






EVs and data collection


A tour of several jurisdictions


In the era of Electric Vehicles (EVs), the surge in embedded electronics and vehicle apps present an unprecedented opportunity to enhance vehicle performance and efficiencies through data utilization. However, this requires stringent data governance practices. In this comparison table, we explore the data requirements and other regulatory considerations relating to EVs and vehicle usage apps across various jurisdictions including Singapore, Hong Kong, China, UK and the U.S. (California).

	Singapore	Hong Kong	China	UK	U.S. (California)
Vehicle usage apps – the operation of the vehicle now requires apps to be set up and typically operated by the manufacturer					
<p>What are the basic data protection considerations in setting up an app?</p> 	<p>The app must comply with the obligations of the Personal Data Protection Act 2012 (PDPA), in particular the transfer limitation and protection obligation.</p> <p>The transfer limitation obligation requires the app to only transfer personal data to another country if the standard of protection is comparable to the protection under the PDPA.</p> <p>The protection obligation requires the app to implement reasonable security arrangements to protect personal data and prevent unauthorized access, collection, use, disclosure or similar risks.</p>	<p>The app must comply with the Personal Data (Privacy) Ordinance (PDPO), in particular the data protection principles regarding data collection, use and security.</p> <p>Personal data must be collected for a lawful purpose directly related to a function or activity of the app. Such data cannot be used for a new purpose without prior consent from the app users.</p> <p>The PDPO requires the app to take all practicable steps to ensure that any personal data held is protected against unauthorized or accidental access, processing, erasure, loss or use.</p>	<p>The collection and processing of personal data via the app shall comply with the Personal Information Protection Law of China (PIPL), in particular, by following the principles of legality, necessity and appropriateness, and also comply with the obligations on notification and consent, special requirements for sensitive personal data, security measures, etc. Some personal data may be deemed as sensitive personal data (e.g., whereabouts data and accurate positioning data) and shall be subject to separate consent of data subjects and more stringent protection measures.</p> <p>The collection of personal data via the app shall be limited to the minimum scope for achieving the purpose for operation of the app.</p> <p>If the personal data collected in the app is stored or transferred outside China, app operators shall obtain the separate consent of data subjects and take necessary measures to ensure that the handling of personal data by the overseas recipient meets the standards for protection in China. Where required by law, data exporters shall implement a cross-border data transfer mechanism, i.e., security assessment, Standard Contractual Contracts for Cross-Border Transfer of Personal Data (SCC) or certification.</p> <p>The app owners/operators shall complete filing with the competent office of the Ministry of Industry and Information Technology (MIIT) by the end of March 2024.</p>	<p>The app must comply with the obligations of the General Data Protection Regulation (GDPR).</p> <p>Personal data can only be transferred to another country if certain safeguards are met – for example, the UK has officially designated such countries as having “adequate protection,” or there must be appropriate safeguards in place, such as standard contractual clauses.</p> <p>The app should also implement appropriate technical and organizational measures, which involve risk analysis, organizational policies, and physical and technical safeguards.</p> <p>Processing and data collection in relation to the app must comply with various principles including on data minimization and purpose limitation and the need for various accountability documentation to be in place. A lawful basis is required for any processing and data controllers will need to comply with various accountability obligations.</p>	<p>The app must comply with the obligations of the California Consumer Protection Act of 2018 and the California Privacy Rights Act of 2020 (collectively, the CCPA).</p> <p>These obligations include limitations on the use, transfer and retention of the personal information collected. Consumers will have a right to request access to, and deletion and correction of, their personal information, as well as the right to opt out of any sale or sharing of their personal information.</p> <p>Further, any personal information collected, used or transferred must be reasonably necessary and proportionate to the business purposes set out by the app.</p>

	Singapore	Hong Kong	China	UK	U.S. (California)
Vehicle usage apps – the operation of the vehicle now requires apps to be set up and typically operated by the manufacturer					
<p>Can the manufacturer use collected data for marketing?</p> 	<p>The manufacturer must obtain express consent from app users to satisfy the consent obligation before conducting marketing. The manufacturer must communicate clearly how the collected data will be used for marketing when obtaining consent from users.</p>	<p>The manufacturer must inform app users that it intends to use their personal data for direct marketing but that it cannot do so without their consent.</p> <p>The manufacturer must provide app users with information in relation to the intended use, for example, that the personal data is provided for gain (if it is to be so provided), the kinds of personal data to be used, the classes of recipients of personal data and the classes of marketing subjects.</p>	<p>The manufacturer shall specify the purpose of marketing in the notification of collection of personal information (e.g., privacy policy) and obtain the consent of data subjects.</p> <p>Where the manufacturer sends commercial marketing through automated decision-making, it shall provide a choice for recipients to opt out.</p>	<p>In the UK, the rules on consent depend on how direct marketing will be sent to the user.</p> <p>For email marketing and texts, the manufacturer must obtain express consent from app users and clearly communicate how the collected data will be used for marketing. The manufacturer might be able to rely on a “soft opt-in” if the user has previously purchased goods or services, the marketing communication relates to similar products, and the user was provided with an opportunity to opt out during data collection. Finally, it is essential that the user continues to have the opportunity to opt out in all subsequent communications. For post and telephone, it may be possible to rely on an opt-out approach, although consent remains best practice.</p>	<p>Yes, provided that marketing has been stated as a business purpose when collecting the data, a manufacturer can use the collected data for marketing purposes.</p> <p>However, the CCPA does have a requirement that would allow a consumer to limit the use of their collected information, with which the manufacturer must comply. This includes the ability to opt out of the sharing of their personal information for cross-context behavioral advertising.</p>
<p>Can the collected data be used for improving products and services?</p> 	<p>Yes, via the PDPA business improvement exception and legitimate interest exception.</p> <p>The business improvement exception is available if the manufacturer cannot reasonably achieve its purpose without using the personal data in individually identifiable form and the purpose is considered appropriate by a reasonable person in the circumstances.</p> <p>The legitimate interest exception allows organizations to collect, use and disclose personal data from an individual without consent if the collection, use or disclosure of the personal data is in the legitimate interests of the organization, the legitimate interests would outweigh any adverse effect on the individual and the organization discloses its reliance on the exception to the individual. Examples of legitimate interests include fraud prevention and dispute resolution.</p>	<p>There is no general exception in relation to the use of personal data to improve products and services. If such purposes are not directly related to the purposes originally communicated to app users during the collection of data, prior express and voluntary consent must be obtained from the app users.</p>	<p>The manufacturer can use the personal data collected for improving products and services if it has specified such purpose in the notification (e.g., privacy policy) and has obtained the consent of data subjects.</p> <p>There is no general exception which allows manufacturers to use personal data for improving products and services without the consent of data subjects.</p>	<p>In the UK, under data protection laws there is no express “business improvement exception” and the requirement is that there is a lawful basis for any processing. Manufacturers will be most likely to consider relying on consent or on legitimate interests to process personal data for the purpose of improving their services. If relying on legitimate interests, they would need to demonstrate that such processing is in the legitimate interest of the organization, that it is necessary for improving the services, and that the legitimate interest is not overridden by the data subjects’ rights and freedoms. Users may also have a right to object to the processing.</p> <p>Another solution would be to use anonymized data to enhance products and services, such as aggregated statistics.</p>	<p>Yes, many of the listed acceptable business purposes under the CCPA are related to improving products and services, including debugging/repairing errors; undertaking internal research for development; and improving, upgrading, enhancing or maintaining the quality of a service or device owned by the business. Assuming one of these business purposes is provided as the reason to collect the data, the data can be used for these purposes.</p>

	Singapore	Hong Kong	China	UK	U.S. (California)
EV vehicles are likely to be connected vehicles with an embedded SIM or eSIM					
<p>What are the regulatory approvals needed to provide an IoT service?</p> 	<p>Infocomm Media Development Authority (IMDA) requires the manufacturer, importer and seller of consumer IoT devices, and the connectivity service provider for consumer IoT devices, to minimally obtain a Telecommunication Dealer's (Class) license and a telecommunications operator license (a Service Based Operator's (Individual) license) respectively for the provision of IoT/M2M services. These two licenses have additional obligations for the record keeping of the SIM device information, as well as end users' information.</p>	<p>The Communications Authority requires Wireless Internet of Things (WIoT) service providers to obtain a WIoT license under the Telecommunications Ordinance for the provision of WIoT platforms and services using the shared frequency band of 920-925 MHz. The license authorizes WIoT service providers to provide automated data-only machine-to-machine type communications only, but does not authorize them to carry any voice communications. The license has an initial validity period of five years and, subject to the discretion of the Communications Authority, may be extended for a further period of up to five years.</p>	<p>The IoT applied in vehicles may involve various levels of business, which will require different value-added telecommunications business licenses (VATS) issued by MIIT:</p> <ul style="list-style-type: none"> • Providing a communications network to connect various device terminals will require a license for internet access services (ISP license). • Providing online data processing and storage services will require a license for online data processing and transaction processing services (EDI license) and an internet data center license (IDC license). • Providing online navigation, entertainment, consulting, advertising and other services will require a license for information services (ICP license), etc. <p>It is important to note that some VATS restrict or prohibit foreign investment.</p>	<p>In the UK license obligations attach to those who operate the physical network and utilize the radio spectrum rather than to the manufacturer of hardware. Therefore, whether or not a license is required will depend on whether the manufacturer is also providing the connectivity or whether this is provided by a separate operator.</p> <p>The Product Security and Telecommunications Infrastructure Act 2022 will come into effect in 2024. The Act requires manufacturers, importers, and distributors of the connected product to comply with minimum security standards. This includes providing a statement of compliance, increasing transparency about support periods before customers make a purchase, and establishing a mechanism for reporting vulnerabilities.</p>	<p>California Civil Code section 1798.91.04 requires a manufacturer of a connected device to equip it with a reasonable security feature or features that are appropriate to the nature and function of the device; appropriate to the information it may collect, contain or transmit; and designed to protect the device and any information on the device from unauthorized access, destruction, use, modification or disclosure.</p> <p>Methods of satisfying these requirements include meeting or exceeding the baseline product criteria of a National Institute of Standards and Technology (NIST)-conforming labeling scheme; satisfying a conformity assessment as described by NIST; or bearing the binary label as described by a NIST scheme.</p>
<p>Is the licensing imposed on the manufacturer or the telecommunications company?</p> 	<p>Both the manufacturer and telecommunications company need to obtain their respective licenses covering their activities above (deploying telecommunications equipment and operating a telecommunications network).</p>	<p>The licensing requirement is imposed on WIoT service providers, irrespective of whether they are manufacturers or telecommunications companies.</p>	<p>The VATS are applicable to any entity that provides value-added telecommunications services, regardless of manufacturer or telecommunications company.</p>	<p>The telecommunications company must obtain the necessary license to operate the network. The manufacturer would be required to meet the relevant security standards.</p>	<p>There is no license requirement. The manufacturer is the party responsible for building a device that meets the standards of California Civil Code section 1798.91.04.</p>

	Singapore	Hong Kong	China	UK	U.S. (California)
To support the EV ecosystem, apps that help find available charging points and pay for charging are being introduced					
<p>What are the data protection considerations for the collection and display of vehicle location data?</p> 	<p>Anonymizing the data: Similar to ride-hailing app interfaces, vehicles can be displayed using generic icons that are not associated with a specific vehicle. Another approach is using a traffic-light indicator to indicate the availability per-station, rather than displaying per-vehicle location.</p> <p>Protecting the data: The APIs used to collect and display the vehicle data must be designed so that bad actors cannot obtain unique identifiers of vehicles, e.g., through the use of end-to-end encryption.</p> <p>Accountability and consent: Privacy policies should set out clearly what information is collected from users, and companies should communicate their policies to users and seek express consent.</p>	<p>In addition to the considerations raised for Singapore, the following considerations also apply:</p> <p>A personal information collection statement shall be provided to the app users on or before the collection of personal data.</p> <p>Permission shall be sought from the app users whenever a new type of information is accessed, transmitted or shared for the first time.</p> <p>A privacy policy statement shall be provided to the app users for outlining the policies and practices in relation to personal data.</p>	<p>The collection and processing of location data shall be specified in the notification (e.g., privacy policy). The location data is deemed as sensitive personal data. The separate consent of data subjects shall be required for the collection of whereabouts data.</p> <p>In addition, the location data may be subject to special requirements:</p> <ul style="list-style-type: none"> • Location tracking data shall not be stored outside the vehicle for more than 14 days, except for the location trajectory data generated by cars used for production and operation and controllable by manufacturers. • Location tracking data shall not be transferred abroad. If there is a need to transfer such data outside China, a security assessment by the Cyberspace Administration of China (CAC) will be required. <p>An app shall obtain the permission of its users to activate the location function.</p>	<p>Same as Singapore. In addition, if the service constitutes an electronic communications service under the Privacy and Electronic Communications Regulations (PECR) and location data is collected through the network, it must undergo anonymization for use for value added services.</p>	<p>Precise geo-location: Under the CCPA, precise geo-location, defined as identifying a location within 1,850 feet, is considered to be sensitive personal information and is held to a higher standard. If a business is utilizing sensitive personal information, it must provide notice to the consumer of what information it is collecting and, while not required, should gain informed consent prior to collecting sensitive personal information. Further, the CCPA grants consumers who have their sensitive personal information collected additional rights to limit the use and disclosure of the information.</p> <p>Accountability and consent: As required under the CCPA, the legitimate business purposes for collecting data must be identified, which could include keeping charging station availability services up to date. As long as these purposes are clearly identified within the privacy policy, manufacturers would be in possession of the required consent.</p> <p>De-identifying the data: If a requirement to share the location of charging points within an application is necessary, and consent has not been received from the consumer for sharing the data, the application should not be required to demonstrate which vehicle is at a charging station and who the vehicle belongs to. Instead, it should only be required to indicate whether the charging station is available at that point in time. A further indicator of when that charging station would become available based on the currently connected vehicle would also be acceptable.</p> <p>Protecting the data: Any and all collected data must be stored and shared in a secure manner, with a recommendation of complying with frameworks such as NIST to ensure the security of the information.</p>

	Singapore	Hong Kong	China	UK	U.S. (California)
To support the EV ecosystem, apps that help find available charging points and pay for charging are being introduced					
<p>What are the cybersecurity considerations for processing of payments through the app?</p> 	<p>Payments should be processed using payment service providers that are licensed by the Monetary Authority of Singapore (MAS). These payment service providers have to adopt cybersecurity measures set out in the MAS Notice on Cyber Hygiene and Technology Risk Management Guidelines.</p>	<p>If payment is made through a stored value facility (SVF) (a facility used for storing the value of an amount of money for making payments for goods or services and/or to another person), payment must be processed using payment service providers that are licensed by the Hong Kong Monetary Authority under the Payment Systems and Stored Value Facilities Ordinance (PSSVFO). These payment service providers have to adopt appropriate risk management policies and procedures for managing the risks arising from the operation of the SVF scheme, including a technology risk management framework, an internal control system and a payment security management framework.</p>	<p>Non-financial institutions shall obtain a payment permit issued by the People's Bank of China to provide online payment services.</p> <p>The processing of payments may involve personal financial data, most of which is deemed as sensitive personal data. The collection and processing of personal financial data will be subject to more stringent requirements, such as the separate consent of data subjects, DPIA, as well as security technical and management requirements.</p>	<p>Payments should be processed using payment service providers regulated by the Financial Conduct Authority (FCA) or the Payment Systems Regulator, depending on classification. FCA-regulated payment service providers have to adopt cybersecurity and operational resilience measures as set out in the FCA's Principles and Senior Management Arrangements, Systems and Controls and the FCA Handbook. The FCA's rules follow the European Banking Authority's Guidelines on ICT and Security Risk Management.</p>	<p>Payments should be processed using payment service providers that meet the PCI Security Standards to ensure secure transactions occur.</p>