



汽车制造商原始设备制造商需要了解中国网络安全法规的哪些要点？

中国是全球汽车市场的重要组成部分，其每年新车销量占全球三分之一，这一数字预计在未来几年仍会增加。由世界汽车法规协调论坛（WP.29）和国际标准化组织（ISO）等理事机构制定的新国际网络安全法规已出台，中国顺势开始确立本国监管框架，也在情理之中。预计到2025年，中国将出台97项法规，目的是减少智能网联汽车（ICV）和电动汽车（EV）使用[软件在线升级功能](#)和更新系统的相关风险。此类法规既是确保驾驶员人身安全、车辆安全和社区安全，也是保护个人和国家数据安全的必要条件。

如果国外汽车制造商们想要在中国市场继续财运亨通，无疑需遵守中国政府的所有法律法规。那么，中国网络安全法是什么？如何影响OTA系统、智能网联汽车和电动汽车？最关键的是，汽车制造商实现合规性的不二法门是什么？请您继续往下看，找出答案。

中华人民共和国网络安全法

2017年出台的[《国家网络安全法》](#)是关乎智能网联汽车和电动汽车的最重要法律之一。依据《国家网络安全法》，任何借助计算机或其他技术收集、储存、处理、传输和发布数据的“供应商”必须遵守特定法规。《国家网络安全法》适用范围包含智能网联汽车和电动汽车，有三点需要特别说明。

第一点，要求制定相关制度流程保护关键信息，例如施行内部安全管理系统，评定和减少网络攻击和安全漏洞。汽车制造商须每年评估其系统和设备风险，确定可能的违规行为及当前预防措施是否充分；再将评估结果上报给国务院等相关政府部门，获得合格证书。

第二点，《国家网络安全法》规定了个人信息保护的相关要求。汽车制造商们只能经用户同意后收集个人信息，且不得向未授权方传输用户数据；此外，还需配套数据保护措施和补救计划，减轻违规行为的影响。该法规定，从“关键网络”（如交通或运输网络）收集的任何个人数据必须储存在中国境内服务器上。

最后一点，《国家网络安全法》规定了收集、储存和管理重要数据保护的设备和产品的相关要求。任何技术服务或产品（包括智能网联汽车）获得中国市场准入之前，必须证明其符合所有中国国家安全标准和

要求。2020年6月，随着中国的网络安全审查措施的出台，这一范围扩大。当前，汽车制造商须预判其违规行为对中国当地的影响程度，预估其产品对中国国家安全的风险，上报所有调查结果至网络安全审查办公室，以便进一步评估。

中国工信部和中国国家标准化管理委员会的网络安全标准

《国家网络安全法》并不是为汽车行业量身定制，但中国有若干负责智能网联汽车和电动汽车监管的委员会。自2017年以来，中国工信部(MIIT)和中国国家标准化管理委员会不间断发布关于发展国家车联网(IoV)行业标准体系的指导方针。该体系分为五类，涵盖智能网联汽车的车联网行业标准。

预计到2025年，将出台约100项智能网联汽车指导方针，其中近30项关乎网络安全。尽管中国工信部在努力构建车联网标准体系，但仍由中国国家标准化管理委员会负责落实新网络安全任务。

TC114/SC系全国汽车标准化技术委员会智能网联汽车分技术委员会，负责中国电动汽车安全法规和标准制修订工作。该委员会的具体责任为：LTE-V2X通信、信息安全、信息泄露预警系统、车辆密码和数字证书的标准制定；监督国际标准一体化进程，此部分将在下文详细叙述。

需要注意的是，如果出现分歧，中国国家标准化管理委员会制定的任何标准以《国家网络安全法》为准。

中华人民共和国个人信息保护法

[《中华人民共和国个人信息保护法》](#) 2021年11月起施行，主要对国外在华机构使用个人信息进行全面的数
据保护监管，并对借助OTA软件收集的数据产生直接影响。《中华人民共和国个人信息保护法》一共74条，绝大多数条款直接取自[《通用数据保护条例》](#)，因此该法与国际标准大同小异。

与国际标准接轨

“中国制造”标志长期以来是批量生产廉价产品的代名词，而中国决定以“中国智造2025”国家战略改变这种看法，该战略旨在使中国从劳动密集型制造业过渡到技术密集型行业先锋，特别是在绿色能源和汽车行业。为加快这一进程，中国已将其诸多OTA标准建立在现有国际法规基础上。

联合国欧洲经济委员会 世界车辆法规协调论坛

中国智能网联汽车新标准的第202项第21条，全国汽车标准化技术委员会智能网联汽车分技术委员会参考[《软件升级及管理系统》](#)，制定了车辆软件更新系统的技术要求，还参考《信息安全及管理系统》制定了第202项第22条规定。因此，希望中国实现合规性的外国汽车制造商可以参考以上联合国法规。

然而，联合国世界车辆法规协调论坛的标准和全国汽车标准化技术委员会智能网联汽车分技术委员会的标准主要区别在于，《信息安全及管理系统》虽然规定“制度流程”必须配套，从而防止数据操纵，保持数据更新，确保数据安全，但并未具体说明何谓“制度流程”，给予汽车制造商摸索解决方案方面的自由；但中国智能网联汽车标准就不那么灵活，涵盖测试程序、制度流程和预期的详细规范。

联合国欧洲经济委员会法规的详细信息，请参阅我们的[WP.29博客系列](#)。

国际标准化组织规定

除了参考联合国世界车辆法规协调论坛的标准，全国汽车标准化技术委员会智能网联汽车分技术委员会也参考若干ISO规定，以制定国家标准。[ISO 21434](#)从工程角度关注网络安全要求，从产品设计、生产到维修保养、报废，检查车辆生命周期的各方面。同时，[ISO 20077](#)阐明了“加长车”相关的概念，或任何超出车身物理范围的概念，包括设计限制、加长车接口和诊断过程的一般要求。

如上所述，中国已施行[ISO/IEC 27001](#)标准：《国家网络安全法》。ISO 27001和《国家网络安全法》均对信息安全管理系统提出详细要求。虽二者与汽车行业不完全相关，但对OTA软件更新系统的开发、实施和使用影响巨大。

《通用数据保护条例》

《通用数据保护条例》系数据保护法，适用于欧盟境内的数据主体。数据处理者们（如OTA提供商和智能网联汽车公司）必须遵守《通用数据保护条例》，前提是：

- 交易的是提供商品和服务的数据，即使在不需要付款的情况下也是如此，或
- 监视人们的行为

《中华人民共和国个人信息保护法》采用同样的保护原则，但仅针对中国境内的数据主体。尽管《通用数据保护条例》和《中华人民共和国个人信息保护法》大体一致，例如强制员工培训和允许代表数据主体提起集体诉讼，但汽车制造商需要注意几点关键性差异。

《中华人民共和国个人信息保护法》限制数据可移植性权利，要求数据处理者为人们提供安全“通道”，只有在满足规定的安全条件时才会启动数据传输。《中华人民共和国个人信息保护法》规定了跨境支付的三个程序：

1. 单独取得数据主体个人的同意
2. 保护影响评估必须由数据运营者执行并记录
3. 必须采用《中华人民共和国个人信息保护法》认可的方式确保充分的安全保障措施

此外，《中华人民共和国个人信息保护法》要求每个外国数据处理者派一名驻华代表。尽管其使用《通用数据保护条例》的“合法基础”方法进行数据处理，但“合法权益”并不能作为访问或收集个人数据的理由。《中

《中华人民共和国个人信息保护法》将个人财务信息归类为“敏感”信息，而《通用数据保护条例》并未有类似规定，还提供事后数据权限。一旦发生数据泄露，《中华人民共和国个人信息保护法》要求数据处理者立即通知通知，而《通用数据保护条例》规定的宽限期为72小时。

尽管中国工信部是最有可能参与智能网联汽车行业的政府部门，但《中华人民共和国个人信息保护法》涉及多个政府部门。有违法行为，处年度收入5%的罚款，但尚不清楚是以全球年度收入还是中国区年度收入为准。

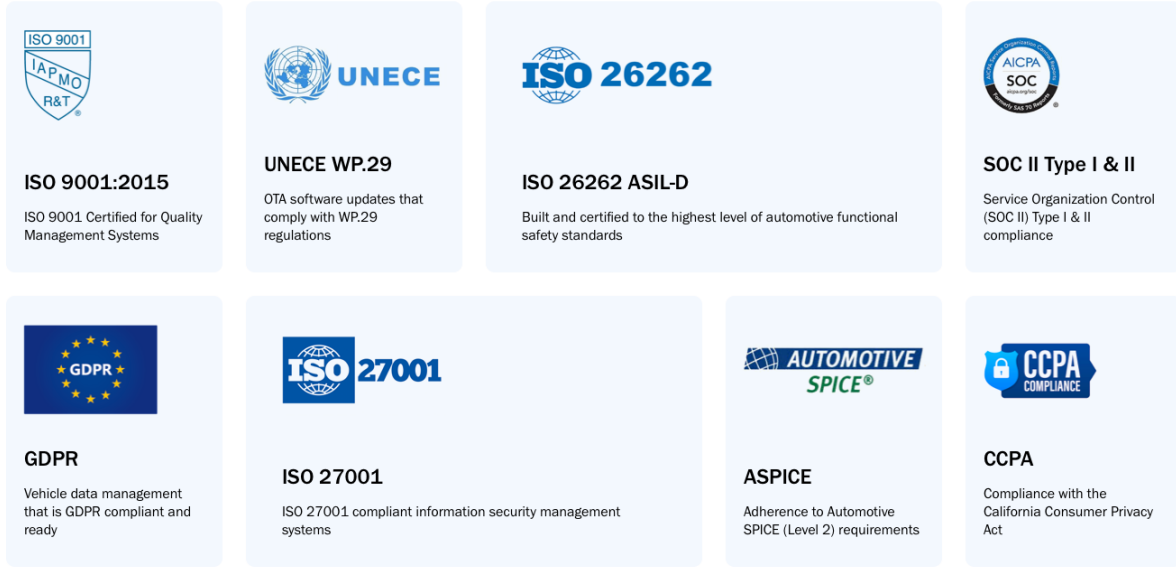
与Sibros 助您实现全球合规性

无论您关注中国或是其他国际网络安全法规，有一点可以确定：想要在汽车行业继续享有竞争优势的汽车制造商必须遵守上述法规。智能互联汽车和电动汽车是汽车行业的未来，但没有全车OTA软件解决方案，就没有未来。

可以选择在汽车内部构建兼容性OTA软件解决方案，但风险极高。除详细了解所有国际法规外，汽车制造商还需配备行业专家智库构建解决方案。即便如此，失败、延误、意外支出和僵局也可能纷至沓来。

与其在版图上浪费时间，不如选择更快速可靠、经济高效的预警解决方案。[Sibros Deep Connected Platform\(DCP\)](#)不仅为汽车制造商提供易于融合、无代码的解决方案，可用于实时数据记录、远程软件更新和[降低远程通信运营成本](#)，而且符合以下国际标准：

Certification & Compliance



图片从上到下，从左到右：

<p>ISO 9001:2015 ISO 9001质量管理体系</p>	<p>联合国欧洲经济委员会 世界车辆法规协调论坛 OTA软件更新符合世界车辆法规协调论坛制定法规</p>	<p>服务组织控制 (SOC II) 一型 &二型 合规性</p>	<p>ISO 27001合规性 信息安全管理 系统</p>
<p>ISO 26262 以构建严格的功能性安全标准</p>	<p>《通用数据保护条例》 汽车数据管理即将要符合 《通用数据保护条例》要求</p>	<p>CCPA 符合《加利福尼亚州 消费者隐私保护法》</p>	<p>ASPICE 符合《汽车软件流程改进和能力测定》(二级)要求</p>

作为汽车生产商，您不应该也不必亲自在OTA解决方案标准和网络安全法规方面寻求出路。今天[联系 Sibros](#)，我方将为您演示，并使您的团队赢在未来做好准备。

