长安汽车数据宣言
Changan Automobile Data Statement

数据安全与隐私保护是数字时代企业发展的基石，也是企业对用户、合作伙伴及社会的基本承诺。重庆长安汽车股份有限公司（以下简称“长安汽车”“公司”“我们”）致力于构建一个安全可信、合规高效、责任共担的数据治理体系，让每一份数据在收集、传输、存储、处理、交换和销毁的全生命周期中都能获得妥善保护，让技术发展始终服务于人的尊严与价值，共同推动数字社会的安全与进步。

Data security and privacy protection are the cornerstone of enterprise development in the digital era, and our fundamental commitment to users, partners, and society. Chongqing Changan Automobile Co., Ltd. (hereinafter referred to as "Changan Automobile," "the Company," or "we") is committed to building a secure, trusted, compliant, and accountable data governance system, ensuring that every piece of data is properly protected throughout its lifecycle, covering collection, transmission, storage, processing, exchange, and disposal. We strive to ensure that technology always serves human dignity and value, and to jointly advance the security and progress of the digital society.

一、概述 Overview

（一）目的 Purpose

为保障用户、合作伙伴及企业的数据安全与隐私权益，构建可信赖的数字化服务体系，长安汽车制定本数据宣言（以下简称“本宣言”），旨在向数据处理者及决策人员阐明个人信息的全生命周期管理流程，并确保数据主体（包括员工、客户及合作伙伴等）知晓其享有的各项法定权利，在合规前提下充分发挥数据价值，推动智能出行生态的可持续发展。

To safeguard the data security and privacy rights of users, partners, and the Company, and to build a trusted digital service system, Changan Automobile has formulated this Data Statement (hereinafter referred to as "this Statement"). This Statement is intended to clarify the lifecycle management process of personal information for data processors and decision-makers, and ensures that data subjects, including employees, customers, and partners, are informed of their legal rights. It aims to unlock the value of data while remaining compliant and drive the sustainable development of the intelligent mobility ecosystem.

（二）编制依据 Basis for Preparation

长安汽车严格遵守运营所在地适用的网络安全、数据安全、个人信息保护、汽车数据安全和数据跨境流动相关法律法规，包括《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《汽车数据安全管理若干规定（试行）》《数据出境安全评估办法》《网络数据安全管理条例》等，以及智能网联汽车数据采集、跨境相关的监管规定；并参照 ISO/IEC 27001、ISO 37301 等信息安全和合规相关的国际

标准，结合公司数字化业务、智能网联产品、客户服务和数据全生命周期管理实践，制定本宣言。

Changan Automobile strictly complies with applicable laws and regulations related to cybersecurity, data security, personal information protection, automotive data security and cross-border data flows in the jurisdictions where it operates, including the *Cybersecurity Law of the People's Republic of China*, the *Data Security Law of the People's Republic of China*, the *Personal Information Protection Law of the People's Republic of China*, the *Several Provisions on Automotive Data Security Management (for Trial Implementation)*, the *Measures for Security Assessment of Data Export*, and the *Regulations on Network Data Security Management*, as well as relevant regulatory provisions on data collection and cross-border transfer concerning intelligent connected vehicles. The Company also refers to international standards relevant to information security and compliance, such as ISO/IEC 27001 and ISO 37301. This Statement is formulated taking into account the Company's digital business, intelligent connected products, customer services and data lifecycle management practices.

如本宣言与运营所在地适用法律法规存在冲突，或本宣言要求低于当地强制性标准，长安汽车优先遵守运营所在地适用法律法规及更高合规要求。

In cases where this Statement conflicts with applicable laws and regulations in any operating jurisdiction, or where its requirements fall below

mandatory local standards, Changan Automobile shall prioritize compliance with applicable local laws and regulations and higher compliance requirements.

（三）原则 Principles

在践行本宣言的承诺、行动路径过程中，公司将遵循以下原则：

In implementing the commitments, and roadmap of this Statement, the Company will adhere to the following principles:

1. 合法合规 Legal Compliance

我们承诺严格遵守中国及业务所涉国家与地区的有关数据安全与隐私保护法律法规，确保在全球范围内的业务运营均符合各司法辖区的监管标准。

We comply with all applicable data security and privacy protection laws and regulations in China and the countries and regions where we operate, ensuring that our global business activities meet the regulatory standards of each jurisdiction.

2. 最小必要 Data Minimization

我们承诺仅收集与业务相关的最小范围数据，禁止过度采集。

We undertake to collect only the minimum scope of data that is relevant to our business operations and prohibit excessive collection.

3. 透明可控 Transparency and Control

我们向用户明确告知数据处理规则，保障其知情权与控制权。

We clearly inform users of our data processing rules and safeguard their

right to know and control.

4. 安全防护 Security Protection

采取技术与管理措施，保障数据全生命周期安全。

We adopt technical and administrative measures to ensure data security throughout its lifecycle.

5. 责任共担 Shared Responsibility

与供应链伙伴协同落实数据保护义务。

We work with supply chain partners to jointly fulfill data protection obligations.

（四）适用范围 Scope of Application

本宣言适用于公司本部及具有实际控制力的各级企业。同时，我们致力于将本宣言中的相关承诺与原则，通过倡导、合作等形式，延伸至全价值链的关键业务伙伴，包括但不限于供应商、经销商、服务商，其他重要的合作伙伴（如研发合作伙伴、行业组织等）。

This Statement applies to the Company's headquarters and all entities under its effective control. Furthermore, we are committed to extending the relevant commitments and principles set out in this Statement to key business partners across our entire value chain through advocacy, cooperation, and other means. These partners include but are not limited to suppliers, dealers, service providers, and other key partners such as R&D partners and industry organizations.

二、治理体系与实施保障 Governance System and Implementation Guarantee

（一）治理体系 Governance System

数据安全管理是长安汽车风险管理体系的重要组成部分，我们积极构建由董事长担任组长的“网络安全和信息化领导小组、领导小组办公室和专责组、执行单位”的三级联防联控机制，同时设置首席网络安全官、首席数字官统筹数据安全工作规划与监督执行，各业务单元相关部门负责属地合规实施与日常管理。同时，建立常态化数据安全协同机制，推动技术、法务、业务等部门在数据治理与隐私保护工作中实现高效联动与统一行动。

Data security management is a key component of Changan Automobile's risk management system. We have established a three-tier joint prevention and control mechanism for Cybersecurity and Informatization, consisting of the Leading Group chaired by our Chairman, its general office and specialized teams, and executing units. We have also appointed a Chief Cybersecurity Officer and a Chief Digital Officer to coordinate data security planning and oversee implementation, while relevant business units are responsible for local compliance and daily management. We maintain a regular data security coordination mechanism to enable efficient collaboration and unified action across technology, legal, and business departments in data governance and privacy protection.

长安汽车以《中央企业合规管理办法》和 ISO 37301 等国内

外标准为依据，充分吸收国际先进合规管理经验，立足业务场景与实际需求，统筹推进数据合规、出口管制、反垄断等领域专项合规体系建设。并在 2025 年 10 月荣获全球权威标准机构 BSI（英国标准协会）颁发的 ISO 37301: 2021 及 GB/T 35770-2022 合规管理双认证证书。针对汽车行业特点和业务模式，公司严格遵循中国《数据安全法》《个人信息保护法》《汽车数据安全管理若干规定（试行）》及其他适用法域的数据合规要求，在数据收集、存储、处理、跨境传输及出境安全评估等关键环节建立专项管控机制，并在研产供销运全业务流程中增设百余个合规管控节点，实现合规管理与业务运营深度融合，确保数据安全与合规管控精准高效、覆盖经营全链条，切实防范化解合规风险。

Based on the Measures for the Compliance Management of Central Enterprises and ISO 37301, as well as other China's and international standards, we draw on advanced international compliance management experience and coordinate the development of specialized compliance systems in areas including data compliance, export controls, and antitrust, tailored to our business scenarios and actual needs. In October 2025, we obtained ISO 37301:2021 and GB/T 35770-2022 dual certification from British Standards Institution (BSI). Given the characteristics of the automotive industry, we strictly comply with the Data Security Law of People's Republic of China, Personal Information Protection Law of the People's Republic of China, Several Provisions on the Management of Automotive Data Security (for Trial

Implementation), and applicable data compliance requirements in other jurisdictions. We have established specialized control mechanisms for key areas including data collection, storage, processing, cross-border transfer, and outbound security assessments, and added over one hundred compliance control points across the full business chain of R&D, production, procurement, sales, and operations. This ensures deep integration of compliance management with business operations, precise and effective data security and compliance controls across the entire business chain, and effective mitigation of compliance risks.

（二）资源保障 Resource Guarantee

我们成立网络安全和信息化领导小组，为公司数据安全相关工作的最高决策机构，投入专项资金用于数据安全能力建设，组建专业数据安全团队，规模随业务增长动态调整。

We have established the Leading Group of Cybersecurity and Informatization as the highest decision-making body for data security matters. We allocate dedicated funding for data security capability building and set up a professional data security team whose size adjusts dynamically with business growth.

（三）培训和能力建设

Training and Capability Building

公司针对不同层级管理者、员工及相关方开展数据安全与隐私保护赋能培训，定期解读国内外数据安全、个人信息保护等相关法律法规，宣贯公司数据安全治理与隐私合规相关制度，提升

全员数据合规意识与安全防护技能。我们特别加强海外业务团队数据合规能力建设，通过属地化法规培训、国际化合规协同实践等，不断提升公司应对全球化数据治理新要求的能力。

We provide data security and privacy protection training for managers, employees, and relevant parties at all levels, covering regular interpretation of China's and international data security and personal information protection laws and regulations, and communicating our data security governance and privacy compliance policies. This builds data compliance awareness and security protection capabilities across the organization. We attach great importance to building data compliance capabilities for our overseas business teams through training on local regulatory requirements and international compliance collaboration practices, continuously strengthening our ability to meet evolving global data governance requirements.

三、数据分类分级机制 Data Classification and Grading Mechanism

（一）分类标准制定 Classification Standards

1. 按数据来源划分为外部数据、内部数据等类别。

We classify data by source into external data and internal data.

2. 按照数据用途、处理目的细化分类：主数据、基础数据、业务数据、报告数据、观测数据、规则数据。

We further classify data by purpose and processing objective into master data, reference data, operational data, reporting data, monitoring data, and rule data.

（二）分级保护策略 Graded Protection Strategies

1. 法务分类：根据数据是否含个人隐私数据，分为一般个人信息、敏感个人信息、其他信息。

Legal Classification: Based on whether it contains personal information, data is classified into general personal information, sensitive personal information, and other information.

2. 数据安全级别：根据数据对公司以及个人的影响程度判定，从高到低划分为 4 级特别严重危害、3 级严重危害、2 级一般危害、1 级无损害共四个等级。

Data Security Levels: Based on the potential impact on the Company and individuals, data is classified into four security levels, from highest to lowest: Level 4 (critical impact), Level 3 (serious impact), Level 2 (moderate impact), and Level 1 (no impact).

3. 国家数据等级：是公司为满足国家各监管部门定期审查要求，对数据进行的分级。参考《数据安全技术数据分类分级规则》内容，按照数据对国家安全、公共利益、公司权益、个人权益的影响程度进行数据分级，分为“重要数据”“一般数据”两个级别。

National Data Grades: To meet periodic review requirements from national regulators, we classify data in accordance with the Data Security Technology—Rules for Data Classification and Grading. Based on the potential

impact on national security, public interest, corporate rights, and individual rights, we classify data into two grades: "important data" and "general data."

四、车端/APP/云平台/外部数据合规收集 Collection of Vehicle/APP/Cloud Platform/External Data

（一）车端数据收集规范 Vehicle Data Collection Standards

1. 车端交付时默认关闭非必要数据的收集功能，用户可以自主选择与同意增强服务功能的数据收集。同时在用户使用阶段，提供“全隐私模式”选项，用户可一键关闭车端与车联网平台的数据传输（不包括法规要求的数据上传）。

Upon vehicle delivery, the collection of non-essential data is disabled by default. Users may independently choose whether to consent to data collection for enhanced services. During vehicle use, a “Full Privacy Mode” is also available, allowing users to disable data transmission between the vehicle and the connected-vehicle platform with a single click, except for data uploads required by applicable laws and regulations.

2. 车辆诊断数据在采集阶段即进行去标识化技术处理，非必要实时数据在本地存储中遵循最小化与定期清理原则。

Vehicle diagnostic data is de-identified at the point of collection, while non-essential real-time data stored locally is subject to the principles of data minimization and periodic deletion.

（二）APP 数据最小化采集 APP Data Minimization

1. 分场景申请权限，首次启动仅请求基础功能权限。

Permissions are requested as needed based on specific scenarios, with only essential permissions requested upon first launch.

2. 提供权限单独管理界面，支持随时撤回授权。

A dedicated permission management interface is provided, allowing users to withdraw their consent at any time.

（三）云平台数据合规管理 Cloud Platform Data Compliance Management

1. 建立数据收集事前评估机制，新增收集需通过合规评审。

A pre-collection assessment mechanism is established, with all new data collection activities subject to compliance review.

2. 采用隐私增强技术，在数据汇聚阶段实施差异化处理。

Privacy-enhancing technologies are adopted to enable differentiated processing during data aggregation.

（四）外部数据合规引入 External Data Compliance Acquisition

1. 对通过采购、合作、授权、公开获取等方式，从自身组织边界之外获取的、用于支撑业务运营、决策分析或创新场景的数据，建立外部数据管理规范。

External data management standards are established for data obtained from outside the organization through procurement, partnerships, licensing, public sources, or other channels to support business operations, decision-making, or innovation.

2. 遵从合规先行、安全可控、权责清晰、最小必要、价值导

向等原则，通过源头把关和合同约束，避免数据引入带来的法律、合规和信誉风险。

We adhere to the principles of a compliance-first approach, security and control, clear accountability, data minimization, and value-driven data use. Through rigorous source verification and contractual safeguards, we mitigate the legal, compliance, and reputational risks associated with acquiring external data.

五、GDPR 及欧盟跨境数据传输合规 GDPR and EU Cross-Border Data Transfer Compliance

（一）跨境传输机制建设 Cross-Border Transfer Mechanisms

1. 优先采用欧盟认可的标准合同条款（SCCs）进行跨境数据传输。

We prioritize the use of EU-approved Standard Contractual Clauses (SCCs) for cross-border data transfers.

2. 在欧盟设立本地化数据中心，对核心用户数据实施区域化存储。

We establish localized data centers in the EU and implement regional storage for core user data.

（二）用户权利保障机制 User Rights Protection Mechanisms

1. 在车机系统及 APP 设置便捷的权利行使入口。

Convenient access points are provided within the infotainment systems and the app for users to exercise their rights.

2. 建立高效响应的用户权利保障流程，确保包括访问、更正、删除等在内的各项数据权利请求得到及时处理与落实。

An efficient user rights protection process is established to ensure timely handling and fulfillment of all data rights requests, including access, correction, and deletion.

（三）合规监控体系 Compliance Monitoring System

积极与欧盟认证机构合作，持续获取隐私保护认证。

We actively cooperate with EU certification bodies and continuously obtain privacy protection certifications.

六、数据安全与隐私保护 Data Security and Privacy Protection

（一）管理与技术双重防线守护数据全生命周期安全 Dual Management and Technical Safeguards for Lifecycle Data Security

1. 完善数据安全管理体系，明确各单位数据安全负责人和管理机构，落实数据安全保护责任。

We improve the data security management system, designate data security officers and management bodies in each organizational unit, and clearly assign data security responsibilities.

2. 仅基于明确、合法的业务目的，在必要的存储期限内，以安全、合规的方式存储数据。

We store data in a secure and compliant manner only for clear, legitimate business purposes and within necessary retention periods.

3. 持续进行数据安全制度建设，建立数据分类分级保护制度，建立数据安全风险评估、报告、信息共享、监测预警机制，建立数据安全应急处置机制，建立数据出境安全管理机制。

We continuously strengthen our data security governance framework by developing a data classification and grading system, and implementing mechanisms for data security risk assessment, reporting, information sharing, monitoring and early warning, emergency response, and cross-border data transfer security management.

4. 从网络安全防护、身份鉴别与访问控制、监测预警、数据加密、数据脱敏、数据防泄漏、数据接口安全、数据备份与恢复、安全审计等方面构建完善的数据安全技术体系。

We establish a comprehensive data security technology framework covering network security, identity authentication and access control, monitoring and early warning, data encryption, data masking, data loss prevention, data interface security, data backup and recovery, and security auditing.

5. 按照数据分类分级结果对数据实施全生命周期差异性防护措施，重点防护国家重要数据、公司数据安全级别 3 级、4 级数据以及个人信息数据。

Based on data classification and grading results, we implement differentiated protection measures throughout the data lifecycle, with enhanced protection for nationally designated important data, company data classified as

security levels 3 and 4, and personal information.

6. 对于不再需要或依法应删除的个人信息，我们将按规定进行安全删除或匿名化处理。

For personal information that is no longer needed or required by law to be deleted, we securely delete or anonymize it in accordance with regulations.

（二）尊重保障个人权益严控隐私泄露 Respect and Protect Individual Rights, Strictly Prevent Privacy Leakage

1. 制定统一客户隐私政策，在销售、车机、APP 等全触点清晰告知数据收集目的、范围、使用方式及留存期限，获取明示、自愿、单独授权；客户可随时查询、更正、删除个人信息，撤回授权，保障数据自主权与控制权；未经客户明确同意，不向他人提供其个人信息。

We formulate a unified customer privacy policy and clearly inform customers, across all touchpoints including sales, infotainment systems, and APPs, of the purpose, scope, methods, and retention period of data collection, while obtaining their explicit, voluntary, and separate consent. Customers may access, correct, or delete their personal information, or withdraw their consent at any time, ensuring their autonomy and control over personal data. We do not disclose customers' personal information to third parties without their explicit consent.

2. 严格遵守员工个人信息保护管理相关办法，仅收集、使用必要的员工信息，不泄露、不滥用、不非法提供员工个人信息；员工信息加密存储、严格访问控制，尊重员工隐私与合法权益。

We strictly comply with our employee personal information protection policies, collecting and using only the employee information necessary for legitimate business purposes, and never disclosing, misusing, or unlawfully sharing employees' personal information. Employee personal information is encrypted at rest and protected through strict access controls, ensuring respect for employees' privacy and legitimate rights and interests.

3. 采取技术措施和其他必要措施，确保个人信息安全，防止信息泄露、篡改、毁损。

We adopt technical and other necessary measures to ensure the security of personal information and prevent its leakage, tampering, or destruction.

4. 建立隐私泄露监测、预警、处置、通报全流程机制及隐私保护技术能力，一旦发生数据泄露，立即启动应急预案，采取止损措施，及时通知受影响主体并向监管报告，最大限度降低损害。

We have established end-to-end mechanisms for privacy breach monitoring, early warning, incident response, and notification, supported by privacy protection technologies. In the event of a data breach, we immediately activate our emergency response plan, take measures to contain the incident, promptly notify affected individuals and report to relevant regulators to minimize potential harm.

七、零容忍政策 Zero-Tolerance Policy

1.零容忍与纪律处分：公司实行数据安全“零容忍”政策。对于违反数据安全管理规定、非法泄露或滥用个人信息的行为，将参照公司规章制度予以扣减个人绩效、行政降职等处分。

Zero Tolerance and Disciplinary Measures: The Company enforces a zero-tolerance policy toward violations of data security requirements. Violations of data security regulations or unlawful disclosure or misuse of personal information will be subject to disciplinary measures, including performance rating deductions and administrative demotion, in accordance with the Company's policies.

2.法律责任追究：任何违反隐私政策和数据安全规定的组织或个人，除面临内部纪律处分外，涉及民事或刑事责任的将送司法机关追究相关责任。

Legal Liability: Organizations or individuals that violate privacy policies or data security regulations will be subject to internal disciplinary measures. Where civil or criminal liability is involved, the matter will be referred to the relevant judicial authorities for investigation and legal action.

3.问责制度：建立问责机制，确保所有违规行为都能追溯到具体的责任人，并受到与其行为性质和影响相匹配的惩处。

Accountability System: We establish an accountability mechanism to ensure that all violations can be traced to the responsible individuals and are subject to disciplinary measures commensurate with the nature and impact of

their misconduct.

八、独立审计与监督机制 Independent Audit and Oversight Mechanism

1. 外部独立审计：公司将定期聘请具备资质的独立第三方机构对数据处理活动进行专项审计，验证公司实践是否符合法律法规及内部政策的要求。

External Independent Audit: We regularly engage qualified independent third-party institutions to conduct targeted audits of our data processing activities, in order to verify compliance with legal and regulatory requirements and internal policies.

2. 常态化内部审计：建立常态化的内部审计机制，定期对各部门的数据安全合规情况进行监督检查，及时发现并堵塞管理漏洞。

Regular Internal Audit: We establish a regular internal audit mechanism to inspect and supervise the data security compliance of each department, promptly identifying and closing management gaps.

3. 持续改进闭环：通过内外部审计结果的反馈与分析，持续优化公司的数据保护控制措施和管理策略，形成“检查–整改–提升”的闭环管理。

Continuous Improvement Cycle: Through feedback and analysis of internal and external audit results, we continuously optimize our data protection

controls and management strategies, forming a closed-loop process of inspection, remediation, and improvement.

九、附则 Supplementary Provisions

本宣言已由董事会战略、投资与可持续发展委员会审查并批准通过，自发布之日起生效实施。

This Statement has been reviewed and approved by the Board's Strategy, Investment and Sustainability Committee and shall take effect from the date of its issuance.

本宣言由长安汽车 ESG 工作部负责解释和修订。

This Statement shall be interpreted and revised by the Changan Automobile ESG Department.

长安汽车将每三年审阅本宣言，并为适应法律法规的变化或公司发展进行相应内容的修订。

Changan Automobile will review this Statement every three years and revise its content as necessary to adapt to evolving legal and regulatory requirements or the development of the Company.

本声明以简体中文和英文两种文字书就。在两种文本理解发生歧义时，应以简体中文文本为准。

This Statement is issued in both Simplified Chinese and English. In the event of any discrepancy, the Simplified Chinese version shall prevail.