Renault Group Data Policy

1. The EU Data Act and this Policy

The purpose of Regulation (EU) 2023/2854 (the "Data Act"), which enters into application on 12 September 2025, is to foster innovation and economic growth in the EU by facilitating the flow of data generated by connected products and related services.

Under the Data Act, users of connected products and related services have a **right to access** some of the data generated by these products and services and a **right to share** this data with third parties.

For example, users of connected vehicles manufactured by Renault could, under certain conditions, have access to odometer data extracted from their vehicles and available on Renault's server in order to share this data with their mechanic or insurance company.

This Policy reflects the application of rules from the Data Act to the relevant activities conducted by Renault Group.

2. What is a connected product and a related service?

A **connected product** is a product (such as a vehicle) that obtains, generates or collects data concerning its use or environment and is able to communicate this data via an electronic communications service, physical connection or on-device access (e.g. Wi-Fi, Bluetooth, or a mobile internet network). Products whose primary function is the storing, processing or transmitting of data on behalf of a party other than the user (e.g. servers operated entirely on behalf of third parties) are excluded from this definition.

For example, a vehicle built by Renault of which certain data can be viewed via the mobile application My Renault or any other electronic method qualifies as a connected product.

A **related service** is:

- a digital service other than an electronic communications service (for example, an internet service provider),
- connected to the product at the time of purchase, rental, or lease, and
- essential to performing one or more product functions.

A related service can also be a service that is connected to the product at a later date by the manufacturer or a third party to add to, update, or adapt the functions of the connected product.

For example, remote charge programming and temperature control via the My Renault application qualify as connected services.

3. To whom does the Policy apply?

This Policy applies:

- to Renault, or potentially one of its subsidiaries, where Renault and/or the subsidiary is a **data holder** as defined by the Data Act (hereinafter "Renault", "we" or "us"),

- to any **user** of connected products or related services for which Renault holds the data within the meaning of the Data Act, and

- any **third party** designated by a user to receive readily available data from Renault (the "third party" or, where the third party acts in a professional capacity, the "data recipient", it being specified that the data recipient may also receive data from Renault pursuant to another legal obligation).

Renault qualifies as a data holder where it has the right or obligation to use data and make it available pursuant to a legal or contractual obligation.

A user is any natural or legal person:

- who owns a connected product, such as a connected vehicle or charging station manufactured by Renault, or

- to whom temporary rights to use a connected product have been contractually transferred (e.g. as part of a rental or lease), or

- who receives a related service.

4. What is the objective of the Data Policy?

The Data Policy defines the rights and obligations of data holders, users, and third parties (including data recipients) under the Data Act.

Where appropriate, the Policy is supplemented by special provisions in the contracts entered into between Renault, users, and third parties. If any of those provisions conflict with this Policy, the contractual clause prevails.

This Policy supplements our privacy policies. In case of conflict between this Policy and our privacy policies, our privacy policies prevail.

5. What data may users access?

Users may access:

- personal and non-personal data generated through the use of a connected product (such as a connected vehicle made by Renault) where that data has been designed to be retrievable by a user, data holder, or third party via an electronic communications service, physical connection, or on-device access (e.g. odometer data from the connected vehicle);

- personal and non-personal data representing user actions or events related to the connected product that were intentionally recorded by the user or are a by-product of the user's actions during the provision of the related service (e.g. a request for remote charging via the My Renault application); and

- the metadata relevant and necessary to interpret and use this data (e.g. the time and date of each piece of reported data).

Users only have access to this data to the extent Renault has lawfully obtained or can lawfully obtain it from a connected product or related service, without disproportionate effort going beyond a simple operation (hereinafter "readily available data").

Users also only have access to "raw" or "primary" data, i.e. data points that have been automatically generated without any type of processing other than to make them useable and understandable. Users do not, however, have access to any "derived" data that results from an additional effort by the data holder (to enhance the raw data, in particular through the use of complex algorithms).

Lastly, there are specific rules listed below for certain types of data:

Type of data	Definition	Examples	Rules
Data on connected product security	Data whose processing may undermine the security requirements of the connected product, leading to seriously adverse effects on personal health, safety, or security.	• Data on vehicle safety components • Data used to detect vehicle intrusions • Data for detecting changes to the vehicle emissions control systems	We can contractually restrict or prohibit access to, use of, of subsequent sharing of this data.
Data protected as a trade secret	Commercially sensitive data that qualifies as a trade secret and is covered by measures taken to preserve data confidentiality.	• Data relevant to the operation of a confidential technology used by Renault	Data qualifying as a trade secret is preserved and only disclosed where Renault has, jointly with the user, taken all necessary steps prior to disclosure to preserve the confidentiality of that data (e.g. encryption, fire walls, etc.). Renault, or the trade secret holder, identifies data protected as a trade secret and agrees with the user on the proportionate technical and organisational measures necessary to protect the confidentiality of data shared via standard contract clauses or other types of agreements. If there is no agreement on what measures are necessary, or if the user fails to implement the agreed measures or

			compromises the confidentiality of trade secrets, Renault may withhold or suspend the sharing of data identified as trade secrets. Our decision will be duly substantiated and provided to the user in writing without undue delay. In exceptional circumstances, where we can demonstrate that it is highly likely that the disclosure of trade secrets would result in serious economic damage despite the measures taken by the user, Renault may refuse requests to access the specific data in question on a case-by-case basis. The demonstration of the risk from disclosure is based on objective factors.
Personal data relating to someone other than the user	Data relating to an identified or identifiable natural person (within the meaning of the GDPR) other than the user and generated through use of a connected product or related service.	• Data from vehicle cameras that record passers-by	This data is only made available to the user if there is a valid legal basis under the GDPR for doing so and if the conditions relating to sensitive data and to trackers and cookies have been satisfied.
Data protected as intellectual property	Data protected by copyright or under a trademark, patent, or design right (not including rights protecting databases).	• Data related to content displayed or viewed by users, such as music users listen to in their vehicle	Users do not have the right to access or share this data.

Below is a non-exhaustive list illustrating the type of data that may be generated from using connected vehicles and related services.

Please remember that the list only contains data already generated by the vehicle, which depends on the following (without limitation):

- the version, equipment, type of use, and changes to and reservations of digital services;

- services that you have activated in your vehicle;

- choices you made in the confidentiality settings for your vehicle.

We would like to remind that the examples of data listed below refer **only to "raw" or "primary" data generated without any processing other than as needed to make it useable and understandable.**

Category	Data examples
Vehicle geolocation data	• Position of vehicle at start and end of trip • Position of vehicle in motion, every 3 seconds • Location of special incidents: sudden braking, sudden swerves, activation of ABS, emergency braking, airbags, etc.
Trip data	• Kilometres travelled • Travel time • Date/day/time of travel • Fuel consumption for the trip
Data on vehicle charging	• Charge amount • Type of charge • Type of station (AC/DC) • Average charging power • Time of start and end of charge
Driving data	• Speed, longitudinal and lateral accelerations • Use of brake, accelerator, and clutch pedals • Speed of steering wheel rotation • Gear lever position • Use of steering wheel paddles
Data on use of secondary vehicle functions	• Use of windshield wipers • Use of low and high beam headlights • Use of turn signals • Choice of driving modes
Data on vehicle occupancy and use of doors and windows	• Opening of doors • Driver and passenger detection • Seatbelt use detection • Opening of windows
Data on use of vehicle temperature functions	• Use of air conditioning and heat: activation, temperature settings, ventilation
Data on weather conditions	• External temperature • Rain sensor • Light sensor
Data on vehicle condition	• Odometer (Distance Totalizer) • Oil change or maintenance warning light • Fuel level warning light

	• Diesel exhaust fluid level warning light • 'MIL ON' warning light • System failure: ABS, AFU, ESC, Airbag • Crash detection
Data on tire pressure	• Tire pressure measurement (direct measurement)
Data on system activations	• Steering wheel lateral force and speed measurement • Instances of brake system activation • Duration of brake system activation • Brake pressure
Data on the engine and system conditions	• Engin torque/RPM • Cooling temperature • Particulate filter load status • Battery cell voltage • Battery temperature • Total power consumption • Battery health • Battery cooling temperature • Battery current • Battery temperature warning • 12 V battery SOC

6. **How can users get access to this data?**

Starting on 12 September 2025, users will be able to view the different types of data generated by the connected vehicle and related services via the platform Mobilize Data Solution: https://datasolutions.mobilize.com/home

The procedure for accessing this data will be communicated to users at a later date, as soon as the access will be available.

If a user's request satisfies the applicable legal requirements, we will disclose readily available data and related metadata:

- without undue delay after the data has been made available to Renault,
- that is of the same quality as is available to Renault,
- easily and securely,
- in a comprehensive, structured, commonly used and machine-readable format (e.g. API or Streaming),
- where relevant and technically possible, continuously and in real time.

All user requests for data disclosure are free of charge.

7. To whom may users disclose the data?

Once users have been informed of the procedures for accessing the data, they will also be able to ask Renault to share readily available data with a third party, as well as metadata they are entitled to access under the Data Act. Third party access will also be provided without undue delay, and the data will be of the same quality as is available to Renault, easily and securely accessible, in a comprehensive, structured, commonly used and machine-readable format. However, third parties will have to pay a compensation to Renault, if applicable (see paragraph 14).

For example, users will be able to ask Renault to share readily available data generated by their connected vehicle with their mechanic or insurance company.

The user's data sharing request can involve any third party except for undertakings designated as a "gatekeeper" under the EU Digital Markets Act, such as Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft.

Users may not share readily available data with third parties in the context of the testing of new connected products, substances or processes that have not yet been placed on the market, unless such third party use is contractually permitted.

8. How do third parties access data by user request?

Starting on 12 September 2025, third parties will be able to view the different types of data that may be generated by the connected vehicle and related services via the platform Mobilize Data Solution: https://datasolutions.mobilize.com/home.

Third parties will be able to obtain information about the conditions and procedures for accessing data by contacting Renault using the form available on the Mobilize Data Solution platform. Access will be available at a later date.

9. What are the obligations of third parties receiving data by user request?

Third parties must process data solely for the purposes and under the conditions agreed with the user and in compliance with personal data protection laws.

Third parties must erase data that is no longer necessary for the agreed purpose, unless otherwise agreed with the user with respect to non-personal data.

Third parties may not:

- make it difficult for users to exercise choices or rights, including by offering biased or coerced choices, deceiving or manipulating users, or impairing their autonomy, decision-making, or choices, including by means of a digital interface;

- use the data they receive for profiling, unless profiling is necessary in order to provide the service requested by the user and they comply with the GDPR;

- make the data they receive available to another third party, unless this is provided for in an agreement with the user and on condition the other third party takes all necessary steps agreed between the data holder and the third party to secure the confidentiality of trade secrets;

- make the data they receive available to a gatekeeper as defined by the EU Digital Markets Act;

- use or share the data they receive to develop a product that competes with the connected product from which the accessed data originates;

- use the data they receive to obtain information about Renault's economic situation, assets, or production methods or about the use Renault makes of that data;

- use coercive means or exploit any potential gaps in Renault's technical infrastructure aimed at protecting the data in order to gain access to that data;

- use the data in a way that adversely impacts the security of the connected product or related service;

- disregard the protections for confidential information and trade secrets agreed with Renault, or the trade secrets holder, and the user;

- prevent users who are consumers from making the data available to other parties.

10. **What protection measures can be implemented if data is used unlawfully?**

Situations where protection measures may be implemented	Protection measures that may be implemented
The third party or data recipient: - provided false information to Renault, used deceptive or coercive means, or exploited potential gaps in Renault's technical infrastructure designed to protect the data in order to obtain that data; - used the provided data for unauthorised purposes, including to develop a competing connected product; - unlawfully disclosed the data to another party; - failed to maintain the technical and organisational measures agreed with Renault or the trade secret holder; or - altered or removed technical protections, without Renault's consent, that were applied by Renault to prevent unauthorised access to the data, including metadata, and to guarantee compliance with the Data Act.	The third party or data recipient must comply, without undue delay, with the request by Renault, the trade secret holder or the user to: - erase the data made available by Renault along with any copies thereof; - end (i) the production, offering, or placement on the market or use of goods, derivative data or services produced on the basis of knowledge obtained from data made available by Renault, or (ii) the importation, export, or storage of infringing goods for those purposes; - destroy any infringing goods produced using knowledge obtained from data made available by Renault if there is a serious risk that the unlawful use of that data could significantly harm Renault, the trade secret holder or the user, or if destruction of the infringing goods would not be disproportionate in light of the interests of Renault, the trade secret holder or the user; - inform the user of the unauthorised use or disclosure of the data and of the measures taken to put an end to that unauthorised use or disclosure;

	- compensate the party harmed by the improper use or disclosure of the unlawfully accessed or used data.

The protection measures listed above also apply to (i) users or data recipients who alter or remove technical and organisational measures implemented by Renault or who do not maintain the measures to protect trade secret data implemented by the user or by the trade secret holder (if different) in agreement with Renault, and (ii) any other party receiving the user's data further to an infringement of the Data Act.

Users may also rely on the above protections if a data recipient makes it unduly difficult for the user to exercise their choices or rights, or uses the data received for profiling, unless profiling is necessary to provide the service requested by that user.

11. **What are the user's obligations with respect to the data?**

Users must:

- use the data solely for the purposes and in accordance with the law and the terms agreed with Renault,
- comply with protection measures agreed with Renault to preserve the confidentiality of shared data,
- not use the data obtained from Renault to develop a product competing with the connected product from which the data originates, and from sharing that data with any third party for the same purpose,
- not use the data to obtain information on Renault's economic situation, assets, or production methods,
- not use coercive means or exploit potential gaps in Renault's technical infrastructure aimed at protecting the data in order to gain access to that data, and
- not share the data with third parties designated as "gatekeepers" under the EU Digital Markets Act.

12. **What are Renault's obligations to data recipients in its capacity as data holder?**

In business-to-business relationships, Renault makes data available to data recipients on terms and conditions that are fair, reasonable, non-discriminatory and transparent.

Renault does not discriminate between comparable categories of data recipients in the terms and conditions for making data available. If a recipient considers that data has been provided on discriminatory terms and submits a reasoned claim to that effect, Renault will provide information demonstrating the lack of any discrimination without undue delay.

Renault does not use unfair contract terms within the meaning of the Data Act, or clauses that exclude, derogate from or vary the effects of the application of user's rights under Chapter II of the Data Act.

Renault only makes data available to a data recipient, including on an exclusive basis, if asked to do so by a user under Chapter II of the Data Act.

Renault and data recipients are not required to provide any information beyond what is necessary to verify compliance with the contract terms agreed for making data available or with their obligations under EU law and national law adopted in accordance with EU law.

Renault can require compensation from the data recipient for making the data available at the user's request. This compensation is non-discriminatory and reasonable, and may include a margin.

Compensation takes the following into account:

- costs incurred to make data available, including the costs necessary to format, electronically disseminate, and store the data;

- investments in collecting and producing data, where applicable, after taking into account whether other parties helped obtain, generate, or collect that data;

- the volume, format, and nature of the data.

However, the compensation charged by Renault cannot exceed the costs referred to in the first bulleted line above if the data recipients are SMEs or non-profit research organisations without any partner enterprises or linked enterprises that do not qualify as SMEs.

Renault will provide data recipients with sufficiently detailed information showing the basis for calculating compensation so the data recipient can determine whether the above requirements have been satisfied.

13. What to do in case of a claim?

If you have a claim, please contact Renault using the form provided on the Mobilize Data Solutions platform (https://datasolutions.mobilize.com/contact-us).

We will endeavour to answer and process your requests as soon as possible.

If you are not satisfied with our response, you may apply to the designated forum for dispute resolution, without prejudice to your right to seek a remedy in the French courts.

The dispute resolution forum is competent to address claims pertaining to:

- contractual restrictions or prohibitions involving connected product security requirements or refusals or suspension of data sharing to protect data confidentiality;

- fair, reasonable, and non-discriminatory terms and conditions applying to the provision of data and the transparent method of making that data available in accordance with Chapters III and IV of the Data Act.