重要数据

4.1.2.1　Ⅱ级重要数据应满足一般数据相应技术要求。
4.1.2.2　数据存储系统应落实第三级及以上网络安全等级保护要求。
4.1.2.3　加工使用阶段应采取严格的访问控制，建立数据可信可控、风险监测评估、实时监控、应急处置、数据溯源等相关技术，确保过程安全、合规、可控、可溯源。
4.1.2.4　传输阶段应采取校验技术、密码技术、安全传输通道或者安全传输协议等技术手段，避免数据泄露、篡改、伪造等风险。
4.1.2.5　提供阶段应采取风险隔离、认证鉴权、威胁告警等安全保护技术措施，定期监测数据共享、调用情况。
4.1.2.6　II 级重要数据在落实相应安全防护要求的前提下，可向数据使用者提供使用。

4.1.3　I级重要数据

I级重要数据应满足Ⅱ级重要数据相应技术要求。

4.1.4　核心数据

4.1.4.1　核心数据应满足Ⅰ级重要数据相应技术要求。
4.1.4.2　存储阶段，存储系统应落实关键信息基础设施安全保护要求或第四级网络安全等级保护要求。

4.2　风险监测预警与应急管理

应采取日志管理、监测预警、应急管理等技术手段，开展数据安全风险监测预警和应急管理，并将地理信息数据处理流程、安全风险及安全事件处置结果等信息实时同步至主管部门。

5　管理要求

5.1　数据分级管理

5.1.1　安全组织架构

5.1.1.1　数据处理者应根据需要配备数据安全管理人员，统筹负责数据处理活动的安全监督管理，并合理确定数据处理活动的操作权限，严格实施人员权限管理。
5.1.1.2　重要数据处理者和核心数据处理者应建立覆盖本单位相关部门的数据安全工作体系，明确数据安全负责人和管理机构，建立常态化沟通与协作机制。
5.1.1.3　重要数据处理者和核心数据处理者应明确数据处理关键岗位和岗位职责，并要求关键岗位人员签署数据安全责任书。
5.1.1.4　重要数据和核心数据处理者应按照业务工作需要和最小授权原则，依据岗位职责设定重要数据和核心数据处理权限，控制数据接触范围，人员变动时应及时调整权限。

5.1.2 数据目录备案

5.1.2.1 数据处理者应定期梳理填报重要数据和核心数据目录，并上报主管部门。

5.1.2.2 应在数据内容发生重大变化后 3 个月内履行变更手续。重大变化包括数据内容变化导致原有级别不再适用，或重要数据和核心数据规模变化 30%以上等。

5.1.3 数据制度体系

5.1.3.1 一般数据

5.1.3.1.1 应建立数据存储管理制度，确保数据存储于境内安全环境。

5.1.3.1.2 应建立数据加工使用管理制度，确保数据来源真实可靠且收集过程经审查核实；涉及利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理，明确数据使用加工过程中的相关责任。

5.1.3.1.3 应建立数据传输管理制度，根据传输的数据类型和应用场景制定安全策略。

5.1.3.1.4 应建立数据提供管理制度，明确提供的范围、类别、条件、程序等，提供的数据应当限于实现数据接收方处理目的的最小范围，并告知数据接收方按照对应级别进行分类分级保护并落实安全保护措施。

5.1.3.1.5 应建立数据公开安全评估制度，在数据公开前分析研判可能对国家安全、公共利益产生的影响，存在显著负面影响或风险的，不得公开。

5.1.3.1.6 应当建立数据销毁制度，明确销毁对象、规则、流程和技术等要求，对销毁活动进行记录和留存。

5.1.3.1.7 应建立数据转移制度，明确数据转移方案，跨主体转移应核验接收方资质与安全能力。

5.1.3.1.8 应建立数据委托处理管理制度，通过签订合同协议等方式，明确委托方与受托方的数据安全责任和义务，未经委托方同意，受托方不得将数据提供给第三方。

5.1.3.1.9 应建立数据日志管理制度，记录数据处理、权限管理、人员操作等日志，一般数据的日志留存时间不少于 6 个月；定期进行安全审计，并形成审计报告。

5.1.3.2 Ⅱ级重要数据

5.1.3.2.1 Ⅱ级重要数据应满足一般数据相关管理要求。

5.1.3.2.2 应建立重要数据收集管理制度，加强对收集生产人员、设备的管理，并对收集来源、时间、类型、数量、精度、区域、频度、流向等进行记录；通过间接途径获取数据的，应与数据提供方通过签署相关协议、承诺书等方式，明确双方法律责任。

5.1.3.2.3 应建立重要数据存储管理制度，采取数据容灾备份和存储介质安全管理，定期开展数据恢复测试；采取分区域存储重要数据。

5.1.3.2.4 应建立重要数据加工使用管理制度，严格控制数据访问控制权限，落实数据可信可控、日志留存审计、风险监测评估、实时监控、应急处置、数据溯源等管理机制。

5.1.3.2.5 应建立重要数据提供管理制度，与数据接收方签署数据安全协议，加强重要数据提供人员、设备的管理，并对数据来源、时间、类型、数量、精度、区域、频度、流向等进行日志记录，明确双方法律责任。

5.1.3.2.6 应建立重要数据销毁制度，事前向主管部门报告数据销毁方案，引起重要数据目录变化的，应当及时向主管部门报备，不得以任何理由、任何方式对销毁数据进行恢复。

5.1.3.2.7 应建立重要数据出境安全评估制度，申请向境外提供数据的，必须履行地图审核程序，并落实国家网信部门数据出境安全评估等有关规定。

5.1.3.2.8 应建立重要数据转移安全管理制度，事前向主管部门报告数据转移方案，引起重要数据目录发生变化的，应当及时向主管部门报备，按照要求履行备案变更手续。

5.1.3.2.9　应建立重要数据委托处理制度，评估受托方的数据安全保护能力及资质情况，明确受托方的数据处理权限和保护责任，并监督受托方履行数据安全保护义务。

5.1.3.2.10　应建立重要数据日志管理制度，涉及重要数据安全事件处置、溯源的，相关日志留存时间不少于 1 年；涉及向他人提供、委托处理、共同处理重要数据的，相关日志留存时间不少于 3 年。

5.1.3.3　Ⅰ级重要数据

5.1.3.3.1　Ⅰ级重要数据应满足Ⅱ级重要数据相关管理要求。

5.1.3.3.2　Ⅰ级重要数据对外提供应配置专人专机，专机需安装安全审计软件，进行实时审计。

5.1.3.4　核心数据

5.1.3.4.1　核心数据应满足Ⅰ级重要数据相关管理要求。

5.1.3.4.2　应建立核心数据提供风险管控制度，采取强化安全保护措施并上报自然资源部，自本年度 1 月 1 日起可能累计达到总量 30%及以上的，应当经自然资源部报国家数据安全工作协调机制组织风险评估。

5.1.3.4.3　应建立核心数据日志管理制度，涉及核心数据安全事件处置、溯源的相关日志留存时间不少于 3 年。

5.2　安全风险评估

5.2.1　数据处理者应建立健全数据安全风险评估制度，覆盖数据全生命周期各环节。

5.2.2　重要数据处理者应自行或委托第三方评估机构，每年对其数据处理活动至少开展 1 次风险评估，并向主管部门报送风险评估报告。

5.2.3　风险评估报告应包括处理的重要数据的类别、数量，开展数据处理活动的情况，面临的数据安全风险、应对措施及其有效程度等。

5.2.4　数据处理者在组织数据安全风险评估时，应对其数据查询、下载、修改、删除等重点操作的日志开展审计分析，发现违规或异常行为，应及时采取相应处置措施。

5.2.5　数据处理者应保留风险评估报告至少 3 年。

5.2.6　核心数据处理者应使用第三方评估机构开展风险评估，每半年对其数据处理活动至少开展 1 次风险评估，并向主管部门报送风险评估报告。

5.3　监测预警与应急管理

5.3.1　数据处理者应建立实施数据安全监测预警与应急管理制度，确保对数据安全风险及安全事件的实时监测和应急处置。

5.3.2　数据处理者应建立数据安全风险监测预警机制，及时排查安全隐患，采取必要的措施防范数据安全风险，并将可能造成较大及以上安全事件的风险向主管部门报告。

5.3.3　数据处理者应建立应急管理制度，在数据安全事件发生后，按照应急预案及时开展应急处置，涉及核心或重要地理信息数据安全事件，第一时间向主管部门、属地公安部门报告，事件处置完成后在一周内形成总结报告。

5.3.4　数据处理者对发生的可能损害用户合法权益的数据安全事件，应当及时告知用户，并提供减轻危害措施。

参 考 文 献

[1] GB/T 44464-2024 汽车数据通用要求
[2] 工业和信息化部. 工业和信息化领域数据安全管理办法. 2022
[3] 自然资源部. 自然资源领域数据安全管理办法. 2024