

Public Consultation on

The Draft Technical Regulations for Internet-Connected Vehicles

Telecommunications Regulatory Authority
2026



Scope	
Second	The provisions of these Regulations shall apply to all companies registered in the Sultanate of Oman, and in particular the following: • Manufacturers of connected vehicles, • Licensed vehicle agents or authorized dealers, • Providers of applications and services related to internet-connected vehicles.
	The following vehicles are excluded from the application of these Regulations: • Military and security vehicles belonging to the State. • Vehicles designated for technical research and development purposes in isolated, approved environments.
Question 1: Do you have any comments on the Scope set out above? If you disagree, please kindly explain the reasons and provide us with alternative suggestions, if any.	
Definitions and Concepts	
	Connected Vehicle: Any vehicle equipped with embedded or additional communication equipment or units enabling it to send or receive data over public networks, including V2N, V2V, V2I, or V2X connectivity in all its forms.
Third	Vehicle Technical Data: information relating to the condition of the vehicle and the performance of its components, such as engine data, fault codes, battery status, and fuel consumption, without direct linkage to personal identity.
	Anonymized Technical Data: digital information generated by the vehicle's components that is completely separated from the identity of the owner, the driver, or the vehicle identification number (VIN).
	Vehicle Data: data collected by smart or connected vehicles and transmitted in real time over the internet to external systems, including information on vehicle operation, location, and driving behavior, used to support safety, predictive maintenance, and smart services such as navigation and remote diagnostics.
	Anonymized Digital Identity (UUID): a unique identifier generated locally to replace the owner's real identity in the external digital environment.
	Data Localization: a requirement to store specific data on servers and systems geographically located within the Sultanate of Oman.
	Over-the-Air Update (OTA): the process of modifying or updating vehicle software over communication networks without direct physical intervention.
	Customer Relationship Management System (CRM): an information system for storing and processing customer data and their transaction history with the agent or service provider.

	Secure Gateway: a technical component that separates the local environment from external systems to ensure that data is free of real personal identifiers.
	Global Cloud Service Provider: any entity outside the borders of the Sultanate of Oman that provides vehicle data processing or storage services.
	UICC: a secure smart card used in mobile communication devices to store subscriber data and applications related to telecommunications services and subscriber identification.
	Connected Vehicle Service Provider: the legal person licensed or authorized to provide, operate, or manage connected vehicles through the collection, transmission, or processing of data between the vehicle and telecommunications networks and digital platforms.
	Sensitive Data: a category of data that reveals biometric characteristics, health condition, or other data of a special nature, the processing or disclosure of which may pose higher risks to a person's privacy and rights.
	Personal Data: data or information relating to an identified or identifiable natural person, directly or indirectly, that is collected, processed, or transmitted.
	Software Update Management System: a system or platform used to centrally organize, distribute, and install software updates, with the aim of improving performance, fixing errors, and closing security gaps in the systems and applications used within the entity or on users' devices.
	Emergency and Public Safety Reporting Centers: dedicated call centers for receiving emergency reports related to incidents from citizens or residents, and subsequently directing them to the competent authorities to ensure rapid response and effective intervention.
	Roadside Assistance Service: an immediate support service provided to drivers in the event of a vehicle breakdown or problems encountered while driving, including services such as tire changes, jump-starting the vehicle when the battery is depleted, fuel delivery, and towing the vehicle to repair shops or designated maintenance locations.
	eSIM: a subscriber identification unit embedded within the device, enabling the subscriber to subscribe to and activate mobile communication services without the need to use a physical SIM card
Question 2: Do you have any comments on the definitions set out above? If you disagree, please kindly explain the reasons and provide us with alternative suggestions, if any	
Communication SIM Cards	
Fourth	Contracting with companies licensed in the Sultanate of Oman to obtain the communication SIM cards used in providing the service.
	Using UICC and eSIM communication SIM cards dedicated exclusively to vehicles; the Authority's prior approval must be obtained if any other type of SIM card is used.

	Directive No. (1153/2/2022/7) issued by the Telecommunications Regulatory Authority regarding the use and activation of SIM cards dedicated to IoT services in vehicles, using designated numbers beginning with level "4", and in compliance with all directives issued by the Authority in this regard.
Question 3: Do you have any comments on the types and technologies of communication SIM cards set out above? If you disagree, please kindly explain the reasons and provide us with alternative suggestions, if any	
Emergency Communications and Roadside Assistance Service	
Fifth	When activating the emergency call service, the connected vehicle service provider shall program and route emergency calls issued from connected vehicles, connecting these calls directly to the hotline of the Royal Oman Police Operations Center (9999) or any other emergency number designated by the competent authorities for vehicle incidents, ensuring compliance with the relevant laws, regulations, and rules.
	When providing the roadside assistance service, the connected vehicle service provider shall provide the service through its own direct local call center within the Sultanate of Oman, or under a contract with a third-party local service provider authorized by the Authority, in accordance with the regulations and legislation in force in the Sultanate of Oman.
Question 4: Do you agree with the requirement to route communications directly to in-country call centers? If you disagree, please kindly explain the reasons and provide us with alternative suggestions, if any	
Data Governance	
Sixth	First: Data Minimization Data collection and processing must be limited to the minimum necessary to achieve the specific purpose of the service, and no additional data that is unnecessary or not directly related to the processing objectives may be collected.
	Second: Purpose Limitation The collection and processing of personal data must be limited to specific and legitimate purposes after obtaining the data owner's prior consent, and it is prohibited to use this data for any purpose incompatible with the purpose for which it was collected.
	Third: Transparency Users must be provided with clear and understandable information about the nature of the data being collected, the purposes of its processing, the mechanisms of its use, and the parties with whom this data may be shared, along with the need to obtain the user's prior written consent, which must be revocable during the period of use.

	Fourth: Data Protection The necessary technical and organizational measures must be applied to protect personal data from unauthorized access, loss, alteration, disclosure, or destruction, including encryption during storage and transmission, identity and access management, continuous monitoring, backups, and periodic cybersecurity testing, in compliance with the adopted standards and controls.
	Fifth: Retention Policy A clear data retention policy must be established and implemented and published on the official website, such that personal data is retained only for the period necessary to achieve the purpose for which it was collected, or in accordance with the legal and regulatory requirements applicable in the Sultanate of Oman, and deleted or destroyed securely upon expiry of the purpose or retention period, with deletion or destruction procedures documented in a manner that ensures auditability and compliance.
	Sixth: Traceability The traceability of data must be ensured throughout all stages of its processing, from collection to deletion, through the implementation of comprehensive electronic audit logs that document all access, modification, transfer, and deletion operations. These logs must be secure, tamper-proof, and available to the competent authorities upon request, in a manner that achieves compliance with the relevant regulatory requirements.
Question 5: What are your views on the Data Governance provisions set out above, and do they protect vehicle owners from risk? If you disagree, please kindly explain the reasons and provide us with alternative suggestions, if any	
Technical Architecture	
Seventh	Customer Relationship Management System First: Data Hosting and Infrastructure - The Customer Relationship Management (CRM) system must be operated within the approved infrastructure inside the Sultanate of Oman, as described in the Annex to the Regulations, with data stored in data centers authorized or approved in accordance with the applicable regulatory requirements. Second: Data Protection and Access Control - The encryption controls specified in the Annex to the Regulations, appropriate to the data, must be applied during storage and during

	transmission, ensuring the protection of its confidentiality and integrity. • Access privileges must be managed according to the principle of least privilege and based on approved functional roles, ensuring that access is restricted to authorized persons and for specified purposes only. • Sensitive data and personal data must be separated from telematics, operational, and reporting data, both technically and operationally, as described in the Annex to the Regulations. Third: Data Classification • Data must be classified according to the following categories: ○ Sensitive data, ○ Personal data, ○ Vehicle technical data. Fourth: Data Management Principles Data management must comply with the following: 1. Applying the principle of Data Minimization in all operations of data collection, processing, and sharing. 2. Maintaining written and approved policies, procedures, and documentation to fully manage all stages of data processing, including collection, processing, storage, sharing, and destruction.
	Data Protection and Privacy First: Data Protection and Security Controls • The data controller must apply the appropriate technical and organizational controls to protect data throughout its processing period, including the use of approved encryption technologies during storage and transmission, and the application of Tokenization, Masking, and Anonymization techniques, depending on the nature of the data and the purpose of its processing, in a manner that minimizes the risk of unauthorized disclosure or re-identification, and ensures that data cannot be linked to its owner except by authorized entities or systems. Second: Identity and Identifier Management • A unique indirect identifier (UUID) must be created for each vehicle and each user within the operating environment, and used in processing, integration, and data exchange operations instead of

	direct identifiers, while maintaining a mapping table linking these identifiers to the original data in a separate, secure, and encrypted environment, and applying strict access controls based on the principle of least privilege and the need-to-know principle. • An approved mechanism must be applied to renew or rotate the unique indirect identifiers (UUID) periodically, or upon the occurrence of specific operational or security events, aimed at reducing the risk of record linkage or long-term tracking, in order to ensure business continuity and traceability and auditability in accordance with regulatory requirements. Third: Protection of Personal Data and Scope of Processing • The transfer, hosting, storage, or processing of personal or sensitive data outside the geographic territory of the Sultanate of Oman is prohibited. The connected vehicle service provider must retain and store all such data exclusively in data centers within the Sultanate licensed by the Authority and the competent authorities, with processing operations limited to the minimum necessary to provide the service • Clear and transparent privacy policies and notices must be established that enable data subjects to manage their privacy settings, discontinue the service, and exercise their right to access, rectify, and delete their data in accordance with the relevant laws and legislation. Fourth: Cross-Border Data Transfer • The cross-border transfer of sensitive and personal data is regulated in accordance with the provisions of the Personal Data Protection Law and the relevant regulations and regulatory decisions Fifth: Geolocation Tracking Services • Activating vehicle geolocation tracking services by default or automatically is prohibited; explicit, prior consent must be obtained from the vehicle owner and the user before activation. • Users must be enabled to manage their privacy settings and disable the tracking service at any time, while limiting the collection of location data to the minimum necessary to achieve the specified purpose, retaining it for a period not exceeding what is necessary, and in a manner consistent with applicable policies and legal and regulatory requirements. Communications Security and Technical Architecture
--	--

	First: Monitoring, Auditing, and Compliance • All data transfer and processing operations must be subject to continuous monitoring, recording, and documentation in secure, reviewable electronic audit logs. • Effective mechanisms for detecting violations and deviations must be applied, with immediate alerts issued upon detection of any unauthorized transfer attempt or any breach of the approved controls, and the necessary corrective and preventive measures taken in accordance with the approved policies and procedures, in a manner that ensures compliance with the relevant legal and regulatory requirements. • The connected vehicle service provider shall subject all data transfer, hosting, or processing operations to a continuous monitoring and evaluation system, with detailed documentation and recording in protected electronic audit logs that are reviewable and technically verifiable. • The service provider must activate automated technical mechanisms and systems to detect violations and abnormal activities, and comply with the following immediately upon detecting any unauthorized transfer attempt or breach of data security: • Issuing immediate security alerts and notifying the Authority and the National Center for Information Safety of the incident within the legally prescribed periods. • Taking immediate precautionary measures and the necessary corrective actions to stop the breach or leak and address its effects. • Documenting the violation and the measures taken regarding it in the security incident log, to ensure auditability and regulatory compliance. Second: Secure Data Gateway • The connected vehicle service provider shall establish and activate a Secure Data Gateway, and subject all outgoing data to a filtering and automated audit structure through this gateway before it is transferred, exchanged, or shared with any external entity or environment, in order to ensure the following: • That the data is completely free of any personal or sensitive information, or indicators that could directly or indirectly identify the user. • Verification that Anonymization or digital concealment of the identity of data subjects has been completed, in accordance with the controls and standards approved by the Authority.
--	--

	• It is technically and administratively prohibited to bypass the secure gateway or to pass any data through sub-paths not subject to prior filtering. Third: Securing Communication Channels • Encrypted and secure communication channels must be used between the vehicle and the technical platforms, ensuring the confidentiality and integrity of data during transmission and reducing the risk of interception or unauthorized intrusion. Fourth: Over-the-Air Software Updates • The service provider or manufacturer shall provide a technical architecture that supports secure Over-the-Air (OTA) software updates, ensuring verification of the integrity and authenticity of updates, protection of their transmission, and the ability to restore previous versions when needed, while maintaining and managing update logs throughout the vehicle's lifecycle.
	Registration and Auditing First: Audit and Review Logs • Comprehensive electronic audit logs must be maintained for all operations of accessing, modifying, transferring, and deleting data, ensuring complete documentation of the data usage cycle and its traceability. Second: Availability of Logs to Competent Authorities • Audit logs must be made available for review by the competent authorities upon request, without restriction or condition, in accordance with the approved controls and procedures, and in a manner that ensures compliance with the relevant regulatory and supervisory requirements.
	Compliance and Standards First: Regulatory Compliance and Additional Requirements • The connected vehicle service provider must comply with all decisions, circulars, standards, and additional controls issued or adopted by the Authority, and periodically update the related

	policies, procedures, and controls to ensure ongoing compliance with the applicable regulatory requirements. Second: Information Security and Privacy Standards - The connected vehicle service provider and the manufacturer shall apply the national standards and approved international frameworks concerning information security, privacy management, and vehicle cybersecurity, and take all necessary technical, organizational, and administrative measures to ensure the confidentiality, digital integrity, and continuous, sustainable availability of data. Third: Security of Connected Vehicles - Compliance with the relevant approved international standards and practices concerning the security of connected vehicles must be observed, ensuring the protection of systems, vehicles, communications, and data from cybersecurity risks and threats, and reducing the risk of intrusion or unauthorized access. Fourth: Cloud Service Providers - Contracts must be concluded with cloud computing service providers holding valid, internationally recognized security certifications and accreditations, including as a minimum the standard ISO/IEC 27001 and reports SOC 2 or their equivalent as a minimum, with periodic verification of the continued validity of these certifications and accreditations, and the provider's compliance with the relevant security and regulatory requirements. Fifth: Service Quality - Connected vehicle service providers shall comply with Quality of Service (QoS) requirements in accordance with the approved international standards, in particular the 3GPP and 5GAA specifications, and in a manner appropriate to the relevant service category, ensuring performance levels suited to the nature of critical and non-critical applications.
	Question 6: What are your views on the Technical Architecture set out above, and does it protect vehicle owners from risk? If you disagree, please kindly explain the reasons and provide us with alternative suggestions, if any
	Disclosure and Reporting

Eighth	First: Reporting Security Incidents In the event that its systems or databases are subject to any security breach, cyber intrusion, or leak that has resulted—or may result—in unauthorized access to or disclosure of personal or sensitive data, the connected vehicle service provider shall be obligated to do the following: • Notifying the Authority: notify the Authority and the National Center for Information Safety immediately and in writing within a period not exceeding (72) hours from the time of becoming aware of the incident, accompanied by a preliminary report explaining the nature of the breach, the volume of data affected, and the precautionary measures taken. • Notifying Users: notify users affected by the security breach immediately and without delay, through direct and reliable means of communication, provided this does not exceed a period of (24) hours from the time it is confirmed that their personal data has been affected, and that the notification includes the nature of the potential risks and the technical recommendations necessary to protect their privacy and rights.
	Second: Transparency and Disclosure to Users • The connected vehicle service provider shall make available a clear, comprehensive, and easily accessible privacy policy to users before beginning to provide or activate the service, provided that this policy includes—as a minimum—detailed disclosure clarifying the nature of the data collected and processed, the rights of data subjects and the mechanisms for exercising them, and the relevant notification procedures and timelines, in a manner that enhances transparency and ensures compliance with the regulations and rules in force in the Sultanate of Oman. • This disclosure must be drafted in clear and direct language (in both Arabic and English), and the service provider is obligated to update it as soon as any change occurs in data processing practices.
Question 7: What are your views on Disclosure and Reporting, and do they guarantee data owners' rights? If you disagree, please kindly explain the reasons and provide us with alternative suggestions, if any	
Annexes	
(1)	Data Category, Protection and Localization Requirements Table

Localization Requirement	Required Level of Protection	Compliance Timeline	Use	Examples	Data Category
Mandatory localization within the Sultanate of Oman	Multi-layer encryption (AES-256), secure key management via HSM, multi-factor authentication (MFA), and strict access controls based on the principle of least privilege.	Immediate	Identity verification, transactions, and risk management	Biometric data, driver-related health data	Sensitive Data
Mandatory localization within the Sultanate of Oman	Data encryption using AES-256 at rest and TLS 1.3 in transit, with the application of Role-Based Access Control (RBAC) and anonymization of identifiers using UUID.	Immediate	Account management and user identification	Name, ID number, address, phone number, email	Personal Data
Mandatory localization within the Sultanate of Oman	Securing data in transit using TLS 1.3, and anonymizing identifiers via UUID, with controls applied to protect location data from tampering or unauthorized modification.	Immediate	Navigation and tracking	Current location, route, direction	Geolocation Data (GPS)
Mandatory localization within the Sultanate of Oman	Data encryption at rest, and anonymization of identifiers using UUID,	Immediate	Driving and safety analysis, and insurance	Acceleration, braking, turning	Driving Behavior Data

	with controls applied to prevent re-identification or linkage of data to individuals.				
Mandatory localization within the Sultanate of Oman	Data encryption at rest, and anonymization of identifiers using UUID, with technical access restricted according to authorized privileges, and audit logs enabled to monitor and track all access and modification operations.	Immediate	Diagnostics and maintenance	Engine status, tire pressure, fault codes, speed, fuel, RPM	Internal Systems Data
Mandatory localization within the Sultanate of Oman	Securing data in transit using TLS 1.3, encrypting data, and applying network protection controls.	Immediate	System operation and updates	Connectivity, updates, cloud services	Communications and Network Data
Mandatory localization within the Sultanate of Oman	Complete, irreversible anonymization of data, secured in transit using encryption.	Immediate	Technical analysis	Anonymized fault codes	Anonymized Technical Data

Question 8: What are your views on the data category, security controls, and localization requirements — do they meet the regulatory requirements?
If you disagree, please kindly explain the reasons and provide us with alternative suggestions, if any