



TABLE OF CONTENTS



Introduction

Bird's Eye View

Executive Summary

The Basics

Analysis

Summary Tables

Next Steps

Contact Us

RELATED SBD REPORTS



528 – Connected Car Legislation Guide

The Connected Car Legislation Guide provides an in-depth analysis of how and where legislation is impacting on automotive connected services.

It identifies the threats and opportunities generated by government mandates, licensing requirements, restrictions, policies, and guidelines within Europe, USA, China, Russia and Brazil.



Cyber Security

#539

Cyber & SDV Legislation Tracker

A comprehensive guide to the cyber security legislation, best practice guidelines and technical standards that impact on in-car and off-board systems.

The Automotive Cyber Security Legislation Guide identifies the threats and opportunities generated by government mandates, guidelines and standards within Europe, USA, China and Japan. Information is also provided on relevant legislation from other countries around the world on an ad-hoc basis when an important development emerges.

The Automotive Cyber Security Legislation Guide has been designed to be a usable reference tool, highlighting the important requirements whilst noting legacy and outdated publications so that you can confidently focus your attention on the issues that matter. The Guide provides the background and timeline of each piece of legislation, best practice and standards, and SBD's Cyber Security team has gone further, showing the implications and where you need to be looking, allowing the Legislation Guide to become a vital part of a robust cyber security strategy.

COVERAGE



GLOBAL



NA



CHINA



EUROPE

FREQUENCY



ANNUALLY



QUARTERLY



ONE-OFF

PUBLICATION FORMAT



PDF



POWERPOINT



EXCEL



ONLINE

PAGES



50+

Request price



Key questions answered

- > What threats and opportunities are generated by government mandates, guidelines and standards?
- > What are the key relevant legislation points from other countries on new policies?
- > What exactly the best practices & standards for complying with all cyber security legislation?
- > How should we be looking at our business to evaluate our cyber security compliance?

This research supports



PRODUCT PLANNERS



ENGINEERS



MARKETING



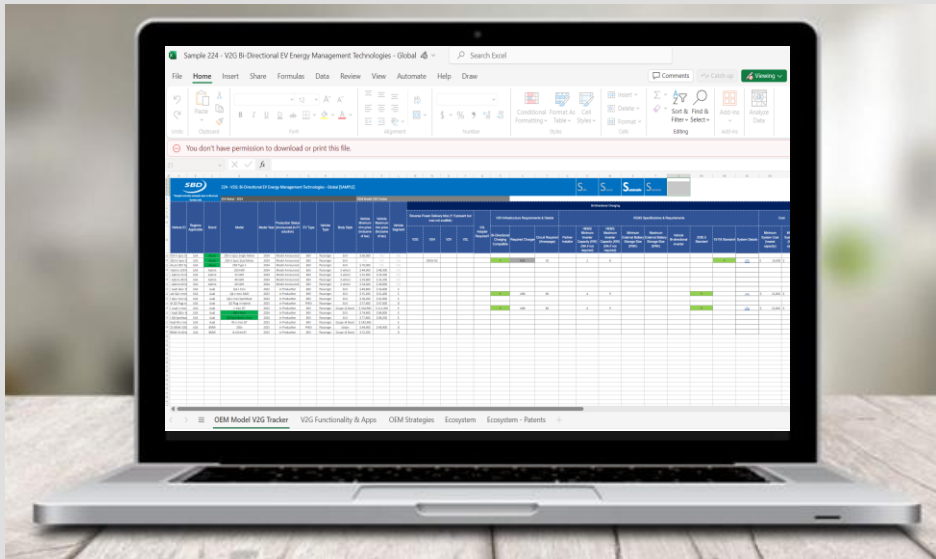
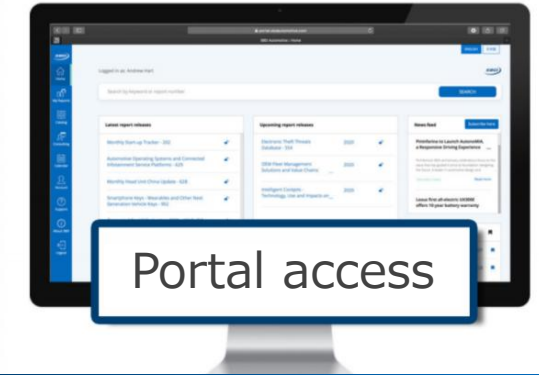
C-SUITE

Do I have access?

100+ Reports published per year

50k+ Slides of insights, forecasts & data

4,000+ # of auto professionals who access our reports



View Excel Data Sheet Sample

Cyber & SDV Legislation Tracker

For a deep dive into the background and timeline of each piece of legislation, best practice and standards

Click for Sample





[Request price](#)



Cyber & SDV Legislation Tracker

539 - Cyber & SDV Legislation Tracker

[Introduction »](#)

4

[Executive Summary »](#)

6

[The Basics »](#)

11

[Analysis »](#)

16

- EU Data Act
- EURO 7 regulation
- EU Cyber Resilience Act
- Protective Security Policy Framework (Australia)
- UK cybersecurity regulation
- UNECE regulations
- ISO/SAE 21434
- NHTSA cyber security best practices
- NIST Special Publications
- China – Cyber security standards

[Summary Tables »](#)

28

- USA – Legislation/Regulation
- USA – Guidelines & Best Practices
- USA - Standards
- EU – Legislation/Regulation
- EU – Guidelines & Best Practices
- EU - Standards
- China – Legislation/Regulation
- China – Guidelines & Best Practices
- China - Standards
- Global – Legislation/Regulation
- Global – Guidelines & Best Practices
- Global - Standards

[Legislation Bird’s Eye View »](#)

43

[Next Steps »](#)

49

[Contact Us »](#)

53



Data Deep Dive
View and analyze deep data in your own way



Customer Feedback
Provide your feedback to SBD regarding this report





Introduction


Industry is proactively introducing more ADAS ahead of policy deadlines

The digitization of modern cars continues to progress rapidly with an ever-rising penetration of connected and automated functionalities. However, this influx of new features has also exposed the cars to external vulnerabilities from a cyber security point of view. The security researchers have found out various 'gateways' through which malicious hackers can get access to the mission-critical elements in the car.

The **Cyber Security Legislation Guide** identifies the threats and opportunities generated by government mandates, guidelines and standards primarily within Europe, USA, China and Japan (and elsewhere). Information is also provided on relevant legislation from other countries around the world on an ad-hoc basis when an important development emerges.

The **Cyber Security Legislation Guide** has been designed to be a usable reference tool, listing the important and the most recent announcements whilst also highlighting the learnings from legacy/outdated publications so that the readers can confidently focus their attention on the issues that matter. The Guide provides the status and timeline of each piece of legislation, best practice and standards, and SBD's team has gone further, discussing some of the most relevant topics in detail allowing the Legislation Guide to become a vital part of a robust cyber security strategy.

Note: This guide only highlights the actual regulatory activities and does not give any recommendations. This guide's analytical and forward-looking statements shouldn't be construed as legal advice.

Layer	Section	Conclusion
STRATEGY & IMPACT	Executive Summary	This section highlights some of the recently enforced and introduced regulations/legislations/guidelines across the regions
	The Basics	A brief overview of the different type of legal aspects (regulation, legislation, standards etc.) covered in this report along with the regions in focus.
LEARNING & ACTION	What's New?	Not applicable
	Analysis	Key regulatory activities that are impacting the automotive cybersecurity ecosystem and key cyber security standards published by the authorities
CORE INSIGHTS	Summary Tables	In summary, legislative activities are increasing, and some laws are nearing enforcement. In contrast, some haven't seen the light of day after being introduced and debated several times.
DATA DEEP DIVE IN EXCEL	Deep Dive	 View and analyze deep data in your own way
	Geographies	
	Legislations/Regulations	
	Standards	
	Definitions	
CONTEXT	Birds Eye View	An overview of the tangential trends to this topic, as identified in SBD's neighboring products
	Future Outlook	Not applicable
	Next Steps	Can SBD help you with any unanswered questions?

Example slides from the report



Request price >



Snapshot of key regulatory activities

	Introduced* Legislation/Regulations recently introduced	Enforced/Published** Legislation/Regulations recently enforced
Global	No new regulations were introduced recently	The Cyber Security Act 2024 (Malaysia) The act establishes the National Cyber Security Committee, defines the Chief Executive of NACSA's duties, outlines roles for NCII sector leads and entities, addresses NCII-related cyber threats, and regulates cybersecurity service providers through licensing.
China	Regulations on Network Data Security Management The regulations aim to standardize network data processing activities, ensure data security, and promote the lawful and effective use of network data.	Artificial Intelligence Security Governance Framework 1.0 version These measures aim to ensure the safety and reliability of connected vehicles using AI technology, promoting the healthy development of intelligent transportation systems.
Europe	The new British government is planning to introduce a Cyber Security and Resilience bill (bill to be presented in UK sometime in 2025)	Regulation (EU) 2024/1257 Euro 7 goes beyond traditional emissions standards by addressing the cybersecurity of connected and software-driven vehicles, ensuring their emissions systems remain tamper-proof and secure throughout the vehicle's lifespan. (Enforced May 2024 and no new updates ever since)
USA	SB 1053 (New Mexico) Bill proposes amendments to the Cybersecurity Act, including changes to the overseeing office (currently under consideration) Insure Cybersecurity Act of 2025 Committee on Commerce, Science, and Transportation. Ordered to be reported without amendment favorably on 5th February 2025 (the bill is dead as of Jan 2025)) Data Protection Act of 2024 To establish a federal Data Protection agency that will oversee and enforce data privacy and protection regulations in the United States (the bill is dead in the committee and needs to be reintroduced)	Executive Order on Improving the Nation's Cybersecurity Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices, requires agencies to comply with the NIST Guidance. Strengthening and Promoting Innovation in the Nation's Cybersecurity Encourages AI-driven cybersecurity and post-quantum cryptography (enforced in Jan 2025)

*In some regions the word 'issued', 'proposed' for the legislation that are used

**Standards and Guidelines/Best Practices are often not enforceable by law. They are introduced and reviewed by the subject experts before being published.



New EU Data Act complements the existing GDPR

Regulation Overview

Status	Introduced	✓	Draft	Enforced
--------	------------	---	-------	----------



The Data Act aims to foster a fair, competitive, transparent data economy. It regulates data access, usage, and sharing to ensure that no one entity can monopolize the data generated by devices or services. For businesses and individuals, this means more control over the data they generate. The Data Act enables users of connected products (e.g. **connected cars, medical and fitness devices**, industrial or agricultural machinery) and related services (i.e. anything that would make a connected product behave in a specific manner, such as an app to adjust the brightness of lights, or to regulate the temperature of a fridge) to access the data that they co-create by using the connected products/ related services.

Details

Scope of 'Data Act'

For the data related to the connected product to fall under the scope of the Data Act, the product needs to have been placed on the Union market, and it needs to be non-personal data (personal data is covered in GDPR)

- **Product Data** – Data obtained, generated, or collected by a connected product (e.g., smartphone, industrial machinery, or medical devices) and related to its performance, use, or environment. Purely descriptive data is not product data.
- **Related Service Data** – Data representing user action, inaction, and events related to the connected product during the provision of a related service (e.g., apps that regulate the fridge's temperature or adjust the brightness of lights).

What's New?

What does the new Data Act entail?

In recent years, there has been a rapid growth in the availability of products connected to the internet ('connected products') on the European market. These products, which together compose a network known as the Internet-of-things (IoT), significantly increase the volume of data available for reuse in the EU. This represents a huge potential for innovation and competitiveness in the EU.

The Data Act will enable a fair distribution of data value by establishing clear and fair rules for accessing and using data within the European data economy, a necessity heightened by the growing prevalence of the **IoT and connected cars**. Connected products will have to be designed and manufactured to empower users (businesses or consumers) to easily and securely access, use and share the generated data.

The Data Act is a cross-sectoral piece of legislation (i.e., it lays out principles and guidelines that apply to all sectors). It does not modify existing data access obligations, however, **any forthcoming legislation should align with its principles**.

The European Commission will cover some requirements related to interoperability in data spaces within the "European Trusted Data Framework". The request is expected to be formally adopted by the end of 2024. An Expert Group managed by the European Commission is currently developing model contractual terms for data sharing and standard contractual clauses for cloud computing contracts. The European Commission is expected to adopt them before September 12, 2025.

The European Commission published an updated set of FAQs pertaining Data Act in January.

Key Takeaways

The EU Data Act is poised to bring about significant changes and benefits. Consumers will have more options for repair services, potentially reducing costs. Businesses can leverage data access to offer innovative services, enhancing their competitiveness. However, the consumers and businesses alike may have difficulty understanding the harmony between this new Data act and the already existing list of similar acts related to data privacy and security.



China is developing its own automotive cyber standards

Standard Overview

Status	Introduced	Draft	✓	Published
--------	------------	-------	---	-----------



Whilst the rest of the world has focused on global ISO/SAE 21434 to embed cyber into the development process, China is developing its own standards that recommend specific technologies and/or security controls for critical in-car and off-board systems.

The National Information Security Standardisation Technical Committee (TC260) in China recently announced the release of 12 national cybersecurity standards. These standards cover various areas including entity authentication, information system security assurance, public key infrastructure, VPN access, and data security.

Details

Legislation: GB Cyber Requirements

The Chinese Ministry of Industry and Information Technology (MIIT) has plans to introduce over 100 optional standards relating to automotive cyber security by 2025. However, in 2021 the MIIT announced that the following two of the standards would be upgraded to mandatory GB, meaning that all OEMs must comply with the requirements:

- **Cybersecurity technical requirements and test methods for whole vehicle**
- **General technical requirement of vehicles software update.**

For OEMs that have already started implementing UNECE R155 and are looking into implementing R156 there is minimal rework expected, as it is understood the two new standards will be similar to and that they align with UNECE R155 and R156 respectively. The implementation timing is expected to be for new models type approved from mid-2023.

Standard: China GB/T- Automotive Standard

The GB/T cyber standards are being developed in batches.

- In March 2022, the first batch of GB/T automotive cyber standards have been published and status updates provided on the second batch. In September 2022, minor updates on availability of draft GB/T standards

The majority of China's automotive cyber standards will be published as GB/T recommended national standards (although 2 will be GB mandated national standards), but it is expected that most domestic OEMs will formally adopt the requirements for their future models. It is unclear if the recommended standards will be mandated, or if OEMs will suffer any indirect penalty for not adopting the standards, but as a first step all domestic and foreign OEMs should at least audit their systems against the requirements to establish their current baseline position.

Key Takeaways

China is creating unique standards for automotive cybersecurity, in contrast to the global approach of integrating it into the development process through ISO/SAE 21434. These standards by China suggest particular technologies and security measures for crucial in-car and off-board systems. This legislation is known as GB Cyber Requirements, while the corresponding standard is referred to as China GB/T- Automotive Standard.

What's New?

Some recently published standards in China are as follows:

ICV specification standard for raw data

This standard specifies the process and operational requirements for the collection of raw data for intelligent networked vehicle scenarios, including general requirements, types of data to be collected, data collection equipment requirements and data collection requirements, etc.

YD/T 4974-2024: This standard outlines the technical specifications for the interface between security situation awareness platforms and supervision platforms within the Internet of Vehicles network. [Link](#)

YD/T 4908-2024: This standard outlines the technical specifications for ensuring the information security of digital car keys that operate via mobile internet. [Link](#)



USA – Regulation & Legislation

Latest activity vs status

About the policy activity placement in the grid

		Status		
		Introduced	Drafting	Enforced
Last updated	Last quarter	1 2 3		
	3-12 months			4
	Older			

S. No	Name of the law	Recent development(s)	Next activity/milestone
1	To Create The Arkansas Cybersecurity Act Of 2025 (Arkansas)	The bill aims to establish comprehensive governance standards and procedures for state agencies, ensuring a unified approach to cybersecurity across Arkansas.	Referred to the Committee on Commerce, Science, and Transportation (no recent activity)
2	To establish a cybersecurity task force (Connecticut)	The bill proposes the establishment of a cybersecurity task force to enhance the state's cybersecurity posture.	Referred to the Committee on Commerce, Science, and Transportation (no recent activity)
3	Insure Cybersecurity Act of 2025 (Federal)	The bill aims to enhance the clarity and effectiveness of cyber insurance policies, particularly for small businesses, by directing the National Telecommunications and Information Administration (NTIA) to establish a working group focused on cyber insurance.	Bill is dead as of January 2025
4	Securing the ICT and Services Supply Chain	The bill reviews transactions involving information and communications technology and services (ICTS)	Comes into effect from February 4, 2025

Key highlights

- The transactions pertain ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that may pose **undue or unacceptable risk to the United States or U.S. persons**.
- The Federal recognizes the critical need for accessible and understandable cyber insurance, especially for small businesses often lacking robust cybersecurity resources. By tasking the NTIA with forming a specialized working group, the bill aims to bridge the gap between complex insurance language and the practical needs of these businesses, ultimately fostering greater resilience against cyber threats through clearer policy frameworks and more effective coverage.



EU – Guidelines & Best Practices

Latest activity vs status

About the policy activity placement in the grid

		Status		
		Introduced	Draft	Published
Last updated	Last quarter			1
	3-12 months			2 3 4
	Older			

S. No	Name of the law	Recent development(s)	Next activity/milestone
1	The Key Principles of Cyber Security for Connected and Automated Vehicles (UK)	The government has released a handbook, “The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles,” outlining eight core principles for manufacturers and supply chain partners to ensure the security of IoT-driven vehicles. In a Parliamentary speech, the Queen emphasized the need for advanced cybersecurity measures in autonomous and electric vehicles to guarantee safe operation on UK roads.	
2	ETSI GR SAI 013 V1.1.1	ETSI releases a multi-partner Proofs of Concepts framework that is used as a tool to demonstrate the applicability of AI technology	No significant change since the last development
3	Ireland Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies)	The Minister of State at the Department of the Environment, Climate and Communications, published Guidelines on Cyber Security Specifications (ICT Procurement for Public Service Bodies) in accordance with the National Cyber Security Strategy 2019-24	Part of Ireland’s National Cyber Security Strategy 2019-2024
4	Cyber security risk management framework (UK)	New updates appended to the NCSC’s risk management guidance	No significant change since the last development

Key highlights

- The role of ETSI ISG SAI is to develop guidance to the standards community and its stakeholders so that they have a common understanding of the threats and vulnerabilities of and from AI. The work of the group is therefore informed by, and reactive to, the wider social concerns of AI as well as by the ongoing mission of **ETSI to ensure that standards are available to give assurance that security and privacy provisions are available by default to the ICT technologies that our world relies on.**

Request the price



Request price >



Contact Us



Contact SBD Automotive

Do you have any questions?

If you have any questions or feedback about this research report or SBD Automotive's consulting services, you can email us at info@sbdautomotive.com or discuss with your local account manager below.



info@sbdautomotive.com



Book a meeting

USA

UK

Germany

India

China

Japan



Garren Carr
North America
garrencarr@sbdautomotive.com
+1 734 619 7969

Luigi Bisbiglia
UK, South & West Europe
luigibisbiglia@sbdautomotive.com
+44 1908 305102

SBD China Sales Team
China
salesChina@sbdautomotive.com
+86 18516653761

Andrea Sroczynski
Germany, North & East Europe
andreasroczynski@sbdautomotive.com
+49 211 9753153-1

SBD Japan Sales Team
Japan, South Korea & Australia
postbox@sbdautomotive.com
+81 52 253 6201