APAC: Data Collection in the Automotive Sector
Key Considerations under Personal Data Protection Act of Thailand

Across the Asia-Pacific region, the automotive industry is transforming automobiles into sophisticated data collection platforms. These platforms can gather/collect everything from location information and driving patterns to biometric data and personal preferences. In Thailand, the Personal Data Protection Act B.E. 2562 (2019) ("**PDPA**") provides the legal framework on how any person or organization collects, uses, or discloses personal data of individuals ("**data subjects**" or "**DS**"). The PDPA creates significant obligations for automotive manufacturers, dealers, and service providers because modern vehicles use hundreds of sensors, cameras, and connectivity modules to collect a large amount of data that can directly or indirectly identify individuals.

LawPlus Ltd. provides an overview of the key considerations for the automotive sector when implementing the PDPA compliance measures. The overview focuses on data collection requirements, consent and lawful basis, security obligations, and cross-border data transfer mechanisms as provided in the PDPA and its implementation rules and notifications issued by the Personal Data Protection Committee ("**PDPC**") under the PDPA.

1. Data Collection Requirements

The personal data must be collected only for specified, explicit purposes and only to the extent necessary. In the automotive sector, this includes:

1.1 General Personal Data

Modern vehicles collect a wide range of personal data beyond traditional sales and service records. In addition to driver and passenger names, government-issued identification numbers, contact details and payment information collected at dealerships, vehicles equipped with connected-car and telematics systems also record data such as:

- Historical GPS logs showing coordinates tracked over time to map daily routes and frequent stops;

- Driving behavior, e.g., acceleration, braking and steering patterns that reveal individual habits and preferences;

- Device and app data, e.g., infotainment platforms that synchronize smartphone contacts; navigation systems that record destination history; and voice-activated that controls capture spoken commands; and

- In-car settings, e.g., seat positions, climate preferences and radio station selections that combine to form unique user profiles.

Any person or organization acting as a Data Controller ("**DC**") or Data Processor ("**DP**") in the automotive sector must collect such personal data only to the extent necessary and for specified, informed purposes under the PDPA.

1.2 Sensitive Personal Data ("**SPD**")

The PDPA classifies biometric and health-related information as SPD. SPD may be collected, used or disclosed only with explicit consent and must be protected by the security measures prescribed by the PDPC. In the automotive sector, SPD includes:

- Biometric identifiers, e.g., facial recognition for driver authentication, fingerprint sensors for ignition and voice prints for security functions.

- Health indicators, e.g., cameras and sensors that detect driver fatigue or drowsiness, steering-wheel heart-rate monitoring and analytics capable of flagging alcohol impairment or medical emergencies.

Before collecting or using any SPD, DC or DP must obtain explicit consent and implement the required measures/safeguards on data security, breach notification and access controls.

2. Consent and Lawful Basis

Processing personal data is permitted only if DS has consented or if an alternative lawful basis applies.

2.1 Consent

DC may process personal data only after obtaining explicit consent from DS. Explicit consent must be given freely without any linkage to sales or warranty terms. Each processing purpose must be clearly defined and explained in plain language at the time of data collection. DS must be able to withdraw their consent with the same ease as they provided it. Automotive manufacturers can meet these standards by prompting the DS drivers for permission when they enable specific features, displaying real-time privacy status on the infotainment screen, or providing companion mobile apps that allow detailed permission management.

2.2 Alternative Lawful Basis

Where consent is impractical or unnecessary, DC may rely on:

- Contractual necessity that is required to perform a contract with the driver or DS, for example, engine management, airbag deployment, electronic stability control and warranty services.

- Vital interests that are required for processing to protect life or physical safety, for example, automatic collision-response calls and driver health monitoring alerts. The threat must be immediate and does not extend to convenience functions.

- Legitimate interests that are required for limited operations such as cybersecurity monitoring, and warranty-fraud prevention. Each activity requires a documented balancing test demonstrating that the DC's interests do not override individual privacy rights and must satisfy the PDPA's stricter standard.

- Legal obligations that are required for processing under Thai laws or court orders, for example, mandatory accident data recorders, emissions reporting and safety-defect notifications. DC must verify that each obligation arises from a genuine legal requirement rather than industry custom.

3. Security Obligations

DC and DP must have security measures to protect personal data collected. The security measures as set out by the PDPC require a combination of technical and organizational controls to prevent unauthorized access, use, alteration, disclosure or loss.

Automotive companies that carry out regular monitoring or large-scale processing of personal data must also appoint a data protection officer (DPO) with the expertise in both data protection law and automotive technology. The DPO must report directly to senior management, operate independently of IT or product development teams and coordinate the PDPA compliance.

In addition to the above, DC and DP must maintain records of processing activities (ROPA). The ROPA must detail processing purposes, lawful basis, data categories, recipients, retention schedules and security measures. ROPA must be updated whenever new data flows start, change of processing purposes or third-party relationships begin. Continuous review of ROPA must be made to guarantee the compliance with the PDPA requirements and evolving technology.

4. Cross-Border Data Transfer Mechanisms

The automotive sector operates across many countries and often sends data internationally. Centralized analytics at headquarters, telematics platforms serving multiple markets, supply chains involving several regions and global research collaboration are all created a need for cross border data flows.

Binding Corporate Rules (BCRs) establish as an internal privacy framework for companies in the same group. Implementation begins by mapping data flows in manufacturing, research and development, sales operations and financial services. Enforceability of the BCRs requires the parent company board resolutions and binding commitments through employment contracts and group level agreements. Approval from the Office of the PDPC (OPDPC) is also required. Translation of the BCRs into the Thai language, employee training, contract updates and global complaint handling are among the main challenges.

Data Transfer Agreements (DTAs) provide as a mechanism for sharing personal data with third parties outside group of companies. DTAs should address automotive specific concerns such as retaining safety critical data despite the request of deletion, maintaining information for product liability purposes, and coordinating procedures for safety recalls, etc.

Conclusion

The compliance with the PDPA in the automotive sector requires a clear, structured approach to every stage before collecting personal data. Personal data may be collected only for the clear and documented purposes and only to the extent necessary. Since vehicles now gather general personal data, e.g., location history, driving behavior, device and app usage, in-car settings, and SPD, e.g., biometric identifiers and health indicators, DC and DP must distinguish between personal data and SPD and apply minimization and purpose-limitation principles and obtain explicit consent before any collection of SPD.

When consent is impractical or unnecessary, automotive companies may rely on alternative lawful basis for core functions by mapping each processing activity to the correct lawful basis. Automotive companies that carry out large-scale data processing must appoint a DPO who understands both vehicle technology and PDPA. They must also keep their ROPA up to date.

Cross-border transfers pose additional complexity to the automotive sector. BCRs offer a group-wide framework but require significant investment, governance and the OPDPC approval. DTAs with third parties must address safety-critical retention, product liability and recall coordination.

The automotive industry stands at the intersection of rapid technological innovation and stringent data protection requirements. By complying with the PDPA requirements into product design, corporate policy and operational practices, manufacturers, dealers and service providers in the automotive sector can transform compliance into a competitive advantage. By keeping customers informed, applying a culture that places privacy at the heart of engineering and collaborating closely with the regulators, companies in the automotive sector can earn trust from their customers and drive the innovation in connected, electric, autonomous and shared mobility. In a world where cars act as rolling data centers, diligent data governance under the PDPA is essential to safeguard individual rights and maintain market standing.

Kowit Somwaiya, Managing Partner
kowit.somwaiya@lawplusltd.com

Usa Ua-areetham, Partner
usa.ua-areetham@lawplusltd.com

Warawut Aroonpakmongkol, Associate
warawut.aroonpakmongkol@lawplusltd.com

LawPlus Ltd., Bangkok
June 2025