



FCAI VOLUNTARY CODE OF CONDUCT

Automotive Data and Privacy Protection

This Code of Conduct will commence operation on 1st July 2021

Introduction

As Australia's new motor vehicles advance, a range of new technologies are being introduced that will bring significant benefits to consumers and the community more broadly. Some of these technologies, particularly in connected and autonomous vehicles, have the capacity to collect, receive, create, and store vehicle generated data and personal information. FCAI members understand that the protection and use of this data is a significant responsibility that requires robust systems, policies, and controls.

The FCAI members have voluntarily agreed that the principles below will drive their approach to treatment of vehicle generated data and associated personal information. These principles are consistent with the Australian Privacy Principles and other Australian laws that apply to the collection and use of vehicle data and personal information.

In addition to these principles, each FCAI member has its own policies, procedures and systems that are tailored to the way they collect and use personal information and vehicle generated data.

Automotive Data Protection Principles

1. We are open and transparent

FCAI members and any other parties who wish to be bound by this code voluntarily ("we") notify customers who use our connected vehicles and services ("customers") about:

- personal information (i.e. information or an opinion that could identify an individual) we collect;
- vehicle generated data (including geolocation and driver behaviour data) that we collect;
- the purposes for which we use personal information and vehicle generated data;
- the types of third parties with whom we may share personal information and vehicle generated data;
- the identity of the company or group of companies that uses the data;



- the way personal information is handled, who has access to it and the process by which customers can obtain a copy of, or correct personal information held about them; and
- if personal information is disclosed to third parties located overseas as part of delivering the service, the countries in which those third parties are located.

We make this information available in a clear, meaningful, and easily accessible manner. This may be done in one or more of the following ways:

- in a contract or policy (including privacy policies and collection statements);
- in a user manual;
- via a special menu / agreement in the vehicle's infotainment system;
- via specific icons, pictures, or graphics in the vehicle;
- in our mobile applications (apps);
- on our websites and web portals; or
- in any other appropriate manner.

2. We give customers choice

Where reasonably possible, customers can choose whether to share personal information as part of the connected vehicle services provided to them by FCAI members.

Where personal information is to be shared with other third parties for marketing or promotional purposes, this will only be done with customer consent or as permitted by law.

Where possible, customers may be able to de-activate connected vehicle services. However, vehicle generated data may still be collected and used and disclosed to third parties to provide accident emergency notifications, to comply with a legal requirement from law enforcement or regulators or, to the extent permitted by law, for the protection of health and safety and for road safety purposes.

3. Privacy by design – we always consider Data Protection

We take data protection requirements into account when we design, develop, and engineer new products, services, and processes.

Where necessary to maintain high levels of data protection in the provision of connected vehicle services, we strive to carry out a privacy impact assessment before:

- putting new products on the market;
- adding product features or services with new technologies relating to vehicle generated data,

and we seek to implement the measures that this impact assessment shows to be appropriate.

4. We maintain Data Security

We implement appropriate and ongoing physical, technical, security, access controls and organisational measures to protect the personal information of



customers against accidental or unlawful destruction, loss, alteration, or disclosure.

Where we outsource data processing functions, we take reasonable steps to protect the personal information of our customers at least in line with the requirements of the *Privacy Act 1988* (Cth) and applicable state and territory legislation.

To protect the safety of drivers and integrity of our vehicles (particularly from cybersecurity threats), before we make any vehicle generated data available to third parties or receive data from third parties to be transferred to a vehicle, we will take reasonable steps to secure the data transmission, which may include the requirement that data is sent and received through a secure off-board facility, see section 6 below for further details.

5. We process personal information in a proportionate manner

We only collect and process personal information, which is adequate, relevant, and not excessive in relation to the purpose of that collection which has been notified to the customer. We consider data anonymisation, pseudonymisation and de-identification important mechanisms for protecting personal data and we apply these principles where appropriate. For example, the location data of vehicles provided to navigation service providers can inform recommended travel routes benefitting users, in this case where personal information is not required in order to provide the service, it may be removed as described above prior to sharing with these providers.

6. We only share data responsibly, legally and driven by our customers' preferences

Vehicles are increasingly 'connected' in the sense that they can exchange information wirelessly with the vehicle manufacturer, third-party service providers, users, infrastructure operators and other vehicles. These functions can increase comfort and convenience for customers, improve products and services and contribute towards achieving societal goals, such as improving road safety, reducing fuel consumption / emissions, as well as facilitating traffic management and parking. Vehicles may collect, store, process and/or transmit data for these purposes. We are committed to ensuring that these opportunities for Australian vehicle users are implemented in a way that is compliant with relevant laws and respects customer's choices.

Types of Data and example use cases

Connected vehicles collect and process data relating to the vehicle itself and its surroundings. Some of this data may be regularly overwritten while other data may be stored for a certain period or aggregated in statistical form.

This 'vehicle-generated data' may relate to:

- safety and security (e.g. Crash Event Data such as whether airbags have been triggered or whether doors and windows are locked or open);
- vehicle functionality status (e.g. engine injection, transmission behaviour, fuel level, battery charging level, Driver Assistance Systems, On-Board Diagnostic malfunctions);



- driving (e.g. fuel consumption, speed, use of brake and accelerator pedals, steering wheel movement, general vehicle operating parameters to inform predictive maintenance or repair);
- location of the vehicle: (e.g. navigation, providing locally relevant information, locating vehicles);
- surroundings (e.g. outside temperature, nearby vehicles, or other objects);
- enabling remote vehicle operations: (for example: remote engine start, remote climate control operation);
- data that has been introduced by customers themselves. This 'user introduced data' may be collected and stored through certain features of the vehicle, including but not limited to:
 - infotainment settings (e.g. preferred radio station);
 - convenience settings (e.g. seat & mirror positions);
 - navigation destinations; and
 - mobile phone address book.

It should be noted that personal information is not limited to information which identifies an individual, but also to information from which an individual is reasonably identifiable. Vehicle generated data may not be personal information when held by itself (because it is not about an identified individual), but if it can be matched with other information available to the manufacturer or otherwise used by the manufacturer to identify an individual (for example by searching a customer database), then it could be considered personal information. The purposes for which data that is collected and may be used include without limitation:

- complying with legal obligations (for example: on-board diagnosis, consumer protection, recall and safety-related field monitoring, direction from law enforcement, courts, and regulators);
- providing vehicle support and services (e.g. repair and maintenance, roadside assistance, warranty, over the air updates, vehicle location and remote vehicle services);
- improving vehicle performance, quality, and safety (e.g. product development, accident research investigation);
- offering information and entertainment (e.g. communications, access to media, navigation, information about weather, traffic, and parking);
- facilitating access to services (e.g. fleet management, pay-as-you drive insurance, trip logbook services which may enable business compliance with certain requirements such as Fringe Benefits Tax); and
- enabling vehicle-to-vehicle or vehicle-to-infrastructure communication (e.g. road hazard warnings, re-routing or traffic management).

Third-Party sharing

With the rising volume of vehicle generated data, third parties (outside of the network of dealers, companies, organisations and contractors engaged by motor vehicle manufacturers, including those that provide the connected vehicle services) which we will refer to as "external third parties" are increasingly interested in accessing and using such data to provide services. These service providers include but are not limited to motor vehicle repairers, breakdown services, insurance companies, operators of parking garages, financial and fleet



service providers, and road infrastructure operators. They can also include participants unrelated to the automotive industry such as entertainment and travel-service providers, social networks, and search engine operators.

Sharing vehicle generated data with these external third parties can improve the driving experience, increase comfort for the driver, optimise products, and contribute to societal goals such as improving road safety, reducing fuel use and consequently vehicle emissions.

Here are some examples of how vehicle-generated data can be used to the end user's benefit:

- to advise the end user on the easiest and safest routes, avoiding traffic jams and road hazards;
- to provide 'smart parking' information;
- to contact emergency services in the event of an accident;
- to forecast when a vehicle will need maintenance or repair to avoid breakdowns;
- to automatically pay for parking or tolls;
- to enable insurance companies to offer tailored premiums (for example based on distance travelled, driving style and itineraries);
- to provide relevant local information in real time;
- to provide tailored entertainment and other services;
- to provide access to music, social media channels, e-mails, etc – making the car an extension of the office or home.

Where we do make vehicle generated data available to external third party service providers, we will strive to inform you that we are doing this, and to the extent personal information is disclosed, we will only do so in accordance with applicable laws and consistent with the principles set out in this Code of Conduct. Where we make vehicle generated data available to these external third-party service providers, we will endeavour to seek their agreement to the principles in this Code of Conduct.

Where we make vehicle generated data available to external third-party service providers, we will seek to do so in a manner that:

- ensures the protection of the vehicle user's personal information;
- does not endanger the safe and secure functioning of the vehicle;
- does not endanger the operator of the vehicle; and
- does not create legal liability for us whether under applicable laws or contractual obligations.

For the safety and integrity of the vehicle, when we do share vehicle related data or receive data from third party providers, we will take reasonable steps to secure the data transmission, which may include the requirement that data is sent and received through a secure off-board facility.

Third-party service providers may be able to access the vehicle generated data they need or provide information back to the vehicle through a secure means which may include the requirement that data is accessed through a secure off-board facility.



Except where we are already legally permitted or required to do so, we will only share vehicle related data which is identifiable to you with third parties with your consent. When we do share this data, we will endeavour to ensure the third party receiving the data contractually agrees to use the data only for the purpose you have consented to and in accordance with all applicable laws.

Review

This Code of Conduct will commence operation on 1st July 2021. FCAI will undertake a review of this Code of Conduct at least every five years from inception, and it may also be updated from time to time in response to regulatory and technology change.

About the FCAI

The Federal Chamber of Automotive Industries (FCAI) is the peak industry organisation representing the manufacturers and importers of passenger vehicles, light commercial vehicles, and motorcycles in Australia. A full listing of FCAI member companies can be accessed as follows:

<https://www.fcai.com.au/about/members>.

More information concerning FCAI can be found on www.fcai.com.au.